UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRIA EN TELEMÁTICA

Diseño de la Seguridad Informática en la implementación del Data Center de la Universidad Nacional de Loja

Proyecto Desarrollado previo a la obtención del grado de "Magíster en Telemática"

HERNÁN LEONARDO TORRES CARRIÓN

DIRECTOR: Msg. Ing. DIEGO ÁVILA

CUENCA – ECUADOR

JULIO 2010

OBSERVACION:

EL CONTENIDO DE ESTA TESIS ES DE ABSOLUTA RESPONSABILIDAD DEL AUTOR.

Ing. Hernán Leonardo Torres Carrión

RESUMEN

Debido a que el uso de las redes de datos y el Internet se encuentran en aumento en las instituciones académicas de Nivel Superior por la facilidad de acceso a la información y más aún información que sirve de base para nuevas investigaciones realizadas por estas entidades educativas y el traslado de las mismas luego a sus estudiantes, que son la razón de ser de la Universidades, cada vez más instituciones permiten a sus usuarios acceder a sus sistemas de información. Por lo tanto, es fundamental saber, qué recursos de la institución necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a los usuarios al Internet.

Este proyecto desarrollado en el marco de ofrecer a la Universidad Nacional de Loja una propuesta que sirva para la implementación de seguridad informática en el acceso a sus redes y a la información que maneje esta institución, información que le sirve solo a ella y que si no se concientiza sobre la importancia de manejar sistemas seguros puede ser utilizada para otros fines no autorizados.

Esta seguridad propuesta en el presente trabajo será manejada desde el Data Center de la Universidad Nacional de Loja, tomando como antecedente, la construcción del Instituto de Informática, proyecto desarrollado para manejar desde este lugar toda la parte informática de la institución y lugar propicio para la implementación del Centro de Datos con infraestructura

adecuada tanto física como lógica para garantizar el acceso seguro a la información.

Se plantea cubrir con objetivos fundamentales para llegar a una propuesta seria, a ser tomada en consideración para su implementación, como: *El análisis de la situación actual tecnológica de la UNL*, en el cual se realizará un diagnóstico de los equipos y tecnología que maneja actualmente la institución para conocer cuáles son sus falencias en cuanto a equipamiento y seguridades y de esta manera tener un panorama más claro para el planteamiento de la propuesta de solución. *Analizar métodos y estándares a implementar para brindar seguridad informática desde el Data Center de la UNL*, en el cual se analiza de acuerdo a la información acerca de los problemas o falencias encontradas en el diagnóstico de la situación actual, los métodos y estándares necesarios para implementarse en la UNL y brindar seguridad informática en la institución, métodos y estándares que nos ayudarán a identificar que se puede implementar para brindar seguridad desde la extranet y en la intranet de la institución. *Generación de la propuesta para el equipamiento tecnológico a utilizarse desde el Data Center de la UNL para brindar la seguridad informática requerida*, en el cual se plantea la utilización de ciertos equipos que ayudarán a brindar mayor seguridad en el acceso a la información dentro de la institución y hacia fuera de ella. *Propuesta de un manual de políticas de seguridad informática manejado desde el Centro de Datos de la UNL que ayude a la protección adecuada de la confidencialidad, la intimidad y la integridad de la información*, en el cual se plantea un manual de políticas de seguridad informática que podría utilizar el Instituto de Informática en sí, para definir reglas claras

en el acceso a la información, utilización de las redes y sistemas informáticas en la institución.

El cambio de la mentalidad de los usuarios de las redes de información en la institución es vital para cualquier mejora o cambio que se desee realizar, la concientización en los usuarios es la mejor arma para combatir las amenazas que se podrían sucintar.

SUMMARY

More and more higher education academic institutions allow their users access to their information system because the use of data networks and the Internet are on the rise for the ease of access to information and such information can used as a basis for further investigations undertaken by these educational institutions and then transfering this to their students, which is the reason that these universities exist. Therefore, it is essential to know, what resources need protection for the institution, controlling access to the system and the rights of users of the information system. The same procedures apply when you allow users access to the Internet.

This project developed as part of providing a proposal to the "Universidad Nacional de Loja" for the implementation of information security in access to their networks and information this institution, handles; information that serves only itself and not only that, but raises awareness about the importance of managing secure systems which cannot be used for other unauthorized purposes.

The security proposal in this work will be managed from the Data Center at the "Universidad Nacional de Loja", based on the construction of the Informatics Institute, a project developed to manage from here all the institution's information and place conducive to the implementation of the Data Center with adequate infrastructure both physical and logical to ensure secure access to information.

This raises fundamental objectives to reach a serious proposal, to be taken into consideration for implementation, including:

1. The analysis of the current situation of the UNL technology which includes making a diagnosis of equipment and technology that currently manages the institution to know what weaknesses it has in terms of equipment and securities and thereby have a clearer picture for the approach of the proposed solution.
2. Analyze methods and standards to be implemented to provide computer security from the Data Center at UNL, which is analyzed according to information about problems or shortcomings encountered in the diagnosis of the current situation,
3. methods and standards needed to be implemented at UNL and provide information security in the institution - methods and standards that will help us identify what can be deployed to provide security from the extranet and intranet of the institution.
4. Generating the proposal for the technological equipment used from the Data Center at UNL to provide the required information security, which considers the use of certain equipment that will help provide more secure access to information within and without of the institution.
5. Proposal for a handbook of information security policies managed from the Data Centre of the UNL to assist with the appropriate protection of confidentiality, privacy and integrity of information, and proposing a policy manual for computer security that the Institute of Informatics in itself, could use to

define clear rules on access to information, use of computer systems and networks within the institution.

Changing the mindset of the users of information networks in the institution is vital to any improvement or change you want to do. Awareness of the users is the best weapon to combat threats that could be happen.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

FASE 1: INICIO

1.1 ANTEPROYECTO

1.1.1 TÍTULO

Diseño de la Seguridad Informática en la Implementación del Data Center de la Universidad Nacional de Loja

1.1.2 INTRODUCCIÓN

Las Instituciones Educativas de Nivel Superior a nivel mundial han experimentado los grandes cambios tecnológicos que ha sufrido el planeta, por lo que les a tocado ponerse a la par de esos cambios, teniendo que implementar infraestructura tecnológica que les permita ofrecer a sus entes investigadores la posibilidad de conectarse con el mundo y de esta manera mejorar sus niveles académicos. Estos cambios no solo han afectado a las Universidades sino también a un sin número de empresas que necesitan de la tecnología para poder seguir ampliando sus mercados; eso ha hecho que las instituciones piensen en montar sus Centros de Datos, para desde ahí poder manejar toda la información y distribuirla a través de medios alambricos o inalámbricos a todos sus beneficiarios, tecnología que cada año tiene que ir mejorando.

Con este antecedente de la realidad mundial tecnológica, la Universidad Nacional de Loja fundada el 31 de Diciembre de 1859, que es una Institución de Educación Superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, de alta calidad académica y humanística, que ofrece

formación en los niveles: técnico y tecnológico superior; profesional o de tercer nivel; y, de postgrado o cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural y étnica y la sabiduría popular, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano y con una edad de 150 años sirviendo a la colectividad, quiere también estar a la par de los avances tecnológicos, con cerca de 20000 estudiantes tanto en la modalidad presencial como a distancia, es de gran necesidad pensar en la implementación de un Centro de Datos acorde y acoplado para ese fin, teniendo en consideración toda la parte de seguridad tanto lógica como física que debería tener ese Data Center, el mismo que la ayudará a esta institución a manejar de manera centralizada toda la información que actualmente posee y de esta maneja brindar mejores servicios tecnológicos a su personal administrativo, estudiantado y colectividad en general. Con la Implementación de este Centro de Datos la institución se debería preocupar de una parte fundamental dentro de este proyecto que es, la seguridad que debería tener este centro, en cuanto a la información, tecnología y medios de transmisión que maneje.

1.1.3 DESCRIPCIÓN DEL PROYECTO

La Universidad Nacional de Loja actualmente posee una infraestructura en redes que le permite trabajar con ciertas

limitaciones, debido al gran campus al que hay que satisfacer en los requerimientos tecnológicos y de comunicaciones, además el crecimiento tecnológico de la institución ha sido significativo en estos últimos años, teniendo que llegar a ofrecer más y mejores servicios a la comunidad universitaria, dejando un poco de la infraestructura adecuada y las seguridades que se tienen que implementar cuando la tecnología va creciendo.

El problema en si para la propuesta de este proyecto es la falta de una infraestructura física y tecnológica adecuada que maneje de manera centralizada la información de toda la Institución y por ende las seguridades que esta infraestructura debe ofrecer a la información y al equipamiento, esto acarrea muchos otros problemas que se analizarán en el transcurso del desarrollo del proyecto.

Actualmente la Universidad Nacional de Loja no posee un lugar adecuado con todos los estándares necesarios para convertirlo en un centro de datos, es por eso que la propuesta de este proyecto va encaminada a ofrecer una alternativa para la construcción e implementación del DATA CENTER para la UNL, y particularmente trabajar en una propuesta de seguridad que pueda cubrir toda la información y equipamiento tecnológico que maneje la institución en este centro de datos, de tal manera que se pueda tener una mejor organización en el manejo de la información. Algunas de las actividades establecidas para llegar a cumplir con esta propuesta serían:

1. Buscar el espacio físico adecuado para la construcción del DATA CENTER.
2. Establecer estándares de seguridad física que tiene que cumplir el DATA CENTER.

3. Realizar un análisis del equipamiento tecnológico actual con el que cuenta la Universidad para poder definir cuales de esos equipos podrían servir para la propuesta que se pretende realizar y cuales se tendría que redefinir su uso.
4. Realizar la determinación del equipamiento tecnológico para la implementación del DATA CENTER y de la seguridad del mismo.
5. Establecimiento de alternativas para la seguridad lógica de toda la red de datos de la UNL.

La alternativa propuesta se adaptará al crecimiento exponencial de los datos y a brindar mejoras sostenibles en cuanto a: Excelencia y Calidad de Servicio, Eficacia en las Operaciones y Procesos de Gestión, dentro de la Universidad Nacional de Loja.

El análisis y diseño de un data center de la Universidad Nacional de Loja pretende disminuir el problema en torno al incremento de los procesos de intercambio y comunicación entre los integrantes de la comunidad universitaria, lo cual amerita una estructura tecnológica que organice, resguarde y administre todos los procesos internos de la Universidad en función de la data (red de datos, voz, internet, etc) que se intercambia de manera permanente en la Universidad, en referencia a esto el proyecto está encaminado a ofrecer las seguridades adecuadas para el buen funcionamiento del Centro de Datos de la UNL.

1.1.4 JUSTIFICACIÓN

1.1.4.1 Justificación Tecnológica

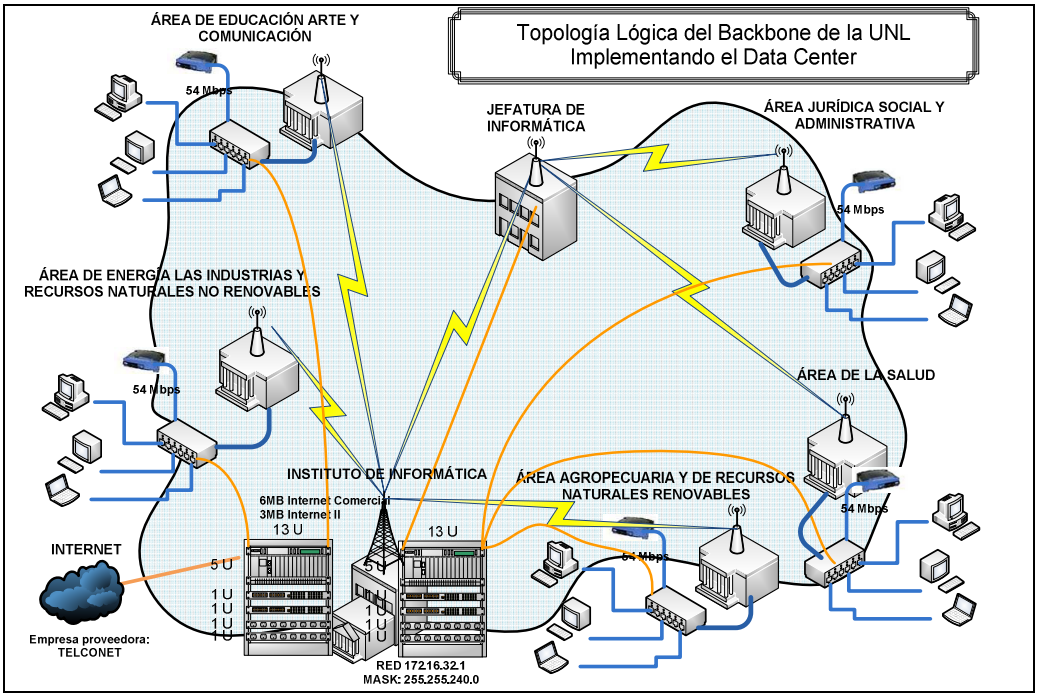
Teniendo en cuenta que la tecnología ha ido creciendo de manera apresurada desde sus inicios en la década de los 40s, 50s con la creación de los computadores y más aún en la década de los 80s en adelante, cuando las grandes empresas fabricantes del hardware y software comenzaron a inmiscuir a la gente en el mundo de la informática y de la nueva era de la información y comunicación a través de PCs, dándonos así una visión moderna de la educación que hoy en día necesitan nuestros jóvenes.

Siempre los países llamados primer mundistas han llevado la batuta en cuanto a los avances tecnológicos, y es por el hecho de que las instituciones educativas se han comprometido a enseñar a sus estudiantes desde muy chicos las exigencias del mundo actual, pero así mismo acompañados de los equipos tecnológicos necesarios para su desenvolvimiento.

En el Ecuador las Universidades tratan de ponerse al tanto en los avances tecnológicos existentes, de tal manera que puedan convertirse en instituciones educativas competitivas. La propuesta que se está desarrollando en este proyecto hace que la Universidad Nacional de Loja se convierta en eso, una Universidad Competitiva. La construcción e implementación del Data Center en la UNL y en sí el encargarse de la seguridad en la información y el equipamiento que maneje el mismo, resolvería muchos problemas que actualmente los atraviesa en la parte informática.

Tecnológicamente el proyecto es totalmente viable ya que se tiene en el mercado toda la infraestructura necesaria para la implementación, se puede realizar convenios con marcas reconocidas como CISCO, 3COM o con sus representantes en el Ecuador para que nos puedan facilitar el asesoramiento necesario para la implementación de estos equipos como Routers, Switchs, firewalls, Servidores, etc; que ofrezcan mayor seguridad en la información también se podría buscar el asesoramiento técnico para implementar un plan de seguridades físicas de Data Center, desde el ingreso al mismo hasta el sistema de enfriamiento interno. Lo importante es poder seleccionar la mejor propuesta en equipos tecnológicos necesarios para el buen funcionamiento del Data Center de la Universidad Nacional de Loja. A demás nos podríamos valer de experiencias de Universidades aleadas en cuanto a la implementación del Data Center de cada una de ellas, para que nos puedan dar un asesoramiento en cuanto a que se debería adquirir como equipamiento para resolver ciertos problemas de la red en la UNL.

En la siguiente figura se muestra de manera general un esquema de cómo sería el funcionamiento de la red de la UNL utilizando el equipamiento tecnológico necesario en el Data Center.



1.1.4.2 Justificación Legal y/o Regulatorio.

Actualmente la Universidad Nacional de Loja cuenta con un proyecto de construcción del Edificio de Informática desde donde se tiene establecido, se manejará toda la infraestructura de comunicaciones e informática de toda la institución. En los estatutos internos de la universidad está establecido que cualquier proyecto de infraestructura tecnológica bien justificado a ser implementado en la UNL tendrá que ser sometido a consejo académico Superior para conocer si la Universidad lo puede financiar directamente o necesita conseguir ayuda externa para su financiamiento en este caso desde el Senplades; por lo que desde el punto de vista legal se tiene toda la disposición para realizar este tipo de proyecto.

1.1.4.3 Justificación Económica – Financiera y Comercial

Es importante tomar en cuenta que la Universidad Nacional de Loja, es una institución pública sin fines de lucro, por lo que el principal objetivo es la educación superior de los ciudadanos Ecuatorianos y especialmente de la región sur del país, por lo que en este tipo de proyecto no se tiene planificado obtener ganancias económicas sino mas bien la satisfacción del estudiantado al tener servicios tecnológicos que ofrezcan una educación de calidad.

El proyecto de la construcción e implementación del Data Center de la Universidad Nacional de Loja, por ser una Institución pública, puede ser financiado a través de la SECRETARIA NACIONAL DE PLANIFICACIÓN Y DESARROLLO (SENPLADES) que es el organismo rector de la planificación pública del país y cuya función es determinar la prioridad de los proyectos de inversión del sector público. En este caso es el único camino de financiamiento a nivel Nacional, definido justamente por la cantidad de presupuesto disponible para el gasto de la UNL. En otro caso la Universidad podría realizar un convenio con algún organismo no gubernamental que quiera aportar con el recurso económico necesario para realizar esta inversión. De todas maneras se establece dos caminos importantes para conseguir el financiamiento para este proyecto de gran significación para la institución.

El Data Center de la UNL ofrecerá básicamente servicios tales como:

1. EL rápido acceso a la información (Internet).
2. Seguridad Física y lógica de la red y su información.
3. Respaldos y restauración de datos en la institución.
4. Ejecución de procesos informáticos centralizados.
5. Manejo de servidores para cada una de las aplicaciones que tenga la UNL.
6. Mantenimiento continúo del flujo eléctrico, garantizando el servicio sin interrupciones.

Los anteriores son algunos de los servicios que el Data Center prestará a la comunidad universitaria, cabe mencionar que el proyecto tiene una buena rentabilidad, pero encaminada al ámbito social, por lo que en este caso no perseguimos fines de lucro, teniendo en cuenta que la sostenibilidad de este proyecto en su trabajo diario dependerá del presupuesto económico que le asigne el Gobierno Nacional a la Universidad Nacional de Loja.

1.1.5 OBJETIVOS

1.1.5.1 General

Realizar el Diseño de la Seguridad Informática en la implementación del Data Center de la Universidad Nacional de Loja.

1.1.5.2 Específicos

- Analizar la situación actual de la infraestructura tecnológica y el procesamiento de la información en la UNL.

- Analizar los métodos y estándares que se podrían implementar para seguridad informática y telemática en el Data Center de la UNL.
- Generar la propuesta para el equipamiento tecnológico y montos de inversión necesarios para brindar la seguridad adecuada del Data Center de la UNL.
- Proponer un manual de políticas de seguridad tanto físicas y lógicas para el Centro de Datos de la UNL que ayude a la protección adecuada de la confidencialidad, la intimidad y la integridad de la información.

1.1.6 ALCANCE

Tomando en consideración los objetivos planteados se analiza que el presente proyecto es parte de la construcción del Data Center; es decir el proyecto que se ofrece a la comunidad Universitaria se podrá poner en marcha una vez que se tenga aprobada la construcción del mismo; como antecedente importante, la Universidad Nacional de Loja tiene un proyecto aprobado denominado "Construcción del Instituto de Informática", por lo que esa es la oportunidad para plantear que el Centro de Datos se lo pueda implementar en ese edificio en donde funcionará este instituto y por ende el proyecto de seguridad sería puesto en marcha. De esta manera nos centramos en analizar, cual es el producto que se ofrece en si, hasta donde llegará este trabajo y cuales serán nuestros beneficiarios directos e indirectos.

Productos	Usuarios
Diseño de la Seguridad Informática como	Todas las personas (Docentes, Administrativos, Trabajadores,

propuesta para ser tomada en cuenta en la implementación del Data Center de la Universidad Nacional de Loja.	Estudiantes, Comunidad en general) que se encuentran de una u otra manera vinculados con la Universidad Nacional de Loja.
Resultados	Beneficiarios Inmediatos
Docentes, Administrativos, Trabajadores, Estudiantes satisfechos con el acceso a la información en cuanto a la rapidez y seguridad. Docentes, Administrativos, Trabajadores, Estudiantes satisfechos con un plan de riesgos en caso que suceda alguna eventualidad. Mejorar el flujo de la información en toda la Universidad de tal manera que el Data Center será el cerebro de toda el alma mater Lojana.	Docentes, Administrativos, Trabajadores, Estudiantes, que se encuentran vinculados con todos los estamentos de la Universidad Nacional de Loja al ver que sus datos están seguros y el acceso a la información es más rápida y desde cualquier punto del campus. La Universidad Nacional de Loja comprometida con la educación de nuestra gente.

Imagen de la Universidad Nacional de Loja preocupada en el mejoramiento tecnológico de la institución y del buen servicio que se le pueda dar a todos los involucrados con la entidad.	
Efectos	Beneficiarios Mediatos
Satisfacción en el flujo de la información en toda la Universidad por parte de los actores de la misma. Barreras de seguridad difíciles de penetrar, por lo que se garantiza la estabilidad y la fiabilidad de la información. La posibilidad de nuevas oportunidades en el campo laborar de las personas que residen en la ciudad, provincia y país.	Los estudiantes de todos los colegios del país que ven en la Universidad Nacional de Loja una institución reconocida que puede brindarles una educación integral y la posibilidad de conseguir un título de tercer y cuarto nivel. La Colectividad en General que buscan instituciones Educativas con la infraestructura física y tecnológica necesaria para que puedan desarrollar sus investigaciones.

El proyecto de seguridad informática para el Data Center está formado por 4 fases las cuales se detallan a continuación.

PRIMERA FASE: INICIO

En esta fase se describe el cómo iniciar el proyecto conjuntamente con todo el conocimiento teórico necesario para el buen planteamiento de la solución.

SEGUNDA FASE: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

En esta fase se realiza un diagnóstico de la situación actual o un análisis de la situación actual, el mismo que nos arrojará información acerca de cómo está actualmente la universidad en cuando a infraestructura y equipamiento tecnológico, lo que me servirá para realizar un buen planteamiento en cuanto a equipamiento necesario para la seguridad en la información y en la infraestructura.

TERCERA FASE: DESARROLLO DE LA SOLUCIÓN PLANTEADA

En esta fase se tiene planificado desarrollar la propuesta de diseño de la seguridad informática del Data Center, por su puesto analizando ya los mecanismos que se deben poner en marcha para ofrecer esta seguridad, así como los estándares que se deberían cumplir.

CUARTA FASE: REQUERIMIENTOS EN EQUIPAMIENTO

Aquí en esta fase se detallará el equipamiento necesario para ofrecer seguridad en los datos y en el equipamiento tecnológico de la institución, así como la inversión que implica la solución planteada.

1.1.7 METODOLOGÍA

Los métodos que se utilizarán en el desarrollo de este proyecto de investigación son los que seguidamente se enuncian. El método inductivo y el método deductivo los mismos que siguen el proceso analítico sintético y satisfacen los requerimientos propios de las ciencias informáticas en lo referente a la recolección de datos, análisis de la información e interpretación de los hechos y descubrimiento de nuevos procedimientos.

Me basaré en la investigación experimental, la misma que está integrada por un conjunto de actividades metódicas y técnicas que se realizan para recabar la información y datos necesarios sobre el tema a investigar y el problema a resolver.

Las actividades que necesariamente se deben realizar para alcanzar los objetivos planteados son:

- Reunión con los directivos de la Universidad Nacional de Loja, para presentar la presentación de la propuesta.
- Reunión en la que se definirá los compromisos adquiridos de parte de la Institución y los autores de la propuesta.
- Recolección de información de la situación tecnológica actual de cada una de las áreas que conforman la

comunidad Universidad, para ello se piensa trabajar conjuntamente con el personal que está directamente ligado a estos temas, como son los directores de cada área y los responsables de los centros de cómputo, para estas tareas utilizaremos el método inductivo deductivo, en las que se incluyen las técnicas como, entrevistas, encuestas, cuestionarios, y observación directa.

- En base a la información obtenida se realizara el diseño de la propuesta tomando como base el Estandar TIA-942 que brinda los requerimientos y lineamientos necesarios para el diseño e instalación de Data Center. En los que se establecen los siguientes Requerimientos de los diferentes elementos de un Data Center, que son: Estructura, Ubicación, Acceso, Protección contra incendios, Equipos, y Redundancia.
- Se realizara una propuesta del equipamiento tecnológico necesario para la puesta en marcha del proyecto, en las que se tomará en cuenta, características técnicas de alto rendimiento basado en los estándares de seguridad adecuados.

1.2 MARCO TEÓRICO

1.2.1 DATA CENTER

1.2.1.1 Definición

Es aquella ubicación en donde se concentran los recursos necesarios para el procesamiento de la información de una organización, dichos recursos consisten esencialmente en unas

dependencias debidamente acondicionadas con toda la infraestructura necesaria en cuanto a Computadoras y Redes de Comunicaciones. También se le conoce con el nombre de Centro de Procesamiento de Datos (CDP) o simplemente su traducción del inglés, Centro de Datos (CD)[1].

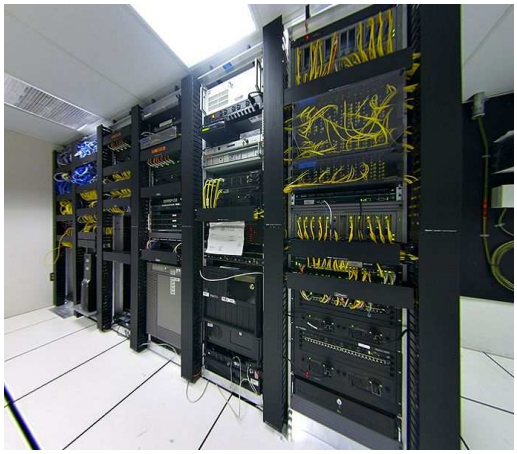


Fig. 1: Data Center

1.2.1.2 Características

Un Data Center (DC) es una sala de gran tamaño o incluso un edificio dependiendo de la cantidad de información que se maneje, usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un Banco (Institución Financiera) puede tener un Data Center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las organizaciones sean estas medianas o

[1] http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

grandes tienen algún tipo de DC, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un DC se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicadas, así como servidores de bases de datos que puedan contener información crítica.

En el Caso de la Universidad Nacional de Loja es muy importante la implementación del mismo ya que el flujo de información generada en la institución cada vez va creciendo más, por lo que se necesita garantizar el buen uso, el correcto acceso y el resguardo de esa información.

1.2.1.3 Diseño[2]

El diseño de un centro de procesamiento de datos comienza por la elección de su ubicación geográfica, y requiere un balance entre diversos factores:

- Costo económico: costo del terreno, impuestos municipales, seguros, etc.
- Infraestructuras disponibles en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
- Riesgo: posibilidad de inundaciones, incendios, robos, terremotos, etc.

[2] http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos requisitos de las dependencias son:

- Doble acometida eléctrica.
- Muelle de carga y descarga.
- Montacargas y puertas anchas.
- Altura suficiente de las plantas.
- Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informático.
- Almacenes.
- Etc.

Aún cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior:

- Piso Falso y Techo falso.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP.
- Etc.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la seguridad física de la instalación, lo que incluye:

- Cerraduras electromagnéticas.
- Torniquetes.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Etc.

Una vez acondicionado el lugar se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un diseño lógico de redes y entornos, sobre todo en aras a la seguridad. Algunas actuaciones son:

- Creación de zonas desmilitarizadas (DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).
- Despliegue y configuración de la electrónica de red: pasarelas, encaminadores, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Etc.

Parte de la seguridad de la información que se maneja en un Data Center, es el tener un Centro de Respaldo.

1.2.1.4 Centro de Respaldo[3]

Es un Data Center diseñado específicamente para tomar el control de otro **DC principal** en caso de contingencia, su misión es la de resguardar la información que maneje una organización.

Grandes organizaciones, tales como Bancos, Administraciones Públicas e Instituciones Educativas de alto nivel, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su Centro de Proceso de Datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un ***centro de respaldo*** para absorber las operaciones del DC principal en caso de emergencia.

Un Centro de Respaldo se **diseña** bajo los mismos principios que cualquier DC, pero bajo algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del DC principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del DC principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.

En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el DC principal. Esto no implica que el equipamiento deba ser *exactamente* igual. Normalmente, no todos los procesos del DC principal son críticos. Por este

[3] http://es.wikipedia.org/wiki/Centro_de_respaldo

motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La *pecera* de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

- Sala blanca: cuando el equipamiento es *exactamente* igual al existente en el CPD principal.
- Sala de back-up: cuando el equipamiento es similar pero no exactamente igual.

En tercer lugar, el equipamiento software debe ser idéntico al existente en el DC principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

1.2.2 SEGURIDAD INFORMÁTICA[4]

La **seguridad informática** consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

[4] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

1.2.2.1 Introducción

Podemos entender como seguridad un estado de cualquier tipo de información o la (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**: La información sólo debe ser legible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

1.2.2.2 Términos relacionados con la Seguridad Informática

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza**: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto**: medir la consecuencia al materializarse una amenaza.
- **Riesgo**: Es la probabilidad de que suceda la amenaza o evento no deseado
- **Vulnerabilidad**: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista

de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. **Una persona no autorizada podría:** Clasificar y desclasificar los datos, Filtrar información, Alterar la información, Borrar la información, Usurpar datos, Hojear información clasificada.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Copia de seguridad completa, Todos los datos (la primera vez), Copias de seguridad incrementales, Sólo se copian los ficheros creados o modificados desde el último backup, Elaboración de un plan de backup en función del volumen de información generada

- **Tipo de copias, ciclo de esta operación, etiquetado correcto.**
- **Diarias, semanales, mensuales: creación de tablas.**

1.2.2.3 Objetivos

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

Información

Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Equipos que la soportan

Software, hardware y organización.

Usuarios

Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

1.2.2.4 Gestión de Riesgo en la Seguridad Informática[5]

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

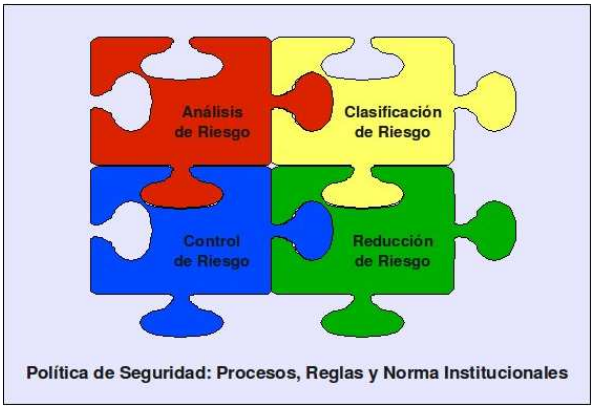


Fig. 2: Gestión de Riesgo

La gestión de Riesgo está formada por cuatro partes:

- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.

[5] http://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

- **Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

  Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

1.2.2.5 Seguridad de la Información y Protección de los Datos

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos.

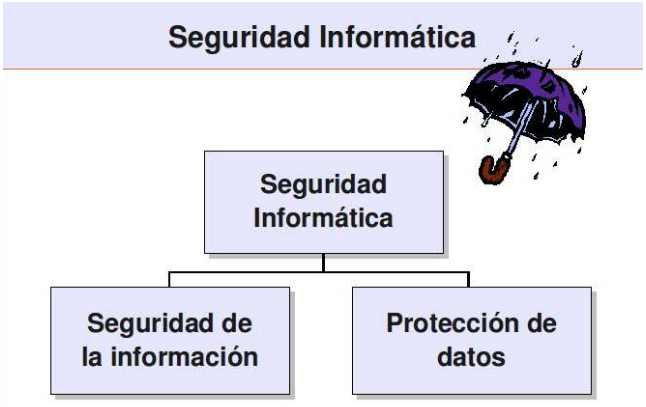


Fig. 3: Seguridad Informática

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

Fig. 4: Seguridad de la Información

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial).

Fig. 5: Protección de Datos

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética

personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Países existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente. En el Ecuador con la nueva constitución existen leyes que protegen a la intimidad personal.

1.2.2.6 Normas ISO

1.2.2.6.1 Norma ISO-IRAM-IEC 17799 - Tecnología de la Información – Técnicas de Seguridad - Código de Práctica para la Administración de la Seguridad de la Información[6]

Es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de

[6] http://es.wikipedia.org/wiki/Iso_17799

revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.

Importancia

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como *"la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)"*.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.
9. Gestión de incidentes de seguridad de la información.
10. Gestión de continuidad de negocio.
11. Conformidad.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

Objetivo

El Objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas

Casos de Éxito

En *España* existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada *Código de buenas prácticas para la Gestión de la Seguridad de la Información*, que es una copia idéntica y traducida del inglés de la Norma Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 se estima que esté disponible en la segunda mitad del año 2006.

En *Perú*, la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto de 2004, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de internet y redes de datos institucionales. La supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI ([1]).

En *Chile*, se empleó la ISO/IEC 17799:2005 para crear una norma que establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documento electrónicos de los órganos de la Administración del Estado de la República de Chile, y cuya aplicación se recomienda para los mismos fines, denominado Decreto Supremo No. 83, "NORMA TÉCNICA SOBRE SEGURIDAD Y CONFIDENCIALIDAD DEL DOCUMENTO ELECTRÓNICO".

Migración

Con la aprobación de la norma ISO/IEC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la seguridad de la información, la ISO/IEC 17799:2005 pasó a ser renombrada como ISO/IEC 27002 en la revisión y actualización de sus contenidos en el 2007.

1.2.2.6.2 Norma ISO/IEC 27000 - Tecnología de la Información – Técnicas de Seguridad – La Seguridad de la Información de Gestión de Sistemas – Fundamentos y Vocabulario

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La serie ISO/IEC 27000 está formado por algunas normas que van desde (27000 a 27019 y de 27030 a 27044) y que indican cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI).

1.2.2.6.2.1 Sistema de Gestión de la Seguridad de la Información (SGSI)[7]

Un **Sistema de Gestión de la seguridad de la Información *(SGSI)*** es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en inglés "Information Security Management System" (ISMS).El concepto clave de un SGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

[7] http://es.wikipedia.org/wiki/SGSI

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

1.2.2.6.2.2 ISO/IEC 27001: Tecnología de la información - Técnicas de seguridad - Especificación de un Sistema de Gestión de Seguridad de la Información

Publicada el 15 de Octubre de 2005, es la certificación que deben obtener las organizaciones. Esta norma específica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

1.2.2.6.2.3 ISO / IEC 27002: Tecnología de la información – Técnicas de seguridad - Código de Práctica para la Gestión de Seguridad de la Información

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

1.2.2.6.2.4 ISO / IEC 27003: Tecnología de la información - Técnicas de Seguridad – Guía de implementación del sistema de administración y seguridad de la información

Publicada el 01 de Febrero de 2010. No es certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

1.2.2.6.2.5 ISO / IEC 27004: Tecnología de la información - Técnicas de Seguridad – Administración de medidas de seguridad de la información.

Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

1.2.2.6.2.6 ISO / IEC 27005: Tecnología de la información - Técnicas de Seguridad – Administración de riesgos en la seguridad de la información

Publicada el 4 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

1.2.2.6.2.7 ISO / IEC 27006: Tecnología de la información – Técnicas de Seguridad - Requisitos para la prestación de auditoría y certificación de sistemas de gestión de seguridad de la información.

Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

1.2.2.6.2.8 ISO/IEC 27033: Tecnología de la información – Técnicas de Seguridad - Seguridad en Redes

Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 10 de Diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (prevista para 2011); 27033-3, escenarios de redes de referencia (prevista para 2011); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (prevista para 2012); 27033-5, aseguramiento de comunicaciones mediante VPNs (prevista para 2012); 27033-6, convergencia IP (prevista para 2012); 27033-7, redes inalámbricas (prevista para 2012).

1.2.2.7 Análisis de Riesgo Informático

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y*

procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

1. Construir un perfil de las amenazas que esté basado en los activos de la organización.
2. Identificación de los activos de la organización.
3. Identificar las amenazas de cada uno de los activos listados.
4. Conocer las prácticas actuales de seguridad.
5. Identificar las vulnerabilidades de la organización.

    - Recursos humanos
    - Recursos técnicos
    - Recursos financieros

6. Identificar los requerimientos de seguridad de la organización.
7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
8. Detección de los componentes claves
9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

    - Riesgo para los activos críticos
    - Medidas de riesgos
    - Estrategias de protección
    - Planes para reducir los riesgos.

1.2.2.8 Tipos de Ataques en las Redes Informáticas

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ***ataques activos***, que producen cambios en la información y en la situación de los recursos del sistema, y los ***ataques pasivos***, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

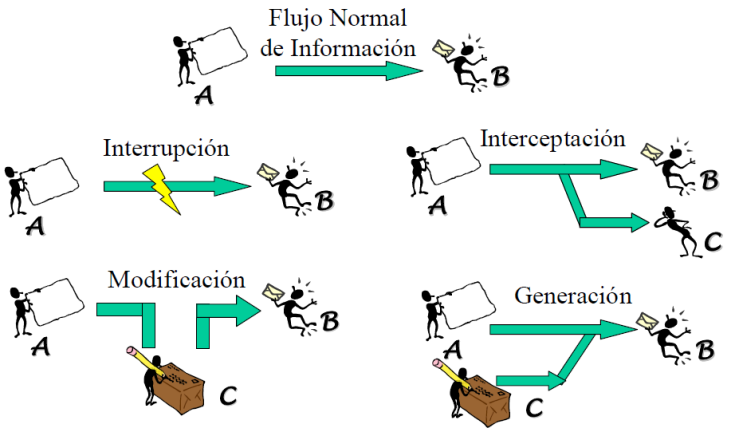


Fig. 6: Ataques en una Red Informática

A continuación se presenta una relación más detallada de los principales tipos de ataques contra redes y sistemas informáticos:

1.2.2.8.1 Actividades de Reconocimiento de Sistemas

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas

informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

1.2.2.8.2 Detección de Vulnerabilidades en los Sistemas

Este tipo de ataques tratan de detectar y documentar las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como “exploits”).

1.2.2.8.3 Robo de información mediante la interceptación de mensajes

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

1.2.2.8.4 Modificación del contenido y secuencia de los mensajes transmitidos

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como “ataques de repetición” (“replay attacks”).

1.2.2.8.5 Análisis del Tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los **"sniffers"**. Así, se conoce como **"eavesdropping"** a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Una organización podría protegerse frente a los "sniffers" recurriendo a la utilización de redes conmutadas **("switches" en lugar de "hubs")** y de redes locales virtuales **(VLAN)**. No obstante, en redes locales que utilizan "switches" (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como ***"MAC flooding"*** para provocar un desbordamiento de las tablas de memoria de un switch (tablas denominadas CAM por los fabricantes, *"Content Addresable Memory"*) para conseguir que pase a funcionar como un simple "hub" y retransmita todo el tráfico que recibe a través de sus puertos (al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria).

Por otra parte, en las redes VLAN (redes locales virtuales) un atacante podría aprovechar el protocolo DTP (Dynamic Trunk Protocol), utilizado para poder crear una VLAN que atraviese varios switches, para intentar saltar de una VLAN a otra, rompiendo de este modo el aislamiento físico impuesto por la organización para separar sus distintas redes locales.

1.2.2.8.6 Ataques de Suplantación de identidad

1.2.2.8.6.1 IP Spoofing

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada “IP Spoofing” (“enmascaramiento de la dirección IP”), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado.

Los propietarios de las redes y operadores de telecomunicaciones podrían evitar en gran medida el “IP Spoofing” implantando filtros para que todo el tráfico saliente de sus redes llevara asociado una dirección IP de la propia red desde la que se origina el tráfico.

Otro posible ataque sería el secuestro de sesiones ya establecidas (“hijacking”), donde el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir. Con el secuestro de sesiones se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.

1.2.2.8.6.2 DNS Spoofing

Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.
Para ello, en este tipo de ataque los intrusos consiguen que un servidor DNS legítimo acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla. De este modo, se persigue "inyectar" información falsa en la base de datos del servidor de nombres, procedimiento conocido como *"envenenamiento de la caché del servidor DNS"*, ocasionando con ello serios problemas de seguridad, como los que se describen de forma más detallada a continuación:

- Redirección de los usuarios del servidor DNS atacado a Websites erróneos en Internet, que simulan ser los Websites reales. De este modo, los atacantes podrían provocar que los usuarios descargasen de Internet software modificado en lugar del legítimo (descarga de código dañino, como virus o troyanos, desde Websites maliciosos).
- La manipulación de los servidores DNS también podría estar detrás de algunos casos de *"phishing"*, mediante la redirección de los usuarios hacia páginas Web falsas creadas con la intención de obtener datos confidenciales,

como sus claves de acceso a servicios de banca electrónica.

- Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS), al provocar la redirección permanente hacia otros servidores en lugar de hacia el verdadero, que de este modo no podrá ser localizado y, en consecuencia, visitado por sus legítimos usuarios.
- Los mensajes de correo podrían ser redirigidos hacia servidores de correo no autorizados, donde podrían ser leídos, modificados o eliminados. Para ello, basta con modificar el registro MX ("Mail Exchanger") de la tabla de datos del servidor DNS atacado.

Por otra parte, un servidor DNS afectado por este tipo de ataque podría provocar falsas respuestas en los restantes servidores DNS que confíen en él para resolver un nombre de dominio, siguiendo el modelo jerárquico del servicio DNS, extendiendo de este modo el alcance del ataque de "DNS Spoofing".

1.2.2.8.6.3 SMTP Spoofing

El envío de mensajes con remitentes falsos ("masquerading") para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Asimismo, este tipo de ataque

es muy utilizado por los “spammers”, que envían gran cantidad de mensajes de “correo basura” bajo una identidad falsa.

En la actualidad, falsificar mensajes de correo resulta bastante sencillo porque el protocolo SMTP carece totalmente de autenticación. Así, un servidor configurado para aceptar conexiones SMTP en el puerto 25 podría ser utilizado por un usuario externo a la organización, empleando los comandos propios del protocolo, para que envíe mensajes que aparenten tener un origen seleccionado por el atacante cuando realmente tienen otro distinto. La dirección de origen puede ser una dirección existente o una inexistente con el formato adecuado.

No obstante, los servidores de correo también podrían ser configurados para no aceptar envíos de mensajes desde equipos externos a la red local.

1.2.2.8.6.4 ARP Spoofing

ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un “host” quiere comunicarse con una IP emite una trama “ARP-Request” a la dirección de “Broadcast” pidiendo la MAC del “host” poseedor de la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas “ARP-REPLY” indicando su MAC como destino válido para una IP

específica, como por ejemplo en un router, de esta manera la información dirigida al router pasaría por el ordenador atacante quien podrá "sniffar" dicha información y redirigirla si así lo desea. El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica solo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer router. La manera más sencilla de protegerse de esta técnica es mediante tablas ARP estática (siempre que las IPs de red sean fijas).

1.2.2.8.7 Ataques de Denegación de servicios

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

1.2.2.8.7.1 IP Flooding

El ataque de *IP Flooding* se basa en una inundación masiva de la red mediante datagramas IP. Este ataque se realiza habitualmente en redes locales o en conexiones con un gran ancho de banda. Consiste en la generación de tráfico basura con el objetivo de conseguir la degradación del servicio. De esta forma, se resume el ancho de banda disponible, ralentizando las comunicaciones existentes de toda la red.

1.2.2.8.7.2 Smurf

Este tipo de ataque de denegación de servicio es una variante del ataque anterior (*IP Flooding*), pero realizando una suplantación de las direcciones de origen y destino de una petición ICMP del tipo echo-request.
Como dirección de origen se pone la dirección IP de la máquina que debe ser atacada. En el campo de la dirección IP de destino se pone la dirección de difusión de la red local o red que se utilizará como trampolín para colapsar a la víctima.
Con esta petición fraudulenta, se consigue que todas las máquinas de la red respondan a la vez a una misma máquina, consumiendo todo el ancho de banda disponible y saturando el computador atacado.

1.2.2.8.7.3 Teardrop

Este tipo de ataque consistente en el envío de paquetes TCP/IP fragmentados de forma incorrecta. Los equipos vulnerables que no hayan sido conveniente parcheados se "cuelgan" al recibir este tipo de paquetes maliciosos.

1.2.2.8.7.4 TCP/SYN Flooding

El ataque de **TCP/SYNFlooding** se aprovecha del número de conexiones que están esperando para establecer un servicio en particular para conseguir la denegación del servicio.
Cuando un atacante configura una inundación de paquetes SYN de TCP, no tiene ninguna intención de complementar el protocolo de intercambio, ni de establecer la conexión. Su

objetivo es exceder los límites establecidos para el número de conexiones que están a la espera de establecerse para un servicio dado.

Esto puede hacer que el sistema que es víctima del ataque sea incapaz de establecer cualquier conexión adicional para este servicio hasta que las conexiones que estén a la espera bajen el umbral.

Hasta que se llegue a este límite, cada paquete SYN genera un SYN/ACK que permanecerá en la cola a la espera de establecerse. Es decir, cada conexión tiene un temporizador (un límite para el tiempo que el sistema espera, el establecimiento de la conexión) que tiende a configurarse en un minuto.

Cuando se excede el límite de tiempo, se libera la memoria que mantiene el estado de esta conexión y la cuenta de la cola de servicios disminuye en una unidad. Después de alcanzar el límite, puede mantenerse completa la cola de servicios, evitando que el sistema establezca nuevas conexiones en este puerto con nuevos paquetes SYN.

Dado que el único propósito de la técnica es inundar la cola, no tiene ningún sentido utilizar la dirección IP real del atacante, ni tampoco devolver los SYN/ACK, puesto que de esta forma facilitaría que alguien pudiera llegar hasta ´el siguiendo la conexión. Por lo tanto, normalmente se falsea la dirección de origen del paquete, modificando para ello la cabecera IP de los paquetes que intervendrán en el ataque de una inundación SYN.

1.2.2.8.7.5 Ping of death

"El ping de la muerte": mediante el comando "ping –l 65510 direccion_ equipo_victima", envía un paquete IP de un tamaño superior a los 65.536 bytes, provocando el reinicio o "cuelgue" del equipo víctima que lo recibe (si no ha sido protegido frente a esta eventualidad).

El ataque ping de la muerte se basa en la posibilidad de construir, mediante el comando ping, un datagrama IP superior a los 65535 bytes, fragmentado en N trozos, con el objetivo de provocar incoherencias en el proceso de reensamblado.

1.2.2.8.8 Ataques de Inyección de código SQL

El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada.

Como consecuencia de estos ataques y, dependiendo de los privilegios del usuario de base de datos bajo el cual se ejecutan las consultas, se podría acceder no sólo a las tablas relacionadas con la operación de la aplicación del servidor Web, sino también a las tablas de otras bases de datos

alojadas en el mismo servidor Web. También pueden propiciar la ejecución de comandos arbitrarios del sistema operativo del equipo del servidor Web.

1.2.2.9 Consecuencias de la Conexiones no autorizadas a los Sistemas Informáticos

Las conexiones no autorizadas a los sistemas informáticos pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes:

- Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido “borrados” del sistema.
- Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización (“mail relaying”). Esto podría facilitar el reenvío masivo de mensajes de spam a través de un servidor SMTP configurado de forma inadecuada.
- Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas.
- Creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido.

- Consumo del ancho de banda de la red de la organización para otros fines.
- Almacenamiento de contenidos ilegales en los equipos: muchos atacantes aprovechan los equipos comprometidos de una organización para guardar y distribuir copias piratas de software, canciones o vídeos, pornografía infantil, etc.
- Modificación o destrucción de archivos y documentos guardados en un servidor.
- "Website vandalism": modificación del contenido y de la apariencia de unas determinadas páginas Web pertenecientes a la organización.

1.2.2.10 Clasificación de los intrusos en las Redes

1.2.2.10.1 Hackers

Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

El perfil típico de un hacker es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de

comunicaciones, sistemas operativos, etcétera), que invierte un importante número de horas a la semana a su afición.

En la actualidad muchos “hackers” defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que sólo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que aunque no se produzca ningún daño, se podría revelar información confidencial.

Por otra parte, la actividad de un “hacker” podría provocar otros daños en el sistema: dejar “puertas traseras” que podrían ser aprovechadas por otros usuarios maliciosos, ralentizar su normal funcionamiento, etc. Además, la organización debe dedicar tiempo y recursos para detectar y recuperar los sistemas que han sido comprometidos por un “hacker”.

1.2.2.10.2 Crackers

Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o simplemente para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etc.

1.2.2.10.3 Sniffers

Los sniffers son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

1.2.2.10.4 Phreakers

Los phreakers son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los phreakers desarrollaron las famosas “cajas azules”, que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando éstas todavía eran analógicas.

1.2.2.10.5 Spammers

Los spammers son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa realizados a través de Internet (los famosos casos de “phishing”).

1.2.2.10.6 Piratas Informáticos

Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

1.2.2.10.7 Creadores de virus y programas dañinos

Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.

En estos últimos años, además, han refinado sus técnicas para desarrollar virus con una clara actividad delictiva, ya que los utilizan para obtener datos sensibles de sus víctimas (como los números de cuentas bancarias y de las tarjetas de crédito, por ejemplo) que posteriormente emplearán para cometer estafas y operaciones fraudulentas.

1.2.2.10.8 Lamers (“wannabes”) “Script-kiddies” o “Click-kiddies”

Los “lamers”, también conocidos por “script kiddies” o “click kiddies”, son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan.

A pesar de sus limitados conocimientos, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de Internet, y que pueden ser utilizadas por personas sin conocimientos técnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

1.2.2.10.9 Amenazas del personal interno

También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como “fisgones” en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización.

Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno (“insiders”) como con los usuarios externos del sistema informático (“outsiders”).

1.2.2.10.10 Ex-empleados

Los ex-empleados pueden actuar contra su antigua empresa u organización por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no

han sido canceladas en los equipos y servidores de la organización. También pueden provocar la activación de "bombas lógicas" para causar determinados daños en el sistema informático (eliminación de ficheros, envío de información confidencial a terceros…) como venganza tras un despido.

1.2.2.10.11 Intrusos remunerados

Los intrusos remunerados son expertos informáticos contratados por un tercero para la sustracción de información confidencial, llevar a cabo sabotajes informáticos contra una determinada organización, etcétera.

1.2.2.11 Mecanismos de Prevención

1.2.2.11.1 Cortafuegos

En inglés se le denomina (Firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

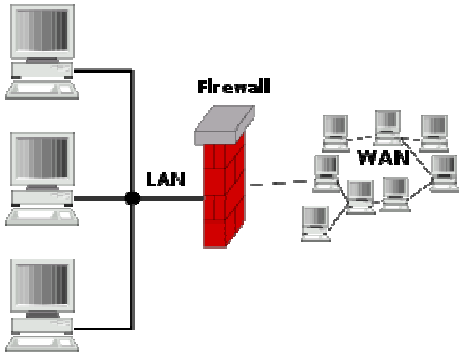


Fig. 7: Firewall

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos.

Firewall basado en Hardware: son máquinas endurecidas, optimizadas y diseñadas para realizar trabajos exclusivos de Firewall, especialmente de filtrado de paquetes. Brindan grandes ventajas:

- Sistema operativo desarrollado y concebido para mitigar ataques.
- Mayor desempeño en comparación con los firewalls basados en software.
- Menor tiempo de implementación que los firewalls basados en software.
- Reducen necesidad de decidir entre hardware, sistema operativo y software de filtrado, ya que todo viene configurado, simplificado y optimizado en un solo paquete.

Algunos Firewall de este tipo utilizados en las medianas y grandes empresas son: Cisco PIX (Private Internet Exchange) que ahora ha sido cambiado por CISCO ASA con la serie 5500, Juniper NetScreen, SonicWall, Checkpoint, Astaro.

Firewall basado en software: Constituyen una alternativa más económica en relación que los firewall basados en hardware, pero presentan mayores desafíos en su implementación: debe seleccionarse adecuadamente la plataforma de hardware y endurecer el sistema operativo, debido a que sistemas Windows o Linux no son optimizados (por defecto) para uso para realizar reenvío de paquetes (forwarding), además corren por defecto servicios que no son requeridos si la máquina funciona como firewall exclusivamente. En conclusión presentan un mayor desafío en su configuración.

Algunos Firewall de este tipo utilizados en las medianas y grandes empresas son: Checkpoint (Virtualizado), IPTables (Linux), Microsoft Internet Security & Aceleration Server, Untangle, SmoothWall, Engarde Secure Linux, mOnOwall.

Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego a una tercera red, llamada *Zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

1.2.2.11.2 Políticas de Seguridad Informática

Además de la seguridad que se pueda implementar al borde de una intranet, se deben establecer reglas o normas que garanticen la seguridad de la información y la integridad física del recurso informático de la organización. Con esto entonces se trata de implementar estas normas en el Data Center de la UNL desde donde se manejará toda la información de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus labores. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

1.2.2.11.2.1 Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la Universidad

(Docentes, Administrativos, Trabajadores y Estudiantes) para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una

comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la Universidad, etc.

1.2.2.11.3 Antivirus y Antispyware

También llamado en Ingles (antimalwares), es un programa cuyo objetivo es detectar y eliminar virus informático. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de *malware*, como *spyware*, *rootkits*, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como la heurística.

Usualmente, un antivirus tiene uno o varios componente residentes en memoria que se encargan de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demanda (los conocidos *scanners*, exploradores, etc.) y módulos de protección de correo electrónico, Internet, etc.

El objetivo primordial de cualquier antivirus actual es detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

Antispyware, es un programa espía que se instala furtivamente en un computador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar

a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a la red

Entre la información usualmente recabada por este software se encuentran: los mensajes, contactos y la clave del correo electrónico; datos sobre la conexión a Internet, como la dirección IP, el DNS, el teléfono y el país; direcciones web visitadas, tiempo durante el cual el usuario se mantiene en dichas web y número de veces que el usuario visita cada web; software que se encuentra instalado; descargas realizadas; y cualquier tipo de información intercambiada, como por ejemplo en formularios, con sitios web, incluyendo números de tarjeta de crédito y cuentas de banco, contraseñas, etc.

Un Data Center debería poseer un buen antivirus para evitar que correos electrónicos ingresen a la red interna de la organización como spyware y utilizar un firewall con antivirus para darles seguridad a sus usuarios.

1.2.2.11.4 Zona Desmilitarizada DMZ

Es otro de los mecanismos de prevención de ataques el cual consiste en una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que

las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

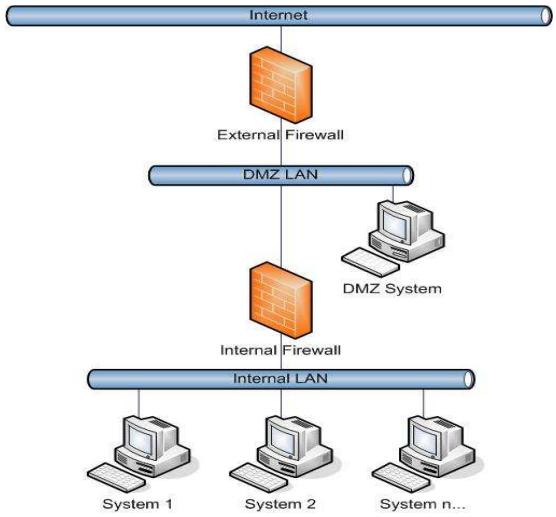


Fig. 8: Zona Desmilitarizada

Habitualmente una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a

la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna.

1.2.2.11.5 AAA (Autenticación, Autorización y Auditoría)

En seguridad informática, el acrónimo **AAA** corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización o Auditoría (Authentication, Authorization and Accounting). La expresión *protocolo AAA* no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Autenticación.- Es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplo de esta credencial son las contraseñas.

Autorización.- se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las

veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Auditoría.- se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos.

Algunos protocolos que utilizan AAA son: RADIUS (***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****erver*), DIAMETER, TACACS (***T****erminal* ***A****ccess* ***C****ontroller* ***A****ccess* ***C****ontrol* ***S****ystem*), TACACS+

1.2.2.11.6 ACLs (Lista de Control de Acceso)

Es otro mecanismo de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.
Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

En redes informáticas, **ACL** se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes)

que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto servidores individuales como enrutadores pueden tener ACLs de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un cortafuego.

Existen dos tipos de ACLs:

- ACL estándar, donde solo tenemos que especificar una dirección de origen.
- ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.

1.2.2.11.7 VLANs (Red de Área Local Virtual)

Es importante considerar a las VLANs como parte de la seguridad informática comúnmente utilizada para ayudar en la administración de la red de una organización.

Es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3 y 4).

Una ***VLAN*** consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

Hasta aquí ya hemos hablado de que se aísla el trafico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etcétera.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente

Clases de VLANs

Como respuesta a los problemas generados en redes LAN (colisiones, trafico broadcast, movilidad, etc) se creó una red

con agrupamientos lógicos independientes del nivel físico, con lo cual si un usuario se encontraba en el piso uno y debía moverse al piso dos ya no tenía que reconfigurar la maquina ni darle una nueva dirección IP (Internet Protocol; Protocolo de Internet) del piso dos, sino que ahora era una acción automática.

Las VLAN forman grupos lógicos para definir los dominios de broadcast. De esta forma existe el dominio de los rojos, donde el broadcast que genera el rojo solo le afectara a este color y el broadcast que genera el amarillo solamente afectara a esta parte de la red.

Aunque físicamente estén conectadas las maquinas al mismo equipo, lógicamente pertenecerán a una VLAN distinta dependiendo de sus aplicaciones con lo que se logra un esquema más enfocado al negocio.

Anteriormente existía la red plana, donde el broadcast se repetía en los puertos y esto provocaba una situación crítica. Ahora con las VLAN existe una segmentación lógica o virtual.

Existen dos clases de VLAN: ***implícitas y explícitas***. Las **implícitas** no necesitan cambios en el frame, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos. En esta clase de VLAN el usuario no modifica ni manipula el frame, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario.

Las VLAN **explícitas** si requieren modificaciones, adiciones y cambios (MAC) al frame, por lo que sacaron los estándares 802.1p y 802.1q, en donde se colocan ciertas etiquetas o banderas en el frame para manipularlo.

Las VLAN deben ser rápidas, basadas en switchs para que sean interoperables totalmente, porque los routers no dan la

velocidad requerida, su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.

Generaciones de VLANs

1. Basadas en puertos y direcciones MAC
2. Internet Working; se apoya en protocolo y dirección capa tres.
3. De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.
4. Servicios avanzados: ya se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host Configuration Protocol ; Protocolo de configuración dinámica) o por AVLAN (Authenticate Virtual Local Area Networks; Redes virtuales autenticadas de área local).

VLAN por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN - , el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla, el servidor estará en la VLAN amarilla.

VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación.
Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

VLAN por Protocolo

Lo que pertenezca a IP se enrutara a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectará automáticamente a la VLAN correspondiente.

VLAN por subredes de IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario aunque esté conectado a la VLAN del protocolo IP sea asignado en otra VLAN subred que pertenecerá al grupo 10 o 20 dentro del protocolo.

VLAN definidas por el usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario protocolo, dirección MAC y puerto.
Si el usuario manifiesta otro patrón de bits, entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente. También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

1.2.2.11.8 Seguridad de Puertos

1.2.2.11.8.1 ARP (Address Resolution Protocol)

Es un protocolo utilizado como parte de la seguridad informática, responsable de encontrar la dirección MAC que corresponde a una determinada dirección IP.

Para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya. Si alguno de ellos se identifica con esta dirección, el equipo responderá al ARP, que almacenará el par de direcciones en la tabla de búsqueda, y, a continuación, podrá establecerse la comunicación.

1.2.2.11.8.2 ARP estática

Son utilizadas para mitigar el riesgo de un ataque ARP Spoofing (definido anteriormente). El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica sólo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer Router. Una

manera de protegerse de esta técnica es mediante tablas ARP estáticas (simpre que las ips de red sean fijas), lo cual puede ser difícil en redes grandes. Para convertir una tabla ARP estática se tendría que ejecutar el comando:

arp -s [IP] [MAC]

1.2.2.11.8.3 RADIUS (Remove Authentication Dial In User Service)

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP[8] mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) *sobre el protocolo PPP*[9]*, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor* RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, ancho de banda, acceso a páginas limitadas y otros parámetros.

[8] Proveedor de Servicios de Internet
[9] Protocolo punto a punto

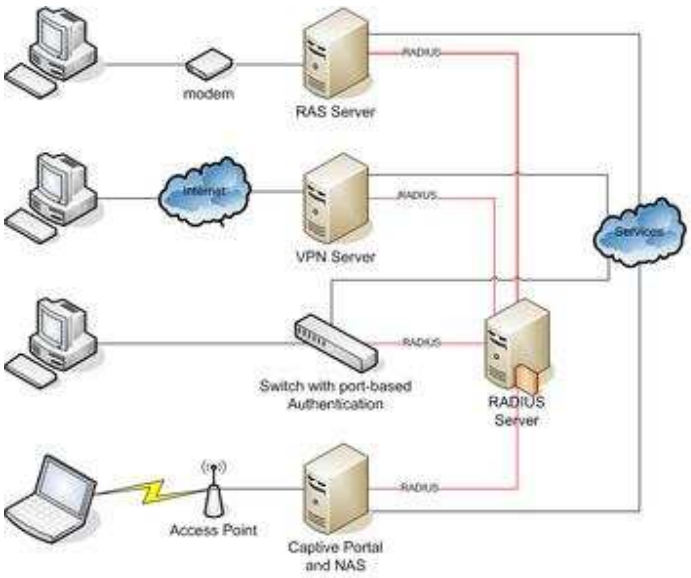


Fig. 9: Servidor RADIUS

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

1.2.2.11.8.4 VPN (Red Privada Virtual)

Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la **autenticación**, **integridad**, **confidencialidad** y **no repudio** de toda la comunicación. Para la autenticación y autorización se utiliza funciones de Hash. Los algoritmos de hash más

comunes son los Message Digest (MD2[10]y MD5[11]) y el Secure Hash Algorithm (SHA[12]). Para la confidencialidad, dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES[13]), Triple DES (3DES[14]) y Advanced Encryption Standard (AES[15]).

Es una forma de comunicación segura cuando se quiere enlazar a una red interna de una organización desde algún lugar en específico fuera de las instalaciones de la institución puede ser desde: casa, desde otra empresa o desde alguna sucursal de la organización. Pueden existir tres opciones para poder realizar estas conexiones:

- **A través de Modem**: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada local, nacional o internacional, a parte no contaría con la calidad y velocidad adecuadas.
- **A través de Línea Privada:** Tendría que tender la UNL su propio cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por

[10] MD2 (Algoritmo de Resumen del Mensaje 2)
[11] MD5 (Algoritmo de Resumen del Mensaje 5)
[12] SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro)
[13] DES (Data Encryption Standard)
[14] 3DES. Hace triple cifrado del DES
[15] AES (Advanced Encryption Standard)

ejemplo necesito enlazar la oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso y eso no le conviene a la Universidad.

- **A través de VPN:** Los costos son bajos porque se paga la utilización del internet de la organización no hay un costo aparte, además de tener la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Ventajas de las VPN:

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
- Se utiliza más en campus de universidades.

Tipos de Conexión:

Conexión de Acceso Remoto: Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN Router a Router: Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers.

El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión Firewall a Firewall: Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

1.2.2.11.8.5 Certificados y Firmas Digitales

Un **Certificado digital** es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Si bien existen variados formatos para **certificados digitales**, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El **certificado** contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

La Autoridad Certificadora en nuestro país es el Banco Central del Ecuador.

La **Firma digital** hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

Las firmas digitales son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave pública; son utilizadas principalmente para verificar la autenticidad del mensaje o la de una llave pública.

Una firma digital, la cual no debe ser confundida con un certificado digital, es una firma electrónica que puede ser utilizada para autenticar la identidad del emisor de un mensaje. Una firma digital es usualmente generada desde un certificado digital usando una tecnología de llave pública y privada, además el certificado digital tiene que llevar la firma

de la autoridad certificadora, que en nuestro país es el Banco Central del Ecuador quién autoriza la creación de una Autoridad de Certificación.

FASE 2: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

2.1 EVALUACION DE LA SITUACIÓN ACTUAL DE LA RED: APLICABILIDAD, USO Y TECNOLOGIA DE LA UNIVERSIDAD NACIONAL DE LOJA

2.1.1 Análisis de la Situación Actual

La Universidad Nacional de Loja, se encuentra ubicada al sur de la ciudad de Loja en el sector “La Argelia” ciudadela Universitaria. Esta Institución está formada por cinco Áreas Académico – Administrativas y un Área Administrativa, las cuales 4 áreas Académico - Administrativas y 1 Administrativa se encuentran localizadas en un mismo sector y 1 Área Académico - Administrativa se encuentra ubicada tras del Hospital “Isidro Ayora” en el centro de la ciudad.

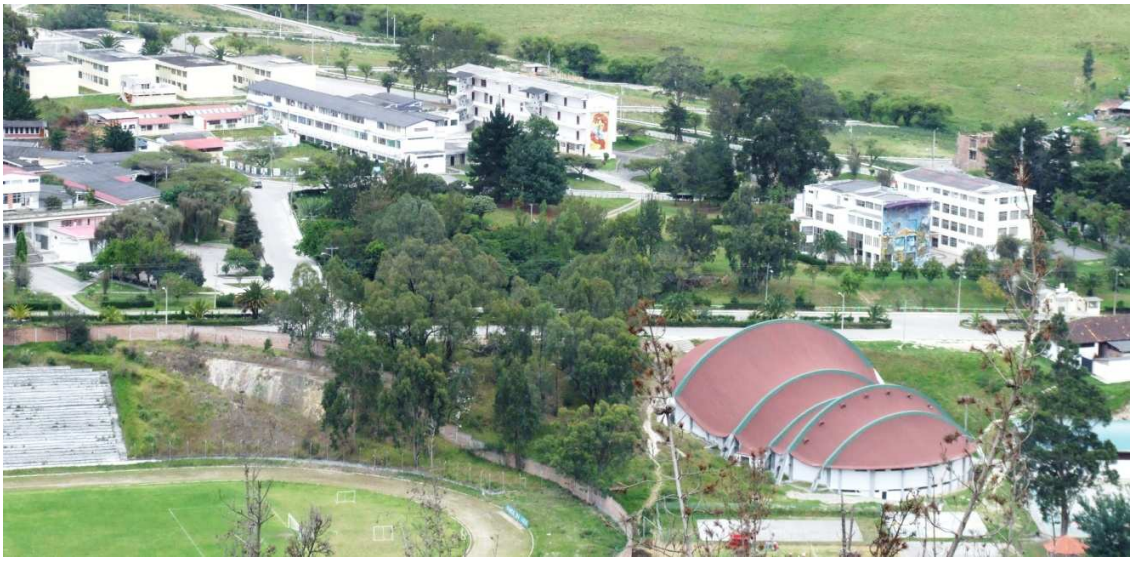


Fig. 10: Campus Universitario (UNL)

Las **Áreas Académico – Administrativas** son: Área Jurídica, Social y Administrativa, Área Agropecuaria y de Recursos Naturales Renovables, Área de la Educación el Arte y la Comunicación, Área de Energía las Industrias y Recursos Naturales no Renovables, Área de la Salud Humana y el **Área Administrativa** que es: Administración Central.

A continuación se presenta el orgánico estructural de la Universidad Nacional de Loja, resaltando la ubicación del departamento de Informática.

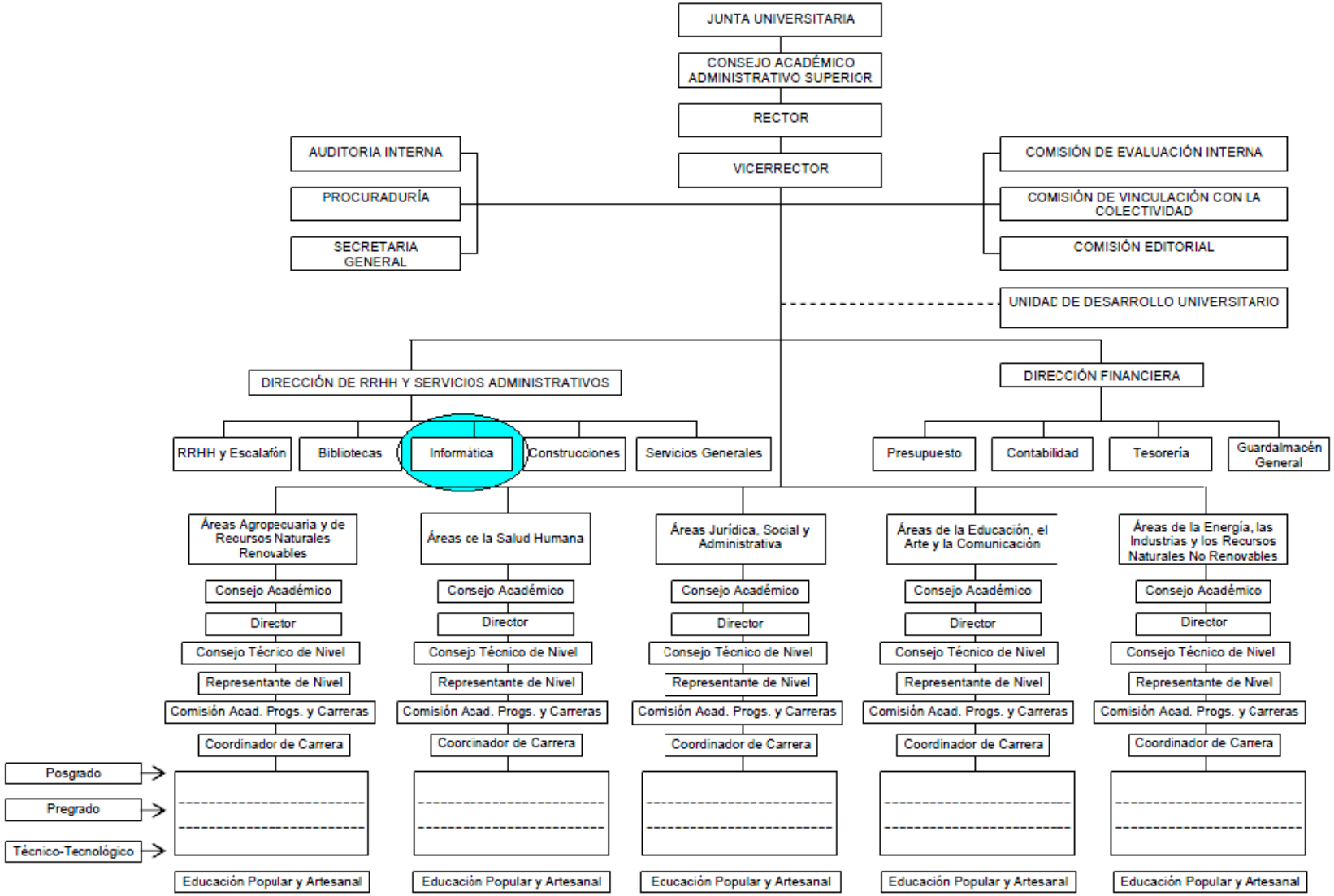


Fig. 11: Orgánico Estructural (UNL)

El Departamento denominado Jefatura de Informática se encuentra en el orgánico estructural como parte de la Dirección de RRHH y Servicios Administrativos y físicamente está ubicado en el edificio de Administración Central, es el ente autorizado de la administración y gestión de la red. Se encarga de la instalación de software, actualizaciones de antivirus, administración de las claves de configuración de equipos de red y de computación, tanto para el sector administrativo como académico de toda la Universidad, excepto al Área de Energía, las Industrias y recursos Naturales No Renovables donde la Carrera de Ingeniería en Sistemas realiza estas tareas.

La Universidad Nacional de Loja, actualmente no posee un Data Center con una infraestructura adecuada para manejar toda la información de la institución, sino más bien existe un cuarto de equipos de red que no ofrece las garantías necesarias para manejar toda la información de la Universidad, este cuarto que se encuentra ubicado en la sección de Redes del Departamento de Jefatura de Informática, desde este departamento se administra y distribuye el internet hacia las demás Áreas; mientras que en el resto de áreas los equipos de red se localizan en los denominados *puntos de distribución (Centros de Computo),* que son sectores de trabajo no apropiados para el alojamiento de equipos, ya que no cuentan con la infraestructura adecuada (ambientes de acceso restringidos, control de temperatura, etc.).

Actualmente se tiene un proyecto denominado “Construcción del Instituto de Informática” el mismo que estará diseñado para el alojamiento de todo el equipo necesario y la infraestructura

adecuada para el manejo de la información de la institución. Se tiene previsto que en este edifico donde funcionará la entidad se manejen 2 pisos de laboratorios de capacitación y en el último piso (3ro) se maneje toda la parte informática de la Universidad, que estaría a cargo de la Unidad de Telecomunicaciones e Información, la misma que manejara algunas líneas de acción como: Soporte Técnico, Desarrollo de Software, Redes y Telecomunicaciones.

2.1.1.1 Análisis de los resultados obtenidos en las encuestas y entrevistas realizadas a los responsables de los Centros de Cómputo de la Universidad Nacional de Loja.

Se desarrollaron entrevistas y encuestas a los encargados de los centros de cómputo de cada una de las áreas que forman parte de la UNL con el objetivo de conocer sobre la situación actual del equipamiento tecnológico y en cuanto al conocimiento sobre seguridad informática y sobre la necesidad de manejar toda la información desde un Data Center.

Este tipo de técnica me permitió conocer a fondo sobre la situación tecnológica de la UNL por lo que para este proyecto es la base fundamental para definir lo que falta en el equipamiento que sirva para mejorar la seguridad lógica de la red de datos que se manejará desde el Data Center. Además conocer los criterios de algunos profesionales sobre posibles mecanismos de seguridad a implementarse.

Para mayor detalle en el **Anexo 1**, se encuentra el análisis realizado de los resultados obtenidos al aplicar estas técnicas.

Según los resultados obtenidos en las encuestas y entrevistas realizadas, me puedo dar cuenta que existen algunos problemas en cuanto a seguridad informática se refiere, que ha sufrido la Universidad Nacional de Loja en estos últimos años, los mismos que los presento a continuación:

1. No existe presupuesto de la institución comprometido con la seguridad informática.
2. Se han producido accesos no autorizados a la red de la institución en algunos casos detectados en la misma intranet, pocos son detectados de la extranet.
3. Problemas con Virus (Spam, Gusanos, Troyanos, etc)
4. Se ha detectado Robo de Datos al acceder a los servidores de la institución.
5. Se realiza Monitoreo no autorizado del tráfico de la red utilizando programas que pueden causar daños en la red (esto es por usuarios de la misma red).
6. Problemas de ataques de Denegación de Servicios.
7. Se han producido Ataques a la Página Web de la Institución causando graves daños en la modificación de contenido.
8. Robo de direcciones IP para la navegación por internet (problemas de duplicación de IP o de nombre de Usuario).
9. Problemas de suplantación de direcciones MAC para el acceso a la red de datos.

2.1.1.2 Análisis de la Tecnología existente (hardware y software) en la Universidad Nacional de Loja.

El presente punto tiene como finalidad conocer la situación actual en cuanto a software y hardware que maneja la UNL,

para luego realizar un análisis y poder recomendar que equipos servirían para brindar la seguridad informática en el Data Center y poder seguir manteniéndolos.

La Universidad Nacional de Loja, posee una red de datos interna, que permite la comunicación entre usuarios de la red. La red tiene como punto central la Jefatura de Informática ubicada en el cuarto piso del segundo bloque de Administración Central, ésta se distribuye para las cinco Áreas Académicas - Administrativas, Departamento de Bienestar Estudiantil, CINFA[16] y Federación de Estudiantes Universitarios de Loja (FEUE).

El backbone está constituido por una serie de puntos conectados a través de enlaces punto a punto, con antenas de elevadas ganancias y equipos confiables que permiten asegurar la disponibilidad de la red. La cobertura hacia los usuarios se proporciona mediante enlaces punto bajo estándar 802.11g.

El Internet llega a la Universidad a través de fibra óptica, la empresa encargada de brindar este servicio es TELCONET. El ancho de banda que posee la Universidad para los usuarios es de 31,14 mbp/s y 450 mbp/s para Internet comercial.

Para facilitar la comprensión de los esquemas y diagramas de redes mostrados a continuación es necesario emplear la siguiente simbología.

[16] CINFA: Centro de Informática Agropecuaria

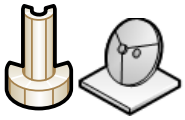
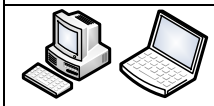
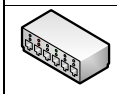
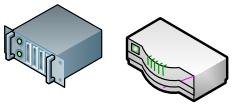
SÍMBOLO	DESCRIPCIÓN
	**Antenas**
	**Cable UTP**
	**Patch Panel de fibra**
	**Convertidores Fibra a UTP "Transceiver"**
	**Fibra Óptica**
	**Patch de Fibra Óptica**
	**PC Personales**
	**Radios**
	**Servidores**
	**Switch**
	**Torres**
	**Router**
	**Firewall**
	**Enlace inalámbrico**

Tabla 1: Simbología de Redes

2.1.1.2.1 Topología Física del Backbone y sus Puntos de Acceso

En la Fig. 12 se muestra la interconexión entre las áreas, haciendo notar que todo sale desde la jefatura de informática en Administración Central y todas las áreas están interconectadas a través de fibra óptica a excepción del área de la salud que se conecta a través de un radio Motorola Canopy, también se maneja en 2 áreas la parte de redundancia a través de enlaces inalámbricos, pero como no se lo tiene como política establecida a la redundancia ni de conexión ni de datos entonces no funcionan todo el tiempo y tampoco se comprueba su funcionalidad.

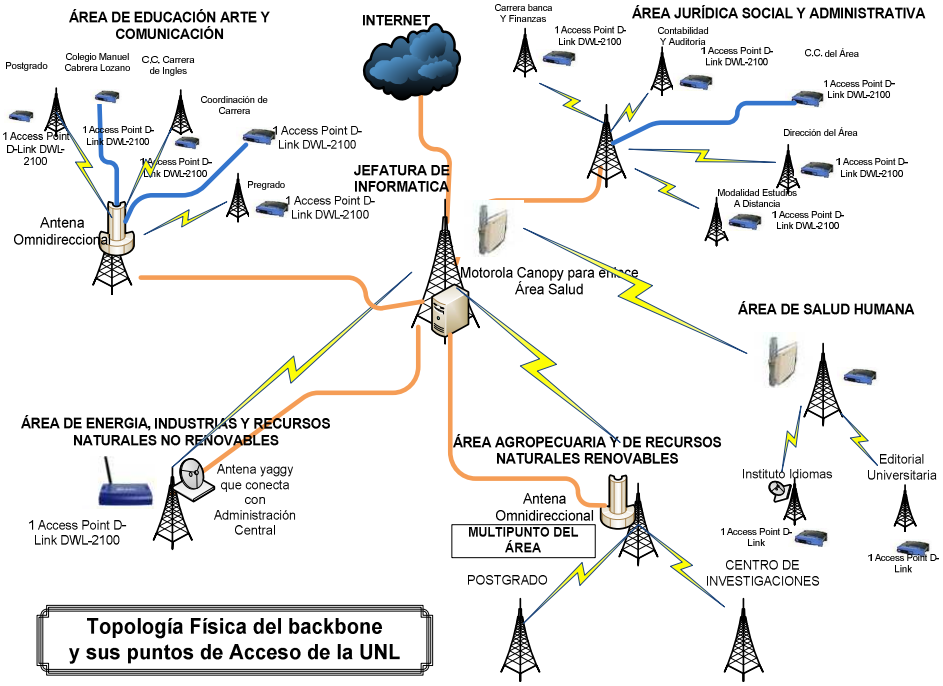


Fig. 12: Topología Física del Backbone y sus Puntos de Acceso

2.1.1.2.2 Topología Lógica del Backbone y sus Puntos de Acceso

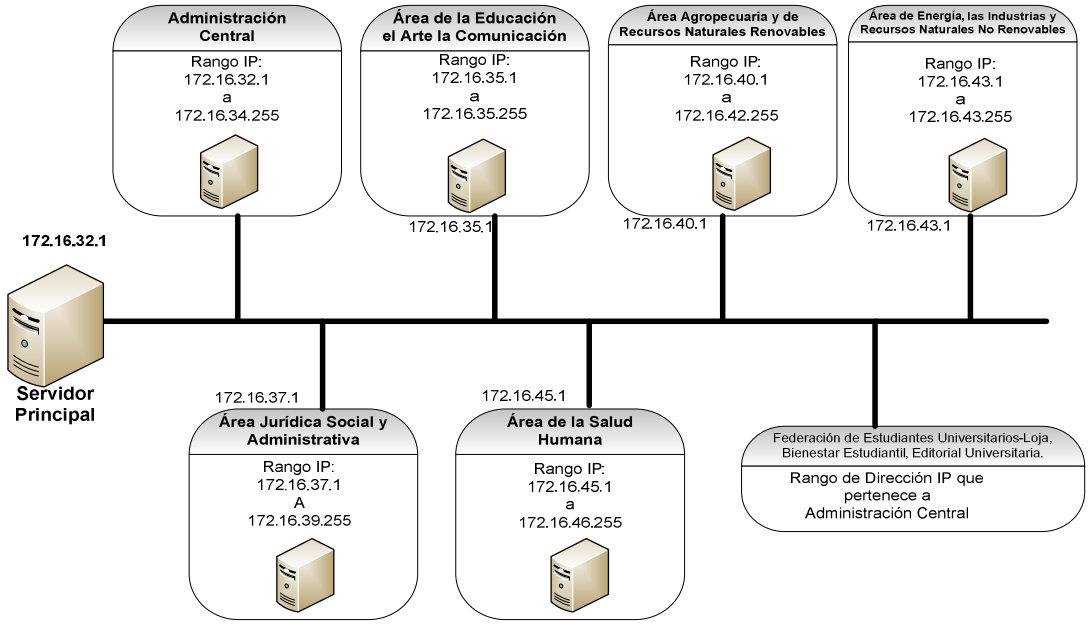


Fig. 13: Topología Lógica del Backbone y sus Puntos de Acceso

Desde el punto de vista lógico el backbone de la red se encuentra operando bajo protocolo TCP/IP con una asignación formal de red clase B (172.16.32.1) con uso de máscara del tipo clase B (255.255.240.0), cada área posee un servidor proxy por donde puede salir a la conexión a internet. El Backbone de esta forma, es un segmento de red Ethernet trabajando en forma conmutada.

2.1.1.2.3 Distribución tecnológica en la intranet de la UNL

2.1.1.2.3.1 Administración Central

En la Administración Central funciona en el último piso la Jefatura de informática, la cual está encargada del manejo de la información en toda la organización y en ese lugar es en donde funciona el Data Center de la UNL, sin ninguna consideración técnica sobre la infraestructura adecuada para el funcionamiento de tan importante departamento de la institución, en el **Anexo 2** de este documento se puede observar a detalle algunas fotografías que dan fe del estado actual del Centro de Datos.

Como pudieron observar no se cuenta con la infraestructura física adecuada para el funcionamiento del Centro de Datos por lo que entre algunos de los problemas están los siguientes:

- Falta de un estudio adecuado de las cargas eléctricas para la protección de los equipos de las caídas de voltaje.
- Falta de un sistema de backup de energía para el todo el Data Center.
- Falta de un adecuado sistema de enfriamiento para todo el Data Center.
- Falta de un adecuado sistema de cableado estructurado para el flujo de la información.
- Falta de sistemas de seguridad física para el ingreso al Data Center.

- Falta de equipamiento adecuado para la ubicación de servidores y fuentes de poder tipo Rack.
- Falta de políticas de seguridad en el acceso del personal.

En el caso de este trabajo de Postgrado no es parte de los objetivos centrarnos en la seguridad física del Data Center, por lo que no toparemos mucho esos temas, pero si es necesario conocer como parte de la situación actual el cómo se encuentra la infraestructura física y recomendar que se necesita que las autoridades de la institución se comprometan a realizar un cambio en equipos y mejorar la infraestructura donde se manejará el recurso más importante de una organización que es la Información.

Los principales equipos y servidores que se encuentran en esta Jefatura de Informática ubicada en la Administración Central de la Universidad Nacional de Loja, se detallan a continuación:

- **Equipos:**

  - Router Cisco, permite la interconexión con Internet comercial e Internet 2. El manejo de este equipo es de uso exclusivo del proveedor de Internet para la Universidad (TELCONET).
  - Un Switch Cisco 2960, que se encuentra conectado a la interfaz LAN del Router. Los servidores que se conectan a este Switch son:

- Firewall,
- Servidor WEB
- Servidor Moodle (Educación Virtual a Distancia)
- Servidor para la Radio Universitaria
- Servidor DNS

- Switch Cisco 2960, conectado al Firewall. Los equipos conectados a este switch son:

  - Servidor de Correos
  - Servidor de Control de Contenido
  - Servidor Financiero
  - Servidor DHCP[17]
  - Switch 3com, desde este equipo se conecta la administración central
  - Se realiza la interconexión con las Áreas Académicas Administrativas. Los equipos conectados a este dispositivo son:

    - Transceiver mc102xl Fast Ethernet media converter, realiza la conexión con el Área Agropecuaria y de Recursos Naturales Renovables por medio de fibra óptica
    - Transceiver D-link def-855, permite la conexión con el Área de la Educación el Arte y la Comunicación por medio de fibra óptica.

[17] Protocolo de Configuración de Host Dinámico: permite que un equipo conectado a una red pueda obtener su configuración

- Transceiver D-link def-855, permite la conexión con el Área Jurídica, Social y Administrativa por medio de fibra óptica.
- Radio Cannopy que permite tener comunicación inalámbrica con el Área de la Salud Humana.
- Transceiver D-link, permite la conexión con el Área de Energía las Industrias y los Recursos Naturales No Renovables por medio de un par de hilos de cobre.
- Modem Cisco 673, permite la conexión con la FEUE.

➢ Servidores

- Firewall, servidor que permite tener la barrera entre la red pública y la red privada de datos, aquí constan las reglas que optimizan el uso del Internet en la Universidad Nacional de Loja. Las características del Firewall son:

  - Sistema Operativo Linux Fedora 3
  - Intel(R) Xeon (TM) CPU 3.2GHz
  - Memoria 1GB
  - Disco 160 GB

- Servidor WEB, aquí se encuentra instalada la página web de la Universidad. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 3
  - Intel(R) Xeon (TM) CPU 3.2GHz

- Memoria 1GB
- Disco 160 GB

- Servidor Moodle. Utilizado para brindar educación a distancia vía internet. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 3
  - Intel(R) Xeon (TM) CPU 3.2GHz
  - Memoria 1Gb
  - Disco 160 GB

- Servidor de Correo. Este servidor permite tener direcciones de correo electrónico bajo el dominio de la Universidad, por ejemplo informatica@unl.edu.ec. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 3
  - Intel(R) Xeon (TM) CPU 3.2GHz
  - Memoria 1GB
  - Disco 160 GB

- Servidor DHCP, permite asignar dinámicamente direcciones de red a los computadores de la Universidad, por medio de la MAC de la interfaz de red. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 6
  - Intel(R) Pentium (r) D CPU 3.4GHz
  - Memoria 1GB

- Disco 160GB

- Servidor para Control de Contenido, hace posible el control efectivo en el acceso a páginas pornográficas y de contenido malicioso principalmente, así como evita un consumo excesivo de ancho de banda. Para este propósito se utiliza Squid y Dansguardian, software que permite realizar el control en cada uno de los servidores de las Áreas. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 3
  - Intel(R) Xeon (TM) CPU 3.2GHz
  - Memoria 1Gb
  - Disco 160 GB

- Servidor Financiero, posee el sistema contable Visual FOX. Las características se describen a continuación:

  - Sistema Operativo Windows 2003 Server
  - Intel(R) Xeon (TM) CPU 3.2GHz
  - Memoria 1GB
  - Disco 160 GB

- Servidor para la Radio Universitaria, replica la señal de “Radio Universitaria”, a través de Internet. Las características se describen a continuación:

  - Sistema Operativo Linux Fedora 6
  - Intel(R) Pentium (r) D CPU 3.4GHz

- Memoria 1GB
- Disco 160GB.

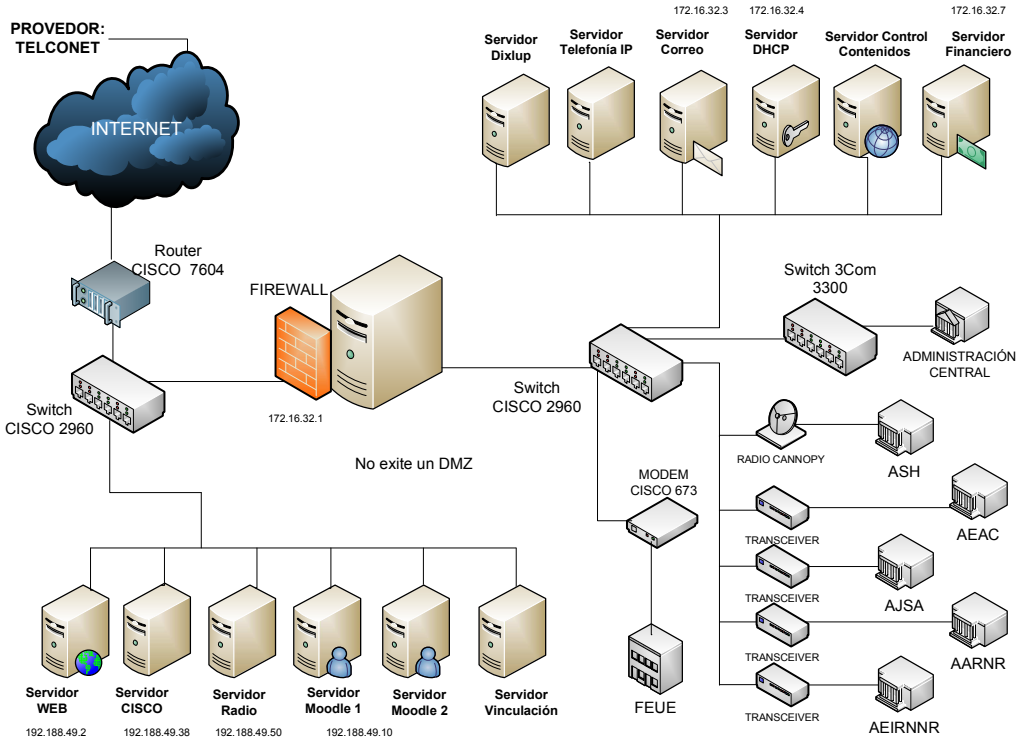


Fig. 14: Equipos y Servidores Principales de la Red de Datos

En el diseño de red de la Fig. 14 podemos darnos cuenta que existen algunas limitaciones en cuanto a seguridades lógicas, las cuales describo algunas a continuación:

- Se maneja un solo Firewall (a nivel de Software) para la seguridad en la intranet de los posibles daños que se puedan sucintar por la extranet.
- No se posee una Zona Desmilitarizada por lo que los servidores que se encuentran con direcciones públicas están expuestos a cualquier tipo de ataques desde la red.

- No se maneja políticas de redundancia en algunos casos por lo que la información siempre está en peligro de perderse.
- No se maneja un protocolo de Autenticación a través de RADIUS para el control de los usuarios que se conectan a la intranet.
- No se utilizan VLANs para la segmentación de las redes y de esa manera asignar privilegios.
- No se utilizan Listas de Control de Acceso.
- No se manejan políticas de seguridad por lo que ni siquiera existe un manual de esas políticas.

Estas son algunas de entre las muchas cosas que faltan para poder brindar seguridad lógica a la red de la UNL, pero considero que esas son las básicas en toda organización.

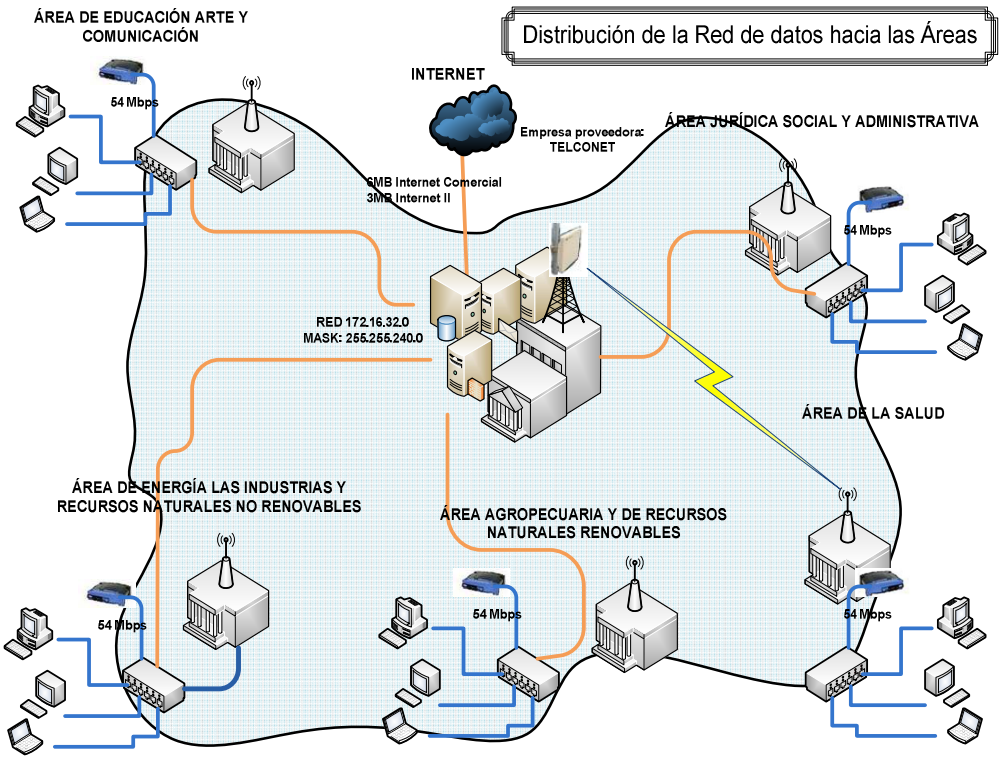


Fig. 15: Distribución de la Red hacia las Áreas

2.1.1.2.3.2 Área Agropecuaria y Recursos Naturales Renovables

La interconexión con el Área es por intermedio de fibra óptica. Los principales equipos que se encuentran en ésta son:

- Una caja multimedia donde llega la fibra óptica.
- Un transceiver D-link def-855 conectado al Patch Panel de Fibra y conectado al Switch 3COM
- Un Switch 3COM que conecta con el servidor del Área.
- Un Switch D-link (Switch Principal) conectado al Switch 3COM
- Un Servidor que tiene instalado: Squid y Dansguardian para el control de contenido del internet a los usuarios del Área. Las características del servidor son:
  - Sistema Operativo Linux Fedora 6
  - Intel(R) Pentium (r) 4 3.0GHz
  - Memoria 512Mb
  - Disco 160 GB
- Un transceiver D-link def-855 enlazado al Switch Principal, el mismo permite conectar por medio de fibra óptica a otras dependencias del Área.

- Una antena omnidireccional D-Link que permite conectar inalámbricamente con el nivel de Postgrado del Área de esta dependencia y con el Centro de Investigación del Área.

El Centro de Cómputo de Ingles que funciona en el área cuenta con los siguientes dispositivos:

- 2 Switch 24 puertos D-Link DES-1024 D 10/100 Fast Ethernet
- 2 Organizadores
- 2 Patch Panel 24 puertos Cat 5e System
- 2 Access Point D-Link DWL-2100

El Centro de Computo del Área Agropecuaria y de Recursos Naturales Renovables se encuentra a cargo de Ing. Ramiro Vásquez.

- **CINFA**

Al CINFA se llega por medio de una conexión de cable utp cat 5e, que parte desde el Switch 3COM al Switch del departamento; desde el cual existe la distribución para los host, posee los siguientes equipos:

- 2 Patch Panel de 24 puertos Quest Cat 5e
- 2 Switch de 12 puertos/cu D-Link DES-1024 D 10/100 Fast Ethernet
- 2 Organizadores

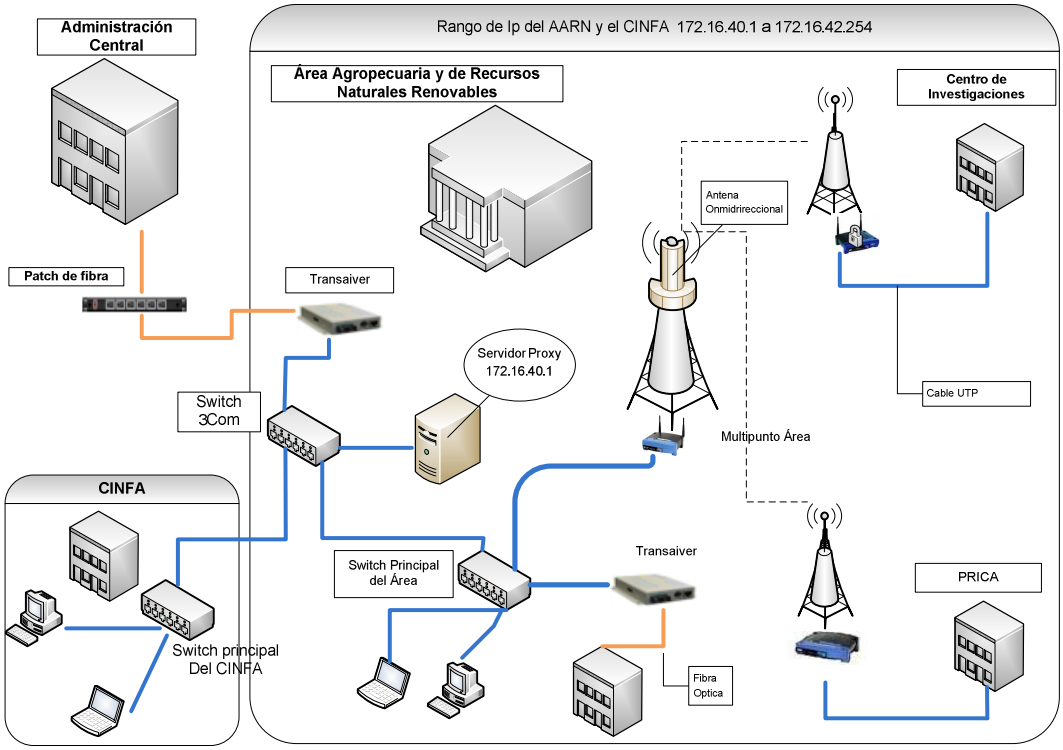


Fig. 16: Red de Datos Área Agropecuaria y de Recursos Naturales Renovables

2.1.1.2.3.3 Área de Energía, Industrias y Recursos Naturales no Renovables

Se parte del Patch Panel de fibra, ubicada en la Jefatura de Informática, propia para el área, de 8 Hilos de los cuales están conectados 4 en multimodo, se encuentra conectado un Transceiver D-LINK DMC 700SC. A esta área se llega por medio de fibra óptica tendido por postes. La fibra se conecta al Patch Panel de fibra del Área y a su vez a su convertidor Transceiver D-LINK DMC 700SC para salir luego a Switch 3COM 10/100/1000 Mbps.

Bloque 1:

Los equipos que posee el AEIRNNR son:

- 1 Switch 3Com 3C16476 Super Star Base Line 10/100/1000 Base T Capa 2 de 50 puertos, conectado al Transceiver y al servidor
- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Transceiver D-Link DMC 700 SC convertidor de fibra óptica a cable utp
- 1 Patch Panel RJ45 Leviton de 24 puertos
- 2 Bandejas de fibra óptica Hubbel 12 puertos cada uno
- 1 Switch D-Link DES 1016D de 16 puertos
- 2 Antenas Omnidireccionales
- 4 Antenas Yaggy
- 1 Access Point D-Link DWL-2100
- 1 Access Point D-Link DWL-2100 en la Torre de Recepción de Señal

Laboratorio 1.1

- 1 Switch Power Switch CNSH-1600 de 16 puertos

Laboratorio 1.2

- 1 Switch 3Com 3C16476 Super Star Base Line 10/100/1000 Base T Capa 2 de 49,50 puertos
- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos

- 1 Transceiver D-Link DMC 700 SC convertidor de fibra óptica a cable utp
- 1 Patch Panel RJ45 Leviton de 24 puertos
- 2 Bandejas de fibra óptica Hubbel 12 puertos cada uno
- 1 Switch D-Link DES 1016D de 16 puertos

Laboratorio 1.3

1 Switch 3Com Capa 2 3C16471 BaseLine de 24 puertos

Departamento Administrativo

- 1 Switch 3COM 3C16794 de 8 puertos

Coordinación De Postgrado

- 1 Switch D-Link DES-1008D de 8 puertos

Unidad De Desarrollo Informático Y Planificación

- 1 Switch 3Com 3CFSUO8 de 8 puertos
- 1 Switch D-Link DES-1008D de 8 puertos
- Un Servidor que tiene instalado: Squid y Dansguardian para el control de contenido del internet a los usuarios del Área. Las características del servidor son:

  - Sistema Operativo Linux Fedora 6
  - Intel(R) Pentium 4 3.2GHz
  - Memoria 1GB

- Disco 160 GB

Existen varios equipos instalados en diferentes dependencias las que a continuación se describe:

Bloque 2:
Carrera de Geología

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Coordinación Administrativa Financiera

- 1 Switch D-Link DES-1008D de 8 puertos

Boque 4:
Secretaria General del Área

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Bloque 5:

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Biblioteca del Área:

- Una caja multimedia donde llega la fibra óptica.
- 1 Transceiver D-Link def-855 conectado a la caja multimedia y al Switch D-Link
- 1 Switch 3Com capa 3 Administrable 3CR 17561-R1 de 26 puertos
- 2 Switch 3Com capa 2 3C16471B de 24 puertos
- 1 Access Point AIR-PLUS DWL -2100
- 1 bandeja de fibra óptica de 12 puertos
- 2 patch panel de 24 puertos Quest NNP-1024
- 2 Access Point D-Link DWL 3200

El Área de Energía, las Industrias y Recursos Naturales no Renovables posee un servidor Web el mismo que tiene las siguientes características:

- Sistema Operativo Linux Fedora 10
- HP ML15063
  - Dual Core Intel Xeon 5120 (1.86 Ghz, 4 MB L2 cache)
  - 1066 Mhz FSB 1.5 Gb Memoria PC2-5300 /0/6 LFFHDD
- HP SATA RAID Controller / RAID 1011) /Red Gigabit
  - /56x CD-RW /Tower/2x HD 160 GB 1.56 SATA RAID (0/1)
  - /Red Gigabit /56x CD-RW /Tower / 2 x HP 160 GB 1.56 SATA
  - 7.2K 3.5” HDD Hot Plug (349238-B21)

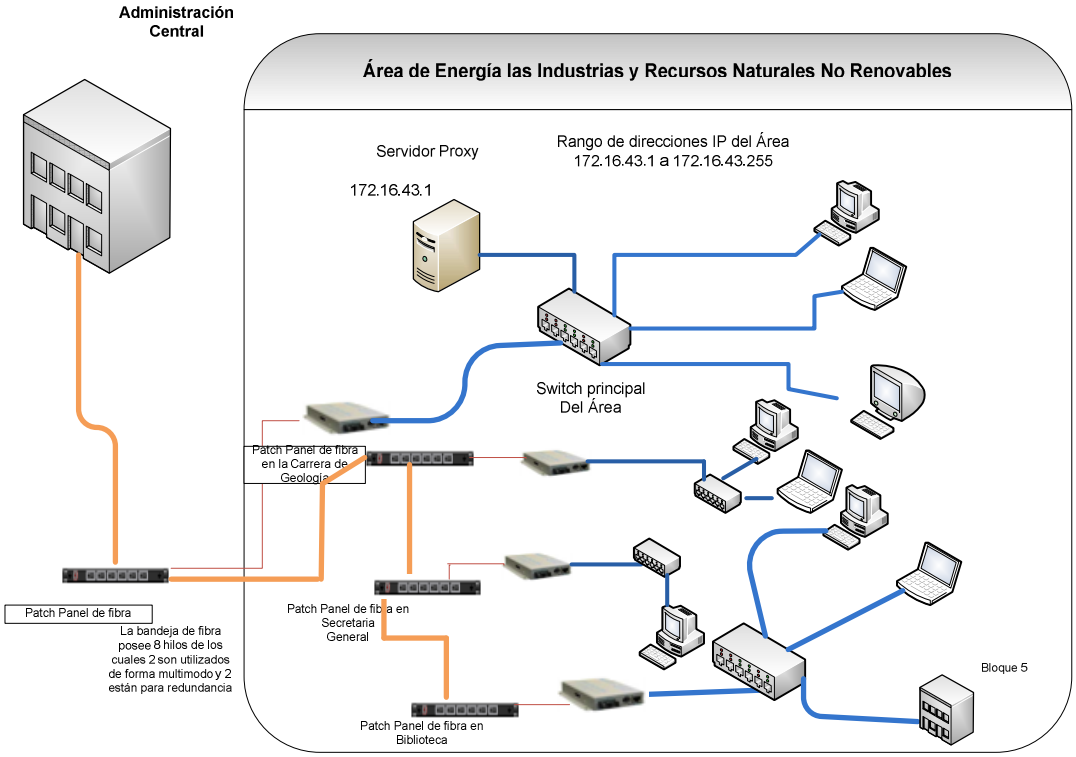


Fig. 17: Red de Datos Área de Energía las Industrias y los Recursos Naturales No Renovables

2.1.1.2.3.4 Federación de Estudiantes Universitarios

- Parte desde el Modem Cisco – 673 de la Administración Central hasta un modem Cisco - 673 que está conectado al Switch principal.
- Swicth D-Link (Switch Principal)
- Swicth D-Link, para conectar las máquinas del Cyber de la FEUE
- Conexión desde Switch Principal hasta el Comisariato Universitario.

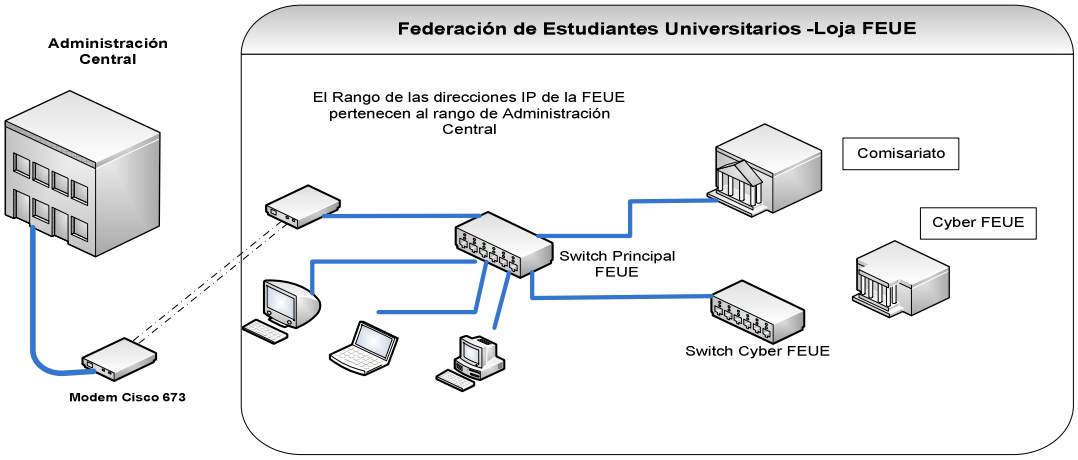


Fig. 18: Red de Datos de la Federación De Estudiantes Universitarios de Loja (FEUE)

2.1.1.2.3.5 Área de la Educación Arte y Comunicación

La interconexión con el área es por intermedio de fibra óptica. Los principales equipos que se encuentran en esta área son:

Biblioteca del Área:

- Tres bandejas de fibra óptica.
- Un Transceiver D-Link def-855 conectado a la caja multimedia (1) y al Switch D-Link
- Un Switch D-Link que está conectado al servidor.
- Switch 3COM conectado con el Switch D-Link
- Un Servidor que tiene instalado: Squid y Dansguardian para el control de contenido de internet a los usuarios del Área. Las características del servidor son:
  - Sistema Operativo Linux Fedora 6

- Intel(R) Pentium (r) 4 CPU 3.0GHz
- Memoria 512MB
- Disco 80GB

- Un Transceiver D-link def-855 conectado con la caja multimedia (2), que permite enlazar la fibra óptica al Centro de Cómputo de Área**.**

Centro de Cómputo del Área

- Una caja multimedia donde llega la fibra óptica
- Un Transceiver d-link def-855 que está conectado a la caja multimedia y al Switch D-Link
- Switch D-Link de 8 puertos, desde el cual se distribuye para los host del centro de cómputo.
- Una antena omnidireccional D-Link que permite conectar inalámbricamente con:
  - El nivel de Pregrado del Área
  - El nivel de Postgrado del Área.
  - Colegio Manuel Cabrera Lozano, anexo al Área.
  - Bloque de Coordinaciones de Carrera
  - Laboratorio de Cómputo de la Carrera de Ingles

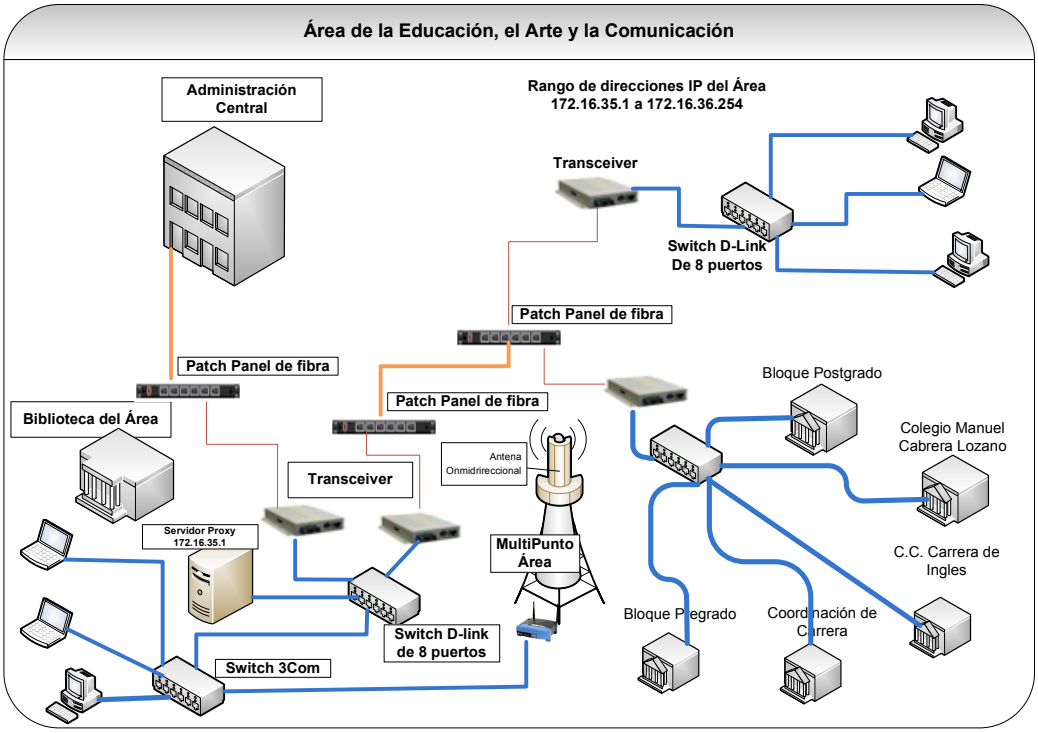


Fig. 19: Red de Datos Área de la Educación el Arte y la Comunicación

2.1.1.2.3.6 Área Jurídica, Social y Administrativa

La interconexión con esta Área es por intermedio de fibra óptica. Los principales equipos que se encuentran en aquí son:

Biblioteca del Área:

- Una caja multimedia donde llega la fibra óptica.
- Un Transceiver D-Link def-855 conectado a la caja multimedia y al Switch D-Link
- Un Switch D-Link que está conectado al servidor.
- Un Servidor que tiene instalado: Squid y Dansguardian para el control de contenido a los usuarios del área. Las características del servidor son:

- Sistema Operativo Linux Fedora 6
- Intel(R) Pentium (r) 4 CPU 3.0GHz
- Memoria 512Mb
- Disco 80GB

➢ Un Transceiver D-Link def-855 conectado con la caja multimedia, que lleva la fibra óptica al nivel de Postgrado del Área.

Nivel de Postgrado del Área

➢ Una caja multimedia donde llega la fibra óptica.
➢ Un Transceiver D-Link def-855 conectado a la caja multimedia y al Switch
➢ Un Switch D-Link que distribuye a los host del bloque.
➢ Un Transceiver D-Link def-855 conectado con la caja multimedia, que lleva la fibra óptica a Bienestar Estudiantil.

Además existe en esta Área dos antenas omnidireccionales que permite conectar inalámbricamente con:

Omnidireccional Uno

➢ Bloque principal del área.
➢ Centro de Cómputo principal del Área
➢ Bloque Modalidad de Estudios a Distancia.

Omnidireccional Dos

- Carrera de Contabilidad y Auditoria
- Carrera de Banca y Finanzas.

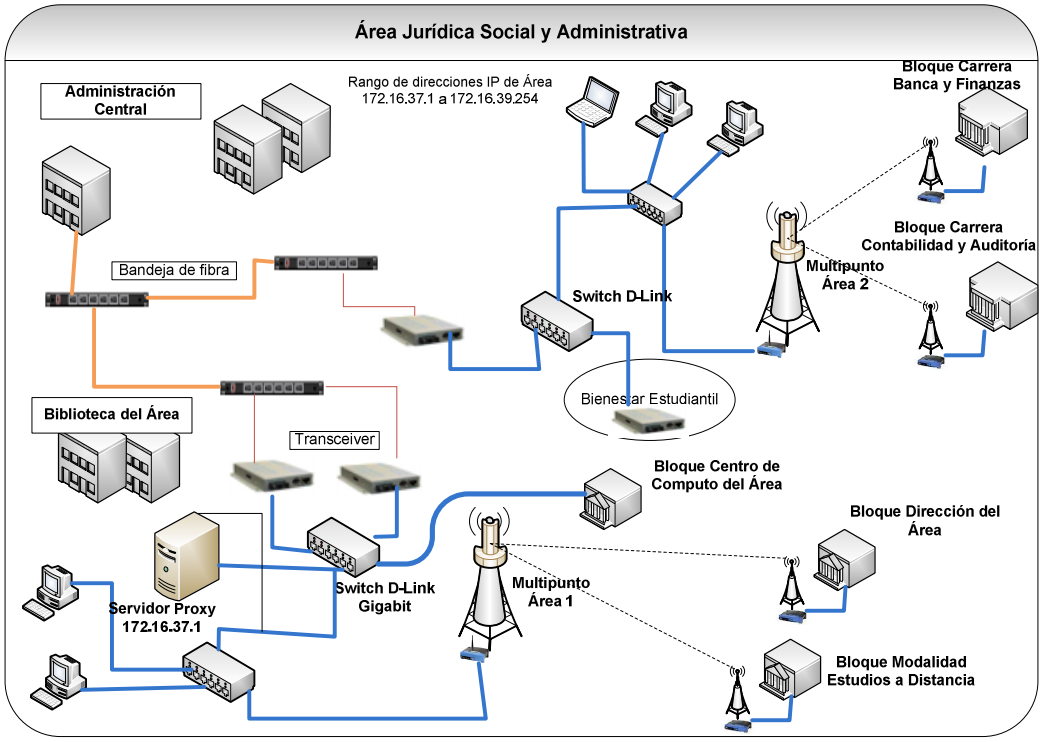


Fig. 20: Red de Datos Área Jurídica, Social y Administrativa

2.1.1.2.3.7 Área de la Salud Humana, Instituto de Idiomas, Editorial Universitaria

Con el Área de la Salud Humana se tiene una conexión inalámbrica. Los siguientes equipos existen instalados:

- Un radio Cannopy conectado al Switch D-Link.

- Un Switch D-Link (Swtich Principal) conectado al servidor y a un radio D-Link.
- Un radio D-Link multipunto, que permite tener comunicación con el Instituto de Idiomas y la Editorial Universitaria.
- Un Servidor que tiene instalado: Squid y Dansguardian para el control de contenido del internet a los usuarios del Área. Las características del servidor son:
  - Sistema Operativo Linux Fedora 3
  - Intel(R) Pentium (r) 4 CPU 2.8GHz
  - Memoria 512Mb
  - Disco 80Gb

- Una antena omnidireccional que permite la comunicación inalámbrica con:
  - Bloque de Postgrado del Área
  - Editorial Universitaria
  - Instituto de Idiomas

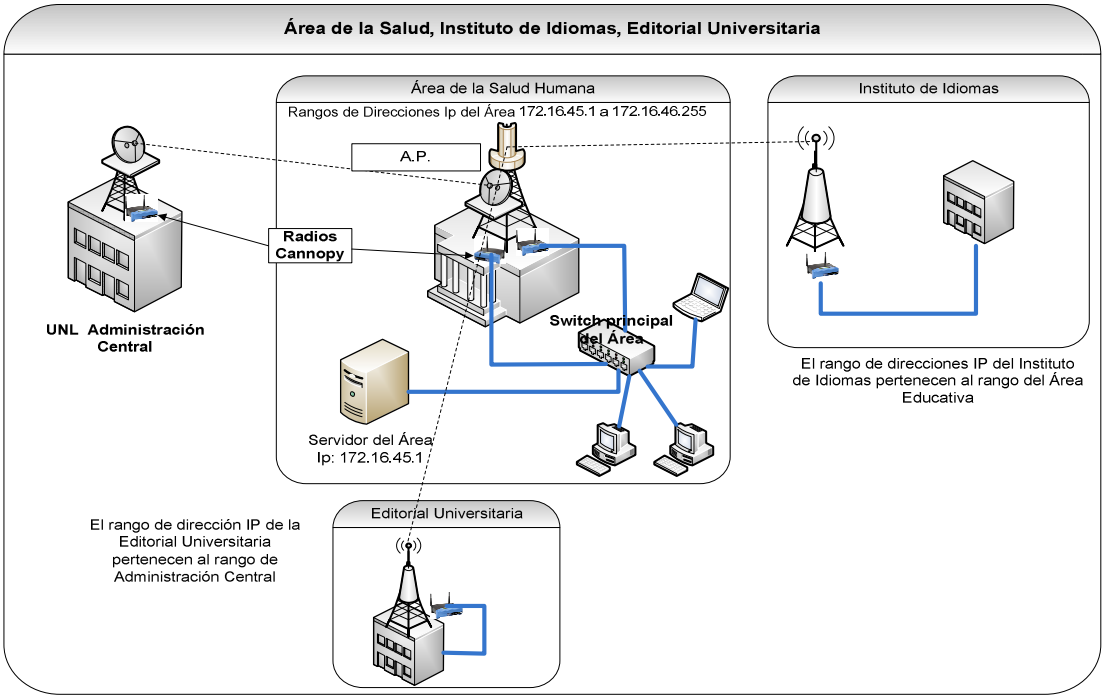


Fig. 21: Red de Datos Área de la Salud Humana, Instituto de Idiomas, Editorial Universitaria

Bienestar Estudiantil

La interconexión con Bienestar Estudiantil es por intermedio de fibra óptica.

- Una caja multimedia donde llega la fibra óptica.
- Un Transceiver D-Link def-855 conectado a la caja multimedia y a un Switch D-Link
- Un Switch D-Link que distribuye la red a los host del departamento.

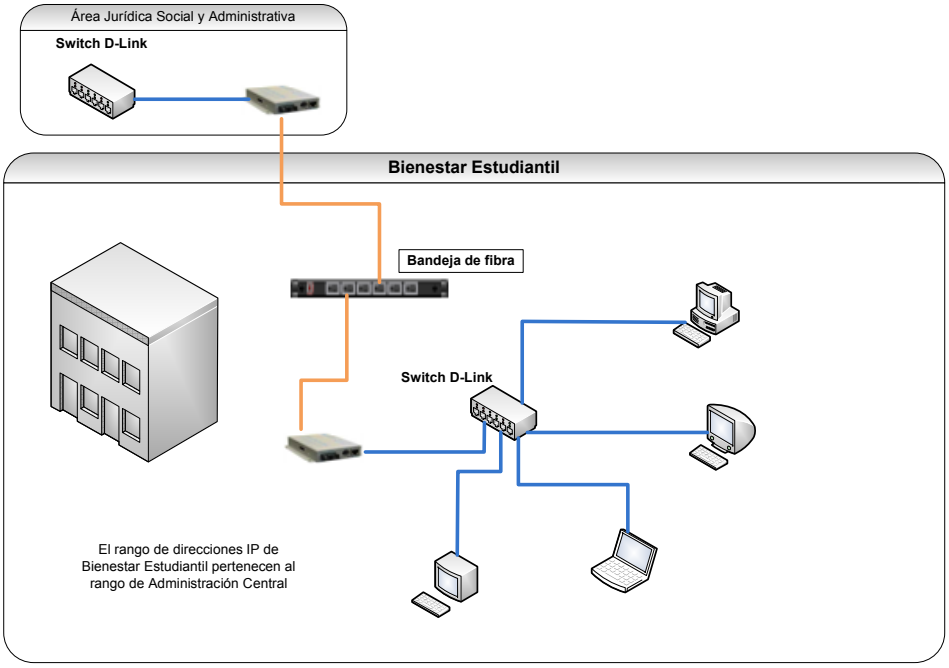


Fig. 22: Red de Datos Bienestar Estudiantil

FASE 3: DESARROLLO DE LA SOLUCIÓN

3.1 DISEÑO DE LA SEGURIDAD INFORMÁTICA MANEJADA DESDE EL DATA CENTER DE LA UNL

3.1.1 Consideraciones Generales

En la Fase 2 se mencionaba algunas consideraciones acerca de la situación actual tecnológica de la UNL y la precariedad del lugar donde funciona el Data Center actualmente en la institución, así como algunos problemas sucintados hasta la fecha en cuanto a los ataques que ha sufrido la red de datos de la institución, por esta situación se tiene como antecedente el proyecto de la construcción del edificio del Instituto de Informática, en el cual en su tercer piso funcionará a un lado del departamento de Redes y Telecomunicaciones el Data Center, tomando en consideración algunas especificaciones para su implementación física, las mismas que se están tratando en otra Tesis de este programa de maestría, en el **Anexo 3** se encuentra unos diseños de la ubicación del Data Center en el Instituto de Informática, el mismo que será construido en el Área de Energía las Industrias y los Recursos Naturales No Renovables.

En esta fase básicamente trabajaré en el diseño en sí de la seguridad informática que se manejará desde el Data Center de la UNL, tomando como consideraciones algunas situaciones básicas para manejar la seguridad hasta la solución en concreto

para algunos ataques que ha sufrido la institución y que se puedan suscitar.

3.1.2 Análisis de Requerimientos

El Centro de Datos de la UNL necesita manejar la seguridad informática de toda la organización a través de un Cortafuegos que sea más potente en cuanto al filtrado de paquetes que el que actualmente se encuentra en uso a nivel de Software, además se necesita proteger los servidores que se encuentran expuestos a través de la extranet, esto significa los que tienen direcciones públicas y por lo tanto tienen conexión a la nube, también se necesita segmentar la red para brindar privilegios a través de VLANs y de esta manera asegurar la conexión de un usuario desde cualquier punto del campus, otro requerimiento es la implementación de ACLs para poder determinar permisos de acceso, también la implementación de VPNs para poder conectar extensiones de la Universidad o simplemente para el acceso a un equipo desde un sitio remoto, es necesario también manejar sistemas de autenticación para el acceso a la red, es por eso conveniente como un requerimiento la implementación de un Servidor RADIUS, es importante ir creando la cultura de firmas digitales y certificados digitales como parte de la seguridad y por ultimo uno de los principales requerimientos sería establecer un manual de Políticas de Seguridad Informática.
Es necesario también conocer como se le puede dar solución a ciertos problemas que pueden suceder al momento de que alguien quiera atacar de alguna forma a nuestra red.

3.1.3 Diseño de la Seguridad

3.1.3.1 Seguridad en los Servidores

La seguridad de los servidores de la UNL es vital para el buen funcionamiento y flujo de la información, es por eso que se cree necesario implementar una DMZ en el borde de la red, esto se lo realizará con el HW necesario, el mismo que pueda proteger los accesos a los servidores públicos desde la extranet e intranet, la utilización de una zona desmilitarizada es vital para impedir que intrusos quieran acceder a la red interna de la organización a través de un servidor web por ejemplo, que está puesto en la red externa, de esta manera se forma un túnel en donde el intruso no puede salir más que por donde entró mismo; este planteamiento de seguridad es tomando en consideración para poder realizar su diseño debido a que en la UNL según el diseño establecido en la situación actual, no posee esta zona; los servidores que ofrecen servicios al exterior de la red se encuentran conectados directamente al Router y no al Firewall que protege la red interna, en este caso toda la seguridad de los servidores dependen de sí mismos, es decir; deben implementar diferentes mecanismos y técnicas de endurecimiento para soportar ataques desde la red insegura y continuar funcionando. El acceso desde los servidores públicos hacia la red interna es estrictamente prohibido debido a que pueden ser utilizados como salto hacia la red interna; esto quiere decir que el diseño funciona pero no es seguro, por lo que se plantea los siguientes diseños a tomarse en cuenta para brindar las respectivas seguridades.

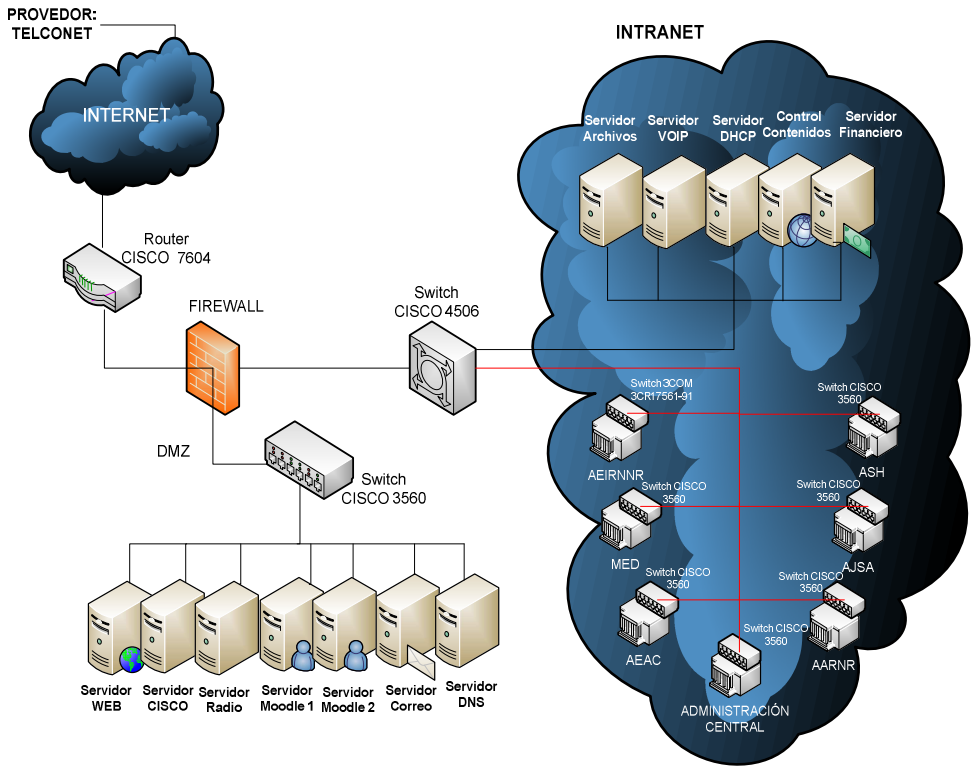


Fig. 23: DMZ con un solo Firewall

En La Fig. 23, se plantea para la seguridad de los servidores públicos y de la red interna de la UNL la utilización de un FIREWALL DMZ. El área en la que se ubican los servidores públicos se conoce como zona desmilitarizada, que puede definirse como un área pública protegida que ofrece servicios al interior y exterior de la red. La red interna se comunica con la DMZ mediante enrutamiento (no debería compartir el mismo segmento de red por razones obvias de seguridad). Este diseño es bastante común debido a su fácil implementación, seguridad y control del flujo de tráfico.

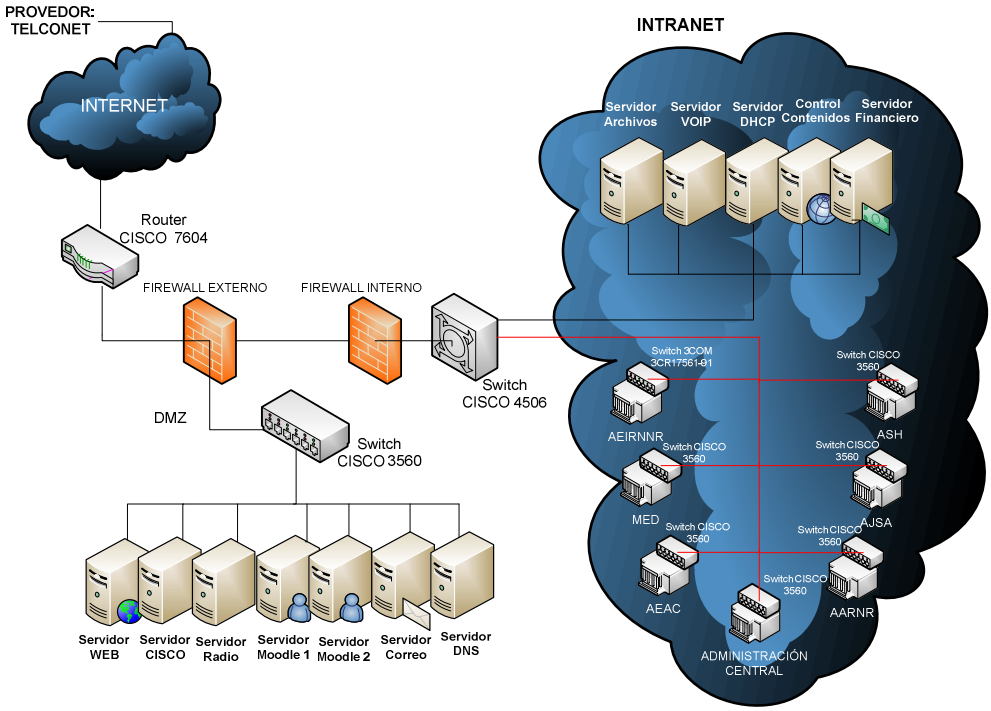


Fig. 24: DMZ con doble Firewall

En la Fig. 24, se plantea la seguridad de los servidores públicos y de la intranet con la utilización de dos Firewall, este diseño adiciona un Gateway Firewall para controlar y proteger la red interna, una de las razones es la protección de los servidores públicos frente a ataques provenientes de la red interna (como es bien conocido la mayor cantidad de ataques son generados desde dentro de la red). Ofrece mayor seguridad a la red interna al no contar con un punto único de ataque como lo que se mostró en la Fig. 23. Como desventaja si se la puede llamar así, es un poco la dificultad de configuración y monitoreo así como mayores costos en Hardware y Software.

Tomando en consideración que la UNL tiene que dar servicio a cerca de 22.000 personas entre Docentes, Administrativos, Trabajadores y Estudiantes, se considera que este diseño sería

ideal por el flujo de tráfico importante entre la red interna y la DMZ y en donde también se demanda una mayor seguridad para la red LAN.
Es conveniente como sugerencia que para este tipo de arquitectura se deberían implementar dos tipos diferentes de Firewall (podrían ser de fabricantes distintos), debido a que si un atacante logra pasar el Firewall exterior, ya tendría suficiente información para superar el Firewall interno (asumiendo que es de la misma clase), ya que tendría similar configuración al firewall ya violentado. También podría considerarse el Firewall externo como Hardware y el firewall interno como software, en la **Fase 4** se encuentra las tablas que describen el tipo de equipo que se debe utilizar para este caso.

3.1.3.2 Cortafuegos

Según la Situación Actual de la UNL, el Firewall que se maneja actualmente es a nivel de Software utilizando un equipo con características de servidor, por lo que se puede plantear en este caso dos tipos de Firewall para la protección de la red desde el Data Center.

Implementar el Cortafuegos en la UNL: Hay que tomar en cuenta que el diseño de la arquitectura y reglas del firewall se soportan sobre las políticas de seguridad de la organización, en este caso la UNL no posee políticas establecidas formalmente y es otro de los objetivos de este proyecto dar la pauta con políticas que se podrían tomar en cuenta para su implementación. Los diseños de las topologías (Fig. 23 y Fig. 24) que fueron realizados en el punto anterior son los que se

manejarán en la UNL de acuerdo a su presupuesto, añadiéndole a esto un sistema de redundancia siendo tan importante para mantener la transparencia de la conexión entre los usuarios y la red, en caso que exista algún problema con el Firewall principal; en cuanto a las reglas que controlarán el tráfico, es recomendable seguir el siguiente procedimiento:

1. Reunir suficiente información que permita una concepción de las reglas ajustada al sistema donde se implementarán, para ello se deben estudiar los servicios ofrecidos en la red y el tipo de usuarios que los reciben, considerando:

   - Nivel de acceso a la información (privado/público)
   - Criticidad de la información (alta, media, baja)
   - Seguridad en comunicaciones (cifrado o texto claro)

2. Con base en los requerimientos reunidos, se definen zonas denominadas “Security Areas”, que constituyen un conjunto de activos de red con atributos y requerimientos de seguridad similares, es decir, la red es dividida en áreas con permisos y restricciones comunes. Cada una de ellas tiene un nivel de riesgo de 1 a 5 (1=alto, 5=bajo) que debe ser debidamente justificado y que permitirá definir prioridades e incluso QoS (calidad de servicio) sobre diferente tipo de tráfico. La siguiente tabla ilustra las Security Areas de un diseño para una red de la UNL.

Área de Seguridad	Nivel de Riesgo	Descripción
Internet	1	Conexión con redes externas. Incluye Router y Firewall
DMZ	2	Servidores Públicos
Servidores Internos	3	Red de servidores para servicios internos
LAN	4	Red de usuarios

Tabla 2: Áreas de Seguridad

3. Construir en un nivel lógico las reglas que serán aplicadas a cada una de las Security Areas. La siguiente tabla explica este concepto que continúa con el ejemplo anterior.

Origen	Destino	Acceso	Protocolos	Logs	Descripción
LAN	Internet	Permitido	HTTP, HTTPS	No	Acceso a páginas Web desde red LAN
LAN	DMZ	Permitido	SMTP	Si	Conexión a servidor de correo en la DMZ
Internet	DMZ	Permitido	HTTP, HTTPS	Si	Acceso a servidores web de la

					red desde internet
LAN	Servidores internos	Permitido	SMB, HTTP, HTTPS, DNS	Si	Acceso a servicios LAN
DMZ	Internet	Permitido	DNS	No	Resolución DNS para servidores públicos de la DMZ

Tabla 3: Accesos de las Áreas de Seguridad

Como se puede apreciar, se define qué tipo de accesos son permitidos entre las Security Areas y cuándo almacenar registros de las conexiones.

4. Una vez finalizado el diseño se procede con la implementación y pruebas correspondientes de la solución.

Como escoger un Firewall: los criterios más importantes para poder escoger un dispositivo de tanta importancia son:

- *Throughput esperado:* un firewall es un bottleneck para la red, una medida que es necesaria en la que se pierde en desempeño y se gana en seguridad. Este es un criterio de diseño importante porque se debe seleccionar una solución que no afecte considerablemente los tiempos de transferencia de información.

- *Presupuesto:* existen diversas alternativas libres y comerciales, a las cuales se les debe evaluar ventajas y desventajas en términos de credibilidad, calidad, soporte, casos de éxito y costos.
- *Número de redes a proteger:* el tamaño de la red es un punto importante que define las capacidades del hardware de la máquina. También debe estudiarse y considerarse el tráfico estimado que controlará el firewall.
- *Nivel de profundidad del filtrado:* dependiendo de los recursos a proteger es conveniente decidir hasta qué capa debe realizarse chequeo de los paquetes, considerando que a mayor nivel de profundidad se pierde en velocidad pero se gana en seguridad.
- *Capacidad de escalabilidad de las funciones del firewall*.

Tomando en consideración todos estos puntos se establece que la UNL tiene que manejar un Firewall para la red Externa basado en Hardware que podría ser un (CISCO ASA 5540) con redundancia utilizando el mismo Hardware y para la red interna se utilizará un Firewall basado en Software que podría ser (IPTABLES) con la utilización de un Proxy (SQUID) con esto tendríamos tecnologías diferentes y configuraciones diferentes para garantizar seguridad en caso de ataques. En la Fase 4 se detallan los modelos y las características de estos Firewall.

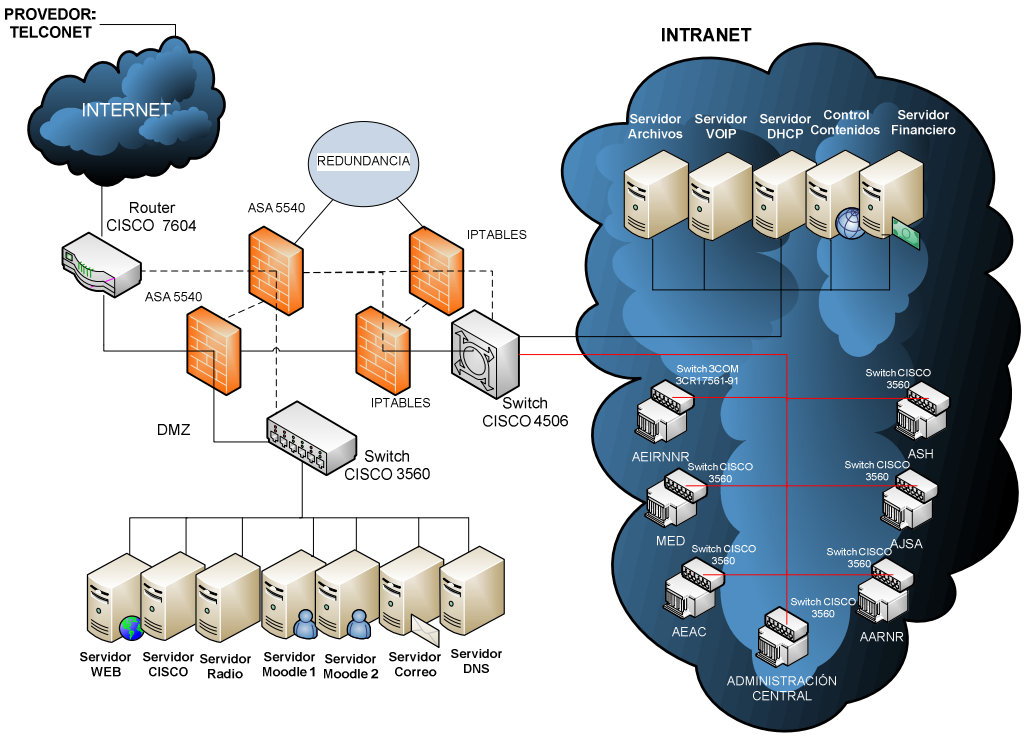


Fig. 25: Diseño de red con Redundancia

3.1.3.3 Utilización de VLANs

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con los switchs que utilizamos en esta propuesta se soporta la utilización de VLANs, y el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los “dominios de colisión” por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los “dominios de broadcast”, en lugar de uno solo, se puede configurar el switch para que existan más “dominios”.
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.
- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán “vernos” como una Red de Área Local independiente a las demás.

El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

En el caso de la UNL se utilizaría **VLANs POR DHCP** se asignará un bloque de direcciones para cada VLAN y se las administrará a través de un servidor DHCP, por lo que al momento de encender cada computador automáticamente lo

reconoce el DHCP y le asigna una dirección IP de acuerdo a la VLAN que corresponda.

A continuación se muestra las VLANs que se manejarían en la UNL, esto es como propuesta, si se cree necesario implementar más VLANs el esquema está totalmente abierto, lo importante es tener dispositivos, en este caso un Switch que soporte la configuración de VLANs y con eso poder administrarla, como el campus universitario es muy grande entonces tendríamos uno o varios switch capa 3 en cada área.

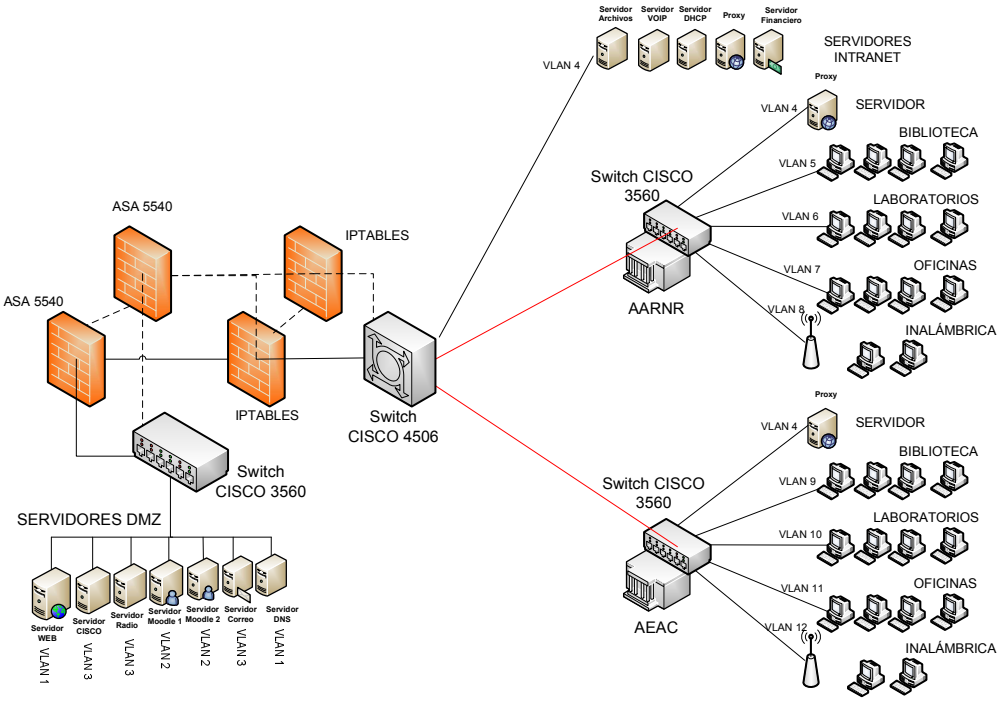


Fig. 26: VLANs en el AARNR y AEAC

En la Fig. 26, se establece las posibles VLANs que se configurarían para algunas dependencias importantes de las áreas de Agronomía y Recursos Naturales Renovables y el Área de Educación Arte y Comunicación.

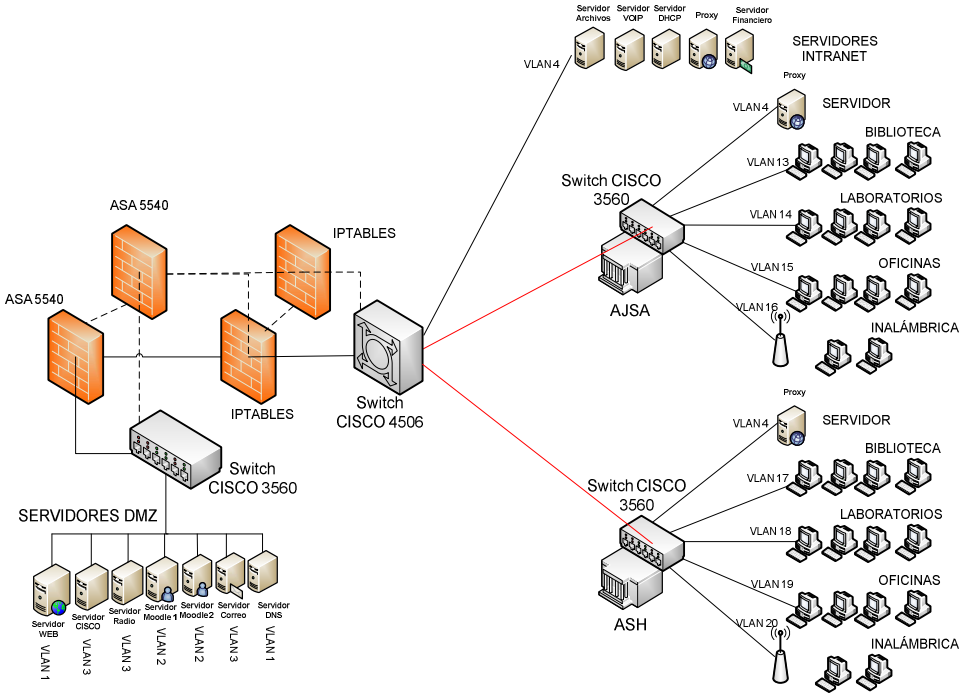


Fig. 27: VLANs en el AJSA y ASH

En la Fig. 27, se establece las posibles VLANs que se configurarían para algunas dependencias importantes de las áreas Jurídica social y Administrativa y el Área de la Salud Humana.

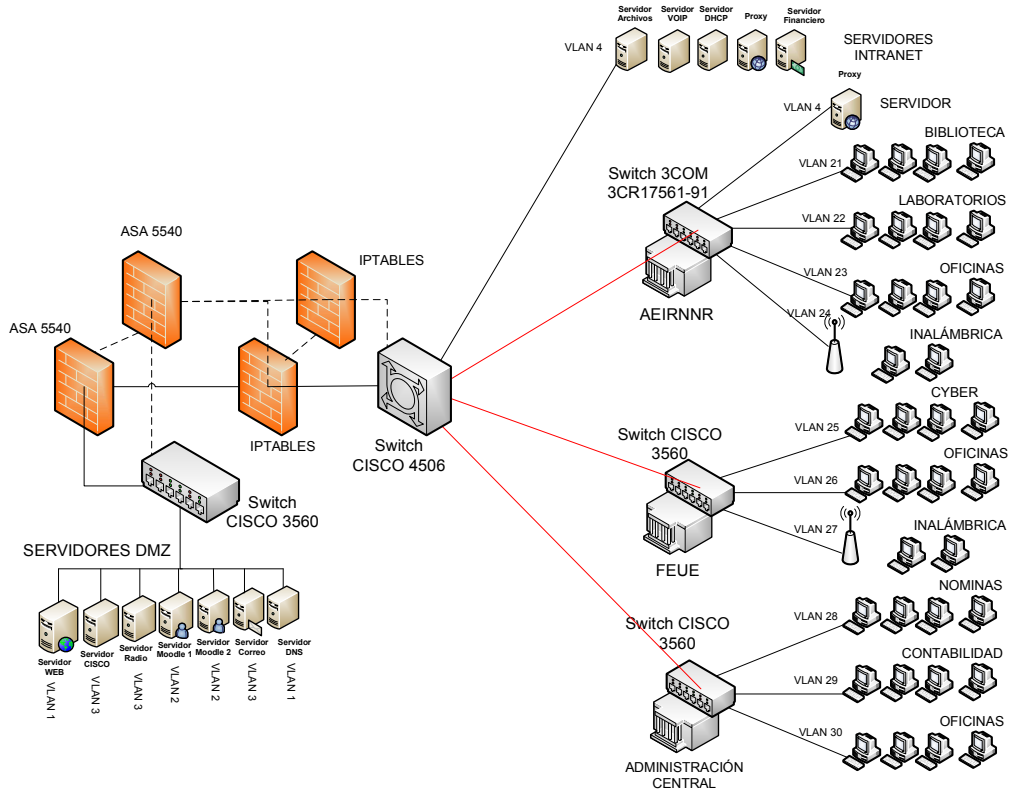


Fig. 28: VLANs en el AEIRNNR, FEUE y ADMINISTRACIÓN CENTRAL

En la Fig. 28, se establece las posibles VLANs que se configurarían para algunas dependencias importantes de las áreas de Energía las Industrias y los Recursos Naturales no Renovables, la FEUE de Loja y la Administración Central.

3.1.3.4 Utilización de ACLs

Una ACL es una colección secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior, estas nos permiten limitar el acceso desde y hacia dispositivos a través de un filtrado de paquetes, este tipo de filtrado de paquetes en combinación con las VLANs, el

Cortafuegos y las políticas de seguridad que establezca la UNL serán mecanismos importantes para brindar seguridad a la información en la organización.

Las ACLs en **Linux** por ejemplo, que es el Sistema Operativo que utiliza la UNL para el manejo de sus servidores, corresponde a un conjunto de permisos complementarios que se encuentran dentro del sistema de archivos ext2, ext3 y nfs por su puesto dependiendo de las distribuciones y de las versiones de esas distribuciones.

En el Caso de los **Router y Switch de capa 3** estos proporcionan capacidades de filtrado de tráfico a través de listas de control de acceso (ACL), las mismas que son listas de instrucciones que se aplican a una interfaz del Router. Estas listas indican al Router que tipo de paquetes se deben aceptar y qué tipo de paquetes se deben denegar. La aceptación o rechazo se puede basar en ciertas especificaciones, como dirección de origen, dirección destino y número de puerto. Cualquier tráfico que pase por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL. Las ACLs se pueden crear para todos los protocolos enrutados de red, como IP e IPX, para filtrar los paquetes a medida que pasan por un dispositivo capa 3. Es muy importante la utilización de ACL en la red de la UNL, a continuación se explican algunas razones para poderlas implementar:

- Mejorar el tráfico y el rendimiento de la red de la UNL. Por ejemplo las ACL pueden designar ciertos paquetes para que un router o switch de capa 3 los procese antes de procesar

otro tipo de tráfico, según el protocolo. Esto se denomina colocación en cola, que asegura que los routers no procesarán paquetes que no son necesarios. Como resultado, la colocación en la cola limita el tráfico de red y reduce la congestión.

- Brindar control de flujo de tráfico. Por ejemplo las ACL pueden restringir o reducir el contenido de las actualizaciones de enrutamiento. Estas restricciones se usan para limitar la propagación de la información acerca de redes específicas por toda la red.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Al host A se le permite el acceso a la red de Recursos Humanos, y al host B se le deniega el acceso a dicha red. Si no se configura ACL en el dispositivo de capa 3, todos los paquetes que pasan a través del dispositivo supuestamente tendrían acceso permitido a todas las partes de la red.
- Se debe decidir qué tipo de tráfico se envían o bloquean en las interfaces del dispositivo de capa 3. Por ejemplo, se puede permitir que se enrute el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de Telnet.

En el caso de Linux por ejemplo, al manejar un Firewall en Linux utilizando IPTABLE el proxy de ese cortafuego será en Linux mismo utilizando una herramienta que se llama **Squid**, que a la final sirve para establecer una Lista de Control de Acceso, dentro de esta lista se podría tener:

- Evitar que los usuarios de la red se conecten a Internet a partir de cierta hora.
- Que no puedan hacer uso de internet el fin de semana.
- Que no se puedan descargar archivos con ciertas extensiones.
- Que no puedan acceder a ciertas páginas de internet.
- Que no se puedan conectar a internet ciertos departamentos de la institución.

Existen muchas más cosas que se podrían realizar, actualmente en la UNL si se maneja este proxy utilizando las herramientas de **Squid y Dansguardian** para poder realizar en control de acceso a internet y el control de contenido en los accesos a internet, por lo tanto se está manejando un nivel de ACL, faltaría implementarlo a nivel de dispositivos de Capa 3 para ver el resultado que se obtiene.

3.1.3.5 Utilización de VPNs

La Universidad Nacional de Loja actualmente utiliza las VPN para establecer una conexión con una sede en Quito y lo realiza a través de una conexión **Firewall to Firewall** o a través de una **Conexión de Acceso Remoto** configurando el OpenVPN, lo que ha dado resultado.
Hay que tomar en cuenta que para cualquier conexión que se realice la seguridad es fundamental en este caso la seguridad lo da el utilizar el protocolo **IPSEC** que protege los datos transferidos y garantiza que el servidor del paquete sea el que dice el paquete IP, pero solo ofrece seguridad en capa 3 y no

en las capas inferiores y además es muy complicada su configuración.

Actualmente la UNL maneja una VPN a nivel de software en este caso utiliza OpenVPN el mismo que lo tiene instalado en el Firewall que se maneja a través de IPTABLE y con ello establece el túnel de conexión con el usuario en Quito, en la Fig. 29 se presenta el diseño del manejo actual de la VPN en la UNL.

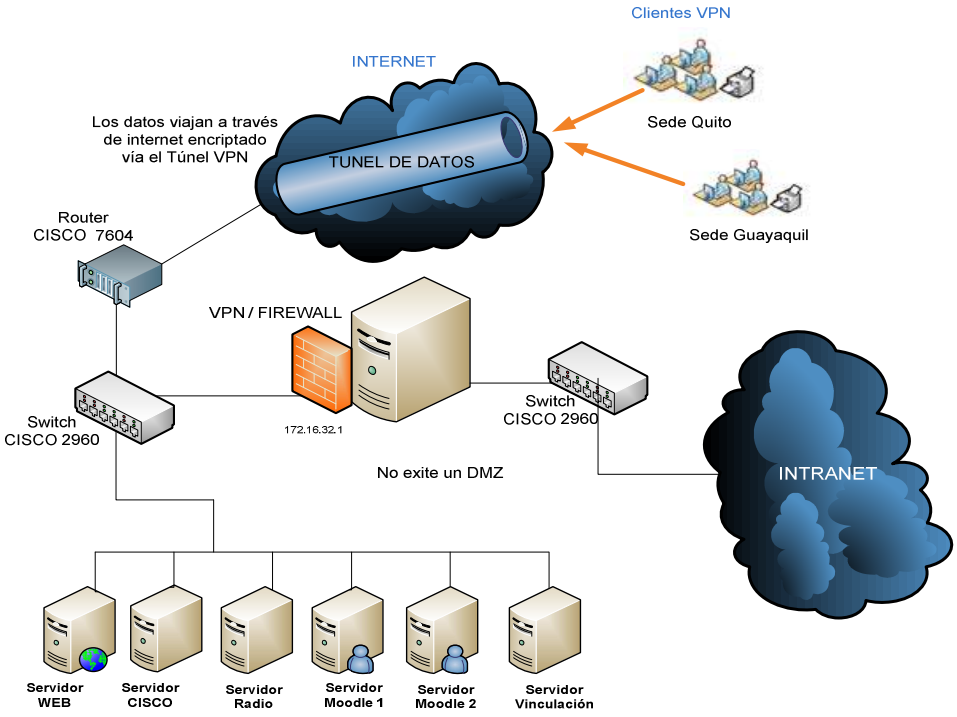


Fig. 29: Manejo de VPN actual en la UNL

Una de las soluciones más comunes en las organizaciones es utilizar Hardware para establecer la VPN por ejemplo (Router to Router) pero el consto es mayor, por lo tanto yo aconsejaría que se siga utilizando OpenVPN con la diferencia que no lo instalaríamos en el Firewall sino más bien utilizaríamos **un**

servidor solo para VPN utilizando **OpenVPN** el mismo que estaría conectado a la DMZ y saldríamos a través del Router del ISP[18], en la Fig. 30 se muestra el diseño de la VPN propuesto.

VENTAJAS Y DESVENTAJAS DE OpenVPN	
VENTAJAS	**DESVENTAJAS**
OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de IPsec	No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).	Falta de masa crítica.
Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un	Todavía existe poca gente que conoce cómo usar OpenVPN.

[18] Proveedor de Servicios de Internet

puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.	
Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.	Al día de hoy sólo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.
Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).	
Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo	

puerto TCP o UDP.	
Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.	
Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.	
Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.	
Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.	
Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.	
Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso	

son increíblemente simples.	

Tabla 4: Ventajas y desventajas de OpenVPN

Es importante conocer que ofrece IPsec y que ofrece OpenVPN para tener el panorama más claro y poder establecer porque escoger OpenVPN; en la Tabla 5, se establece una comparación entre estas dos.

COMPARACIÓN ENTRE OpenVPN e IPsec VPN	
IPsec	**OpenVPN**
Estándar de la tecnología VPN	No compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles, ya comienzan a encontrarse dispositivos que cuentan con OpenVPN
Tecnología conocida y probada	Probada y sigue en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla
Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados

Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender y éxito rápido para principiantes
Necesidad de uso de muchos puertos y protocolos en el firewall	Utiliza solo un puerto del firewall
Problemas con direcciones dinámicas en ambas puntas	Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía
	Control de tráfico (Traffic shaping)
	Velocidad (más de 20 Mbps en máquinas de 1Ghz)
	Compatibilidad con firewall y proxies

	Ningún problema con NAT (ambos lados puede ser redes NATeadas)
	Posibilidades para **Road Warriors**[19]

Tabla 5: Comparación entre OpenVPN e IPsec VPN

Una de las razones fundamentales para la propuesta de seguir manejando OpenVPN es por su condición de software libre y por el costo $ 0 que le implica a la universidad, a continuación se muestra el diseño de la VPN propuesta.

[19] **Road Warrior**: Es una de las formas más utilizadas y solicitadas por los estudiantes. Es el permitir que una máquina de alguien que esté fuera de nuestra red (de forma temporal o permanente) pueda comunicarse con el servidor OpenVPN de nuestra red y una vez autenticado pueda entrar a ver y acceder los recursos de nuestra red local.

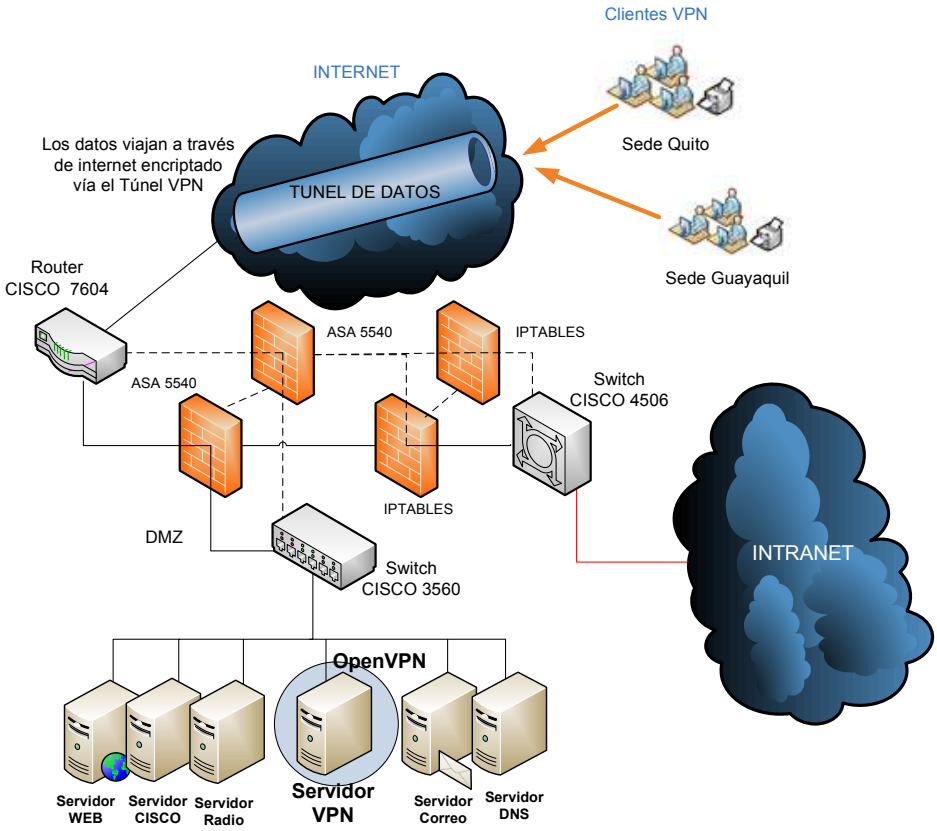


Fig. 30: Propuesta del manejo de VPN

3.1.3.6 Utilización de Protocolo AAA a través de RADIUS

Sabemos que AAA significa (Autenticación, Autorización y Auditoría), y se convierte en un mecanismo más para poder brindar seguridad a la red manejada desde el Data Center de la UNL, permitiendo conocer que usuarios son los que se conectan a la red. La utilización de este protocolo que más bien no se refiere a uno solo, si no a un conjunto de protocolos que ofrecen los tres servicios, se lo puede realizar a través de redes cableadas e inalámbricas a continuación daré la propuesta para los dos casos.

Redes Cableadas: para estas redes y las inalámbricas la mejor propuesta que he analizado por lo que significa trabajar con software libre, sería utilizar un servidor RADIUS y un servidor LDAP y como la UNL maneja bastante Software Libre utilizaríamos **OpenLDAP** que contendrá la información de los usuarios que se conectan a la red trabándolo a través de perfiles, con la diferencia que los switches que se utilicen tiene que soportar conexión mediante RADIUS, es decir, autenticación; ventajosamente según la propuesta que se plantea los switches CISCO 2960, 3560 y 4506 si soportan RADIUS por lo que se hace más fácil la configuración, ahora depende de la Universidad la compra de equipamiento si no lo posee para establecer este tipo de seguridad a nivel de redes cableadas o si se implementaría RADIUS pero para redes inalámbricas, en la Fig. 33 se observa como quedaría el diseño de esta red.

- **El Suplicante**, o equipo del cliente, que desea conectarse con la red.

- **El Servidor de Autorización/Autenticación**, que contiene toda la información necesaria para saber cuáles equipos o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las redes de área local alambradas e inalámbricas.

- **El Autenticador**, que es el equipo de red (switch, ruteador, servidor de acceso remoto, punto de acceso) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

- **Servidores de Autenticación,** Aunque en la especificación 802.1x se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (Authentication, Authorization and Accounting). Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA.

RADIUS es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). Estos elementos envían información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la

comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red.

Redes inalámbricas: para las redes inalámbricas así como lo dije anteriormente igual se utilizará un servidor RADIUS y un servidor OpenLDAP con la diferencia que aquí se debe seleccionar el mecanismo de autenticación, debido a que podemos tener autenticación por dirección física del dispositivo de red o autenticación por usuario-contraseña.
Para efectos de la propuesta se escoge la validación por usuario contraseña la misma que para que se pueda realizar se debe cumplir ciertas condiciones tanto por parte del usuario, por parte de los dispositivos de acceso así como por parte del servidor de autenticación.

Usuarios: Desde el punto de vista de los clientes de acceso cableado e inalámbrico, exactamente sobre los requerimientos de la conexión, se debe validar si las plataformas utilizadas en los clientes soportan el tipo de autenticación elegido o si por el contrario requieren un componente de software que los habilite para realizarla, en este caso los clientes tendrían que tener instalado el Hot Spot para poder ingresar su usuario y contraseña.

Access Point y Switch: Entre los principales requerimientos, sobre estos dispositivos, para poder implementar un mecanismo de seguridad para el control del acceso inalámbrico, se encuentran:

- Compatibilidad con 802.11 y soporte de cifrado WPA

- Capacidad de implementar el servicio de control de acceso 802.1x
- Configuración del protocolo 802.1q para VLANs.

El Servidor de Autenticación: Finalmente, los principales requerimientos en este componente, para poder implementar la solución de seguridad basada en 802.1x, son:

- Compatibilidad con 802.1x
- Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)
- Capacidad de registro (Accounting)

Flexibilidad para validar a los suplicantes mediante varios métodos (Base de datos de usuarios local, directorio de usuarios OpenLDAP, certificados, entre otros)

3.1.3.6.1 Validación por Usuario – Contraseña

Anteriormente se determinó que la mejor solución para el control de acceso a la red es el uso de un servidor RADIUS trabajando con el estándar 802.1x, utilizando un servidor de bases de datos OpenLDAP y Hot Spot.

El servidor RADIUS elegido (**freeradius**) permite interactuar con el Hot Spot. La interacción de estos, más el servidor de bases de datos (OpenLDAP), son las herramientas necesarias para satisfacer los requerimientos de control de acceso por usuario-contraseña que la propuesta requiere.

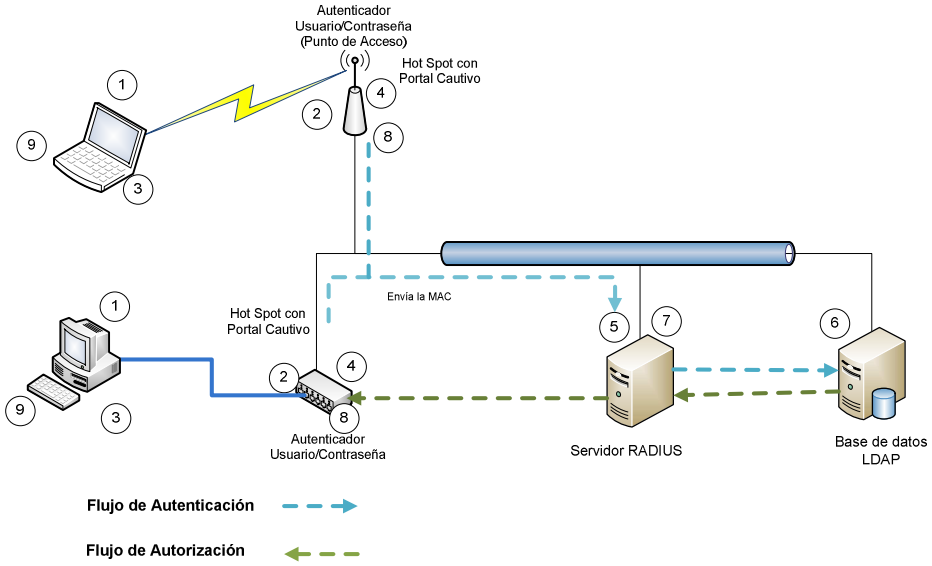


Fig. 31: Esquema de validación por usuario - contraseña

El autenticador juega un rol importante en el proceso de validación por usuario-contraseña, ya que además de servir como autenticador bajo el estándar 802.1x, es quien contiene el Hot Spot, encargado de entregar al usuario la página en formato web donde deberá ingresar el usuario - contraseña. Dicha página está alojada en el servidor web.

El proceso de validación es el siguiente para un caso favorable:

- El suplicante levanta su tarjeta de red (alámbrica o inalámbrica), enviando las características de su equipo al autenticador en forma automática.
- El Hot Spot (o autenticador) recibe el paquete con la información proveniente del suplicante y le entrega la configuración de su dispositivo de red, por medio del

protocolo de asignación dinámica de servidores (DHCP), mientras aguarda por la información de validación (usuario-contraseña).

- El suplicante recibe el paquete, quedando configurada su interfaz de red. Luego, debe abrir el explorador de Internet (puede abrir cualquier página inicial, distinta de la página en blanco “about:blank”) siendo re direccionado, por el portal cautivo, a la página de validación donde ingresará el usuario-contraseña que le corresponda. El usuario-contraseña es enviado al Hot (autenticador).
- El autenticador recibe el paquete con la información proveniente del suplicante, y envía el usuario-contraseña de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.
- El servidor RADIUS consulta a la base de datos, la existencia de usuario y contraseña del suplicante en las tablas de almacenamiento de estas.
- El servidor de bases de datos, chequea que el usuario y contraseña del suplicante se encuentre en las tablas de validación. Si corresponde, envía esta información al servidor RADIUS.
- El servidor RADIUS válida al suplicante y lo autoriza a hacer uso de la red de servicio, enviando la decisión al autenticador.
- El autenticador recibe la decisión del servidor RADIUS, y abre los puertos para que el suplicante pueda hacer uso de la red de servicio.
- El suplicante puede hacer uso de la red de servicio.

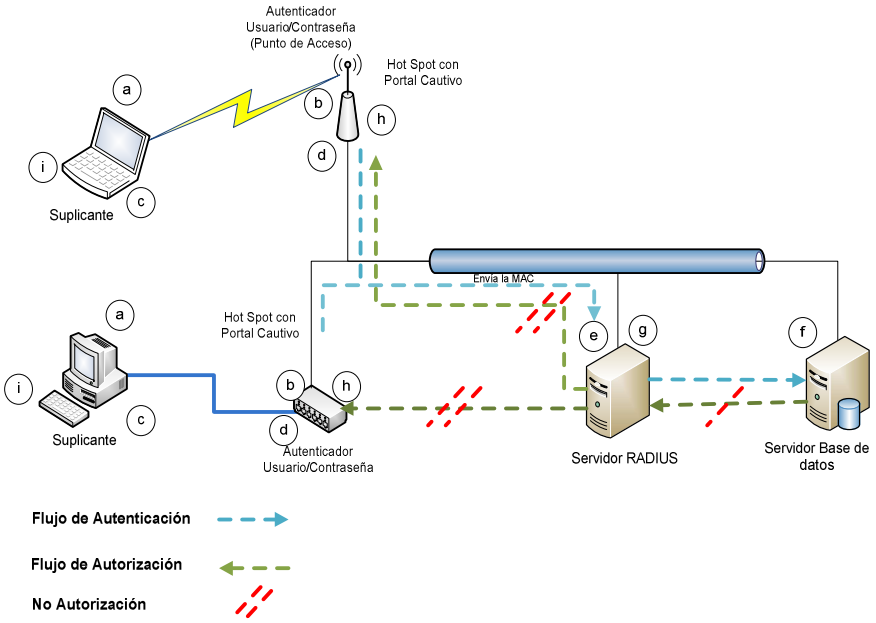


Fig. 32: Esquema de validación por usuario – contraseña no favorable

- El suplicante levanta su tarjeta de red (alámbrica o inalámbrica), enviando las características de su equipo al autenticador en forma automática.
- El Hot (o autenticador) recibe el paquete con la información proveniente del suplicante, y le entrega la configuración de su dispositivo de red por medio del protocolo de asignación dinámica de servidores (DHCP), mientras aguarda por la información de validación (usuario-contraseña).
- El suplicante recibe el paquete, quedando configurada su interfaz de red. Luego, abre el explorador de Internet (puede abrir cualquier página inicial distinta de la página en blanco “about:blank”) siendo redireccionado, por el Hot, a la página de validación donde ingresará el usuario-contraseña que le corresponda, que en este caso es

erróneo. El usuario-contraseña es enviado al Hot Spot con portal cautivo (autenticador).

- El autenticador recibe el paquete con la información proveniente del suplicante y envía el usuario-contraseña de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.
- El servidor RADIUS consulta a la base de datos la existencia de usuario y contraseña del suplicante en las tablas de almacenamiento de estas.
- El servidor de bases de datos chequea que el usuario y contraseña del suplicante se encuentran en las tablas de validación. Como no corresponde, envía esta información al servidor RADIUS.
- El servidor RADIUS no válida al suplicante, y por lo tanto, no lo autoriza a hacer uso de la red de servicio, enviando la decisión al autenticador.
- El autenticador recibe la decisión del servidor RADIUS y mantiene los puertos de comunicación con la red de servicio cerrados para el suplicante y espera por un usuario-contraseña nuevo, repitiéndose el proceso anterior.
- El suplicante no puede hacer uso de la red de servicio.
- El proceso cumple con los requerimientos que el proyecto necesita para el control de acceso por usuario-contraseña.

Para llegar a ejecutar la propuesta se deberá conocer sobre la configuración del Servidor Radius con todos los certificados que este implica, se recomienda trabajar sobre la plataforma CentOS de Linux por lo que la UNL maneja gran cantidad de

servidores sobre esta plataforma, esto por el hecho de estandarización de herramientas y de software, además se habla de configurar un servidor OpenLDAP en el que contendrá la información de todos los usuarios de la red, por lo que podríamos valernos de la base de datos que maneja el Grupo de Desarrollo de Software de la UNL, con lo que se tendría que investigar como poder migrar la información de esta BD[20] que ellos manejan a la BD de OpenLDAP.

A continuación se presenta el diseño de la validación por **usuario – contraseña** desde el esquema de red general de la UNL.

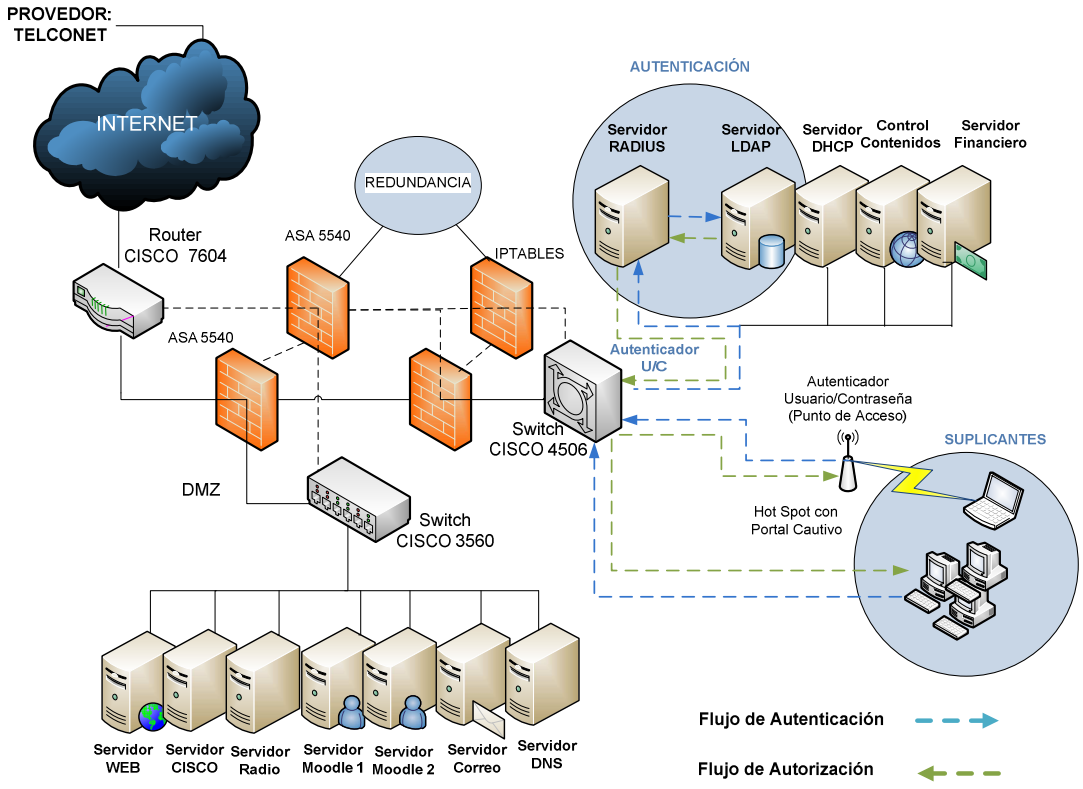


Fig. 33: Esquema general de la red utilizando AAA a través de RADIUS

[20] Base de Datos

3.1.3.7 Importancia de utilizar Certificados y Firmas Digitales

Certificado Digital: Estos brindan una forma conveniente y fácil de asegurar que los participantes en una transacción electrónica puedan confiar el uno en el otro. Esta confianza se establece a través de un tercero llamado Autoridades Certificadoras como por ejemplo: IpsCA, Certisur, Verisign.

En pocas palabras, los certificados digitales garantizan que dos computadoras que se comunican entre sí puedan efectuar transacciones electrónicas con éxito. La base de esta tecnología reside en los códigos secretos o en la **encriptación**. La encriptación garantiza la confidencialidad, la integridad y la autenticidad de la información que se desea transmitir y que tiene vital importancia para la persona o empresa, en este caso para la UNL.

El procedimiento de encriptación es sencillo. Un mensaje puede pasar por un proceso de conversión o de encripción, que lo transforma en código usando una clave, es decir; un medio de traducir los signos de un mensaje a otro sistema de signos cuya lectura no tenga ningún sentido para un desconocido que los intercepte. Esto se conoce como el proceso de encripción de un mensaje. Un ejemplo sencillo de una clave puede ser el reemplazar cada letra con la próxima letra del alfabeto. Así la Palabra VISA se convertiría en WJTB. Para descifrar el mensaje o revertir la encripción el que lo recibe necesita conocer la clave secreta (o sea el certificado digital).

Existen algunos tipos de Certificados Digitales, pero se le recomienda a la UNL comprar certificados SSL porque permiten:

- *Verificación de la identidad del servidor*. Los usuarios de un Sitio Web pueden verificar si el certificado es válido y pertenece a una Autoridad Certificadora CA oficial. De esa manera el usuario puede comprobar la autenticidad de un Sitio Web y decidir si compartir o no datos confidenciales, como números de tarjetas de crédito, con él.
- *Verificación de la identidad del usuario*. Un servidor puede consultar los datos personales de un usuario de su Sitio Web a través de la Firma Digital o Certificado Personal, y verificar si se haya registrado oficialmente por una Autoridad Certificadora CA. Esta funcionalidad es muy importante en instituciones financieras que transmiten datos confidenciales de sus Clientes, pues deben asegurarse que la información llegue al destinatario real.
- *Conexiones seguras*. Toda la información enviada desde un usuario hacia el Sitio Web viaja encriptado, por lo que de ser interceptada es imposible de descifrar. Además la información se marca digitalmente, lo que permite verificar si fue alterada en su viaje por Internet.

El protocolo SSL soporta diferentes algoritmos criptográficos (ciphers) que se usan para los procesos de autenticación y cifrado de información:

- DES. Data Encryption Standard, algoritmo utilizado por el gobierno de los Estados Unidos de América.

- DSA. Digital Signature Algorithm, parte del estándar de autentificación digital usado por los Estados Unidos de América.
- KEA. Key Exchange Algorithm, algoritmo utilizado para intercambio de llaves públicas y privada por los Estados Unidos de América.
- MD5. Message Digest, algoritmo desarrollado por Rivest.
- RC2 y RC4. Algoritmos de Rivest desarrollados para RSA Data Security.
- RSA. Algoritmo desarrollado por Rivest, Shamir y Adleman para encripción y autentificación.
- RSA key exchange. Algoritmo para el intercambio de llaves públicas y privadas basado en RSA.
- SHA-1. Secure Hash Algorithm, función Hash utilizada por los Estados Unidos de América.
- SKIPJACK. Algoritmo simétrico compatible con hardware FORTEZZA, del gobierno de los Estados Unidos de América.
- Triple-DES. DES aplicado tres veces.

La elección del cipher más adecuado dependerá de las necesidades de seguridad de una organización y de la compatibilidad requerida. Los cipher para SSL más populares son RSA.

Firma Digital: Con el Certificado digital se permite garantizar que el autor del mensaje es quien realmente dice ser. Es decir, se garantiza que el receptor pueda verificar que el documento ha sido enviado por el autor, que el autor no pueda negar la

realización del documento, y que el receptor no pueda altera su contenido.

Por ejemplo, cuando un usuario A genera un mensaje para un usuario B, lo encripta junto con su certificado. Opcionalmente puede protegerlo con la clave pública del usuario B. Esto es lo que se llama **Firmar Digitalmente** o construir lo que se denomina un Sobre electrónico. Nadie puede modificar el contenido del mensaje sin destruir el certificado del emisor, lo que garantice la inviolabilidad del mismo.

Las **firmas digitales** son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave pública; son utilizadas principalmente para verificar la autenticidad del mensaje o la de una llave pública.

Es importante que la **Universidad Nacional de Loja** a través de su Centro de Datos maneje transacciones electrónicas seguras para ello se crea los **certificados digitales y Firmas digitales** que no es lo mismo que firma electrónica, para Suramérica se tiene algunas filiales a la empresa **Verisign** por ejemplo: en Brasil, Argentina y Chile; en esta última se tiene la empresa afiliada llamada **E-Sign** que da servicio a Chile, Perú, **Ecuador** y Colombia, por lo que se tendría que hacer el contacto respectivo para saber cuáles son los beneficios y el costo de los mismos.

3.1.4 Nuevo Esquema de Seguridad Informática en la Implementación del Data Center de la UNL

A continuación se presenta el esquema como propuesta para ser tomado en cuenta en la seguridad informática que se manejará desde el Data Center de la Universidad Nacional de Loja.

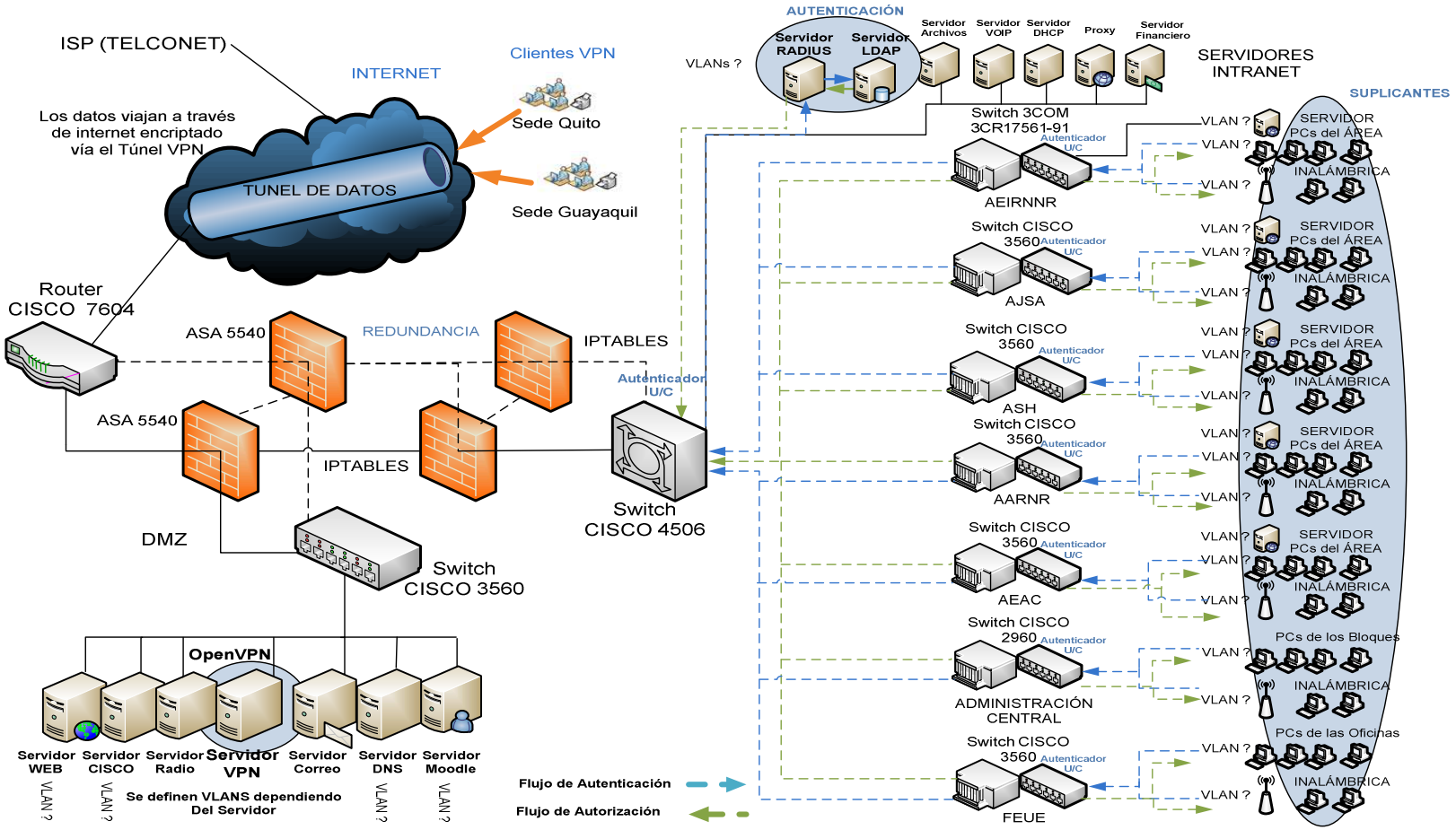


Fig. 34: Esquema de Seguridad Informática para la UNL manejada desde el Data Center

3.1.5 Solución contra Amenazas

3.1.5.1 Solución al IP Spoofing

Prevención

Una de las formas de prevenir este problema es utilizando un Router en el borde de la red, normalmente los ISP colocan ese dispositivo, luego se tendría que configurar el mismo de tal manera que no permita que un paquete lo atraviese si el mismo tiene como dirección origen una que corresponde a la red interna, este tipo de configuraciones se las puede encontrar fácilmente en el Internet.

Otra manera es colocando un Firewall que pueda detener el acceso de intrusos con direcciones públicas que quieran ingresar o enviar paquetes a host de la red interna, ventajosamente el Firewall ASA 5540 de CISCO realiza este trabajo por lo que el administrador tiene un peso menos de que preocuparse.

3.1.5.2 Solución al DNS Spoofing

Prevención

Se pueden tomar algunas medidas para prevenir el DNS Spoofing como administradores, estas son:

- Limitar el cache y asegurarse que no está guardando registros adicionales.
- Mantener el servidor DNS actualizado y con los últimos parches.
- No hacer que los sistemas seguros dependan de DNS

- Usar encripción: firmar las zonas con tsig hmac-md5 y usar OpenDNS.

Las medidas que se pueden tomar como usuario son:

- Siempre checar que la pagina no tenga problemas de direccionamiento.
- No depender de cookies como único método de autenticación.
- Tener los últimos parches del sistema.
- Usar encripción

3.1.5.3 Solución a SMTP Spoofing

Prevención

Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales, así como también denegar el acceso a través del puerto 25. Existen otras maneras de evitar el Spoofing de manera general, estas se encuentran al final en el punto 3.1.5.5.

3.1.5.4 Solución al ARP Spoofing

Prevención

Un método para prevenir el ARP Spoofing, es el uso de tablas ARP estáticas, es decir añadir entradas estáticas ARP, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP. Sin embargo, esta no es una solución práctica, sobre todo en

redes grandes, debido al enorme esfuerzo necesario para mantener las tablas ARP actualizadas: cada vez que se cambie la dirección IP de un equipo, es necesario actualizar todas las tablas de todos los equipos de la red, porque esto se aplica siempre que las IPs sean Fijas.

Por lo tanto, en redes grandes es preferible usar otro método: el DHCP snooping. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC que están conectadas a cada puerto, de modo que rápidamente detecta si se recibe una suplantación ARP. Este método es implementado en el equipamiento de red de fabricantes como Cisco, Extreme Networks y Allied Telesis.

Otra forma de defenderse contra el ARP Spoofing, es detectarlo. Arpwatch es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía email al administrador de la red, cuando una entrada ARP cambia.

Comprobar la existencia de direcciones MAC clonadas (correspondientes a distintas direcciones IP) puede ser también un indicio de la presencia de ARP Spoofing, aunque hay que tener en cuenta, que hay usos legítimos de la clonación de direcciones MAC.

RARP (“Reverse ARP”, o ARP inverso) es el protocolo usado para consultar, a partir de una dirección MAC, su dirección IP correspondiente. Si ante una consulta, RARP devuelve más de una dirección IP, significa que esa dirección MAC ha sido clonada.

3.1.5.5 Cómo evitar el Spoofing

La mayoría de estas soluciones se encuentran en los mismos dispositivos que se utilizan para el manejo de la red, estos son:

1. Utilizar la autentificación basada en el intercambio de claves entre las máquinas en la red; el uso de IPsec o RADIUS, por ejemplo, reducirá drásticamente en el riesgo de spoofing.
2. Utilizar ACLs (Access Control Listo o listas de control de acceso) para negar tráfico de direcciones IP privadas (no confiables) en tu interfaz en sentido descendente.
3. Poner en producción filtrado del tráfico de entrada y de salida del interface.
4. Configurar switches y routers para que denieguen tráfico dentro de la red que debería originarse fuera y viceversa.
5. Permitir el acceso hacia servidores locales desde máquinas externas confiables mediante sesiones cifradas establecidas contra los routers frontera de la LAN mediante VPNs

3.1.5.6 Solución para la Denegación de Servicios

Los ataques de denegación de servicio causan que el servicio o programa deje de funcionar o impide que otros hagan uso de ese servicio o programa. Estos ataques pueden ser realizados al nivel de red enviando datagramas cuidadosamente preparados y malintencionados de tal forma que puedan causar que las conexiones de red fallen. También pueden realizarse a nivel de aplicación, donde órdenes cuidadosamente construidas se envían contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento. Impedir que el tráfico

de red sospechoso alcance sus máquinas y que lleguen órdenes y peticiones de programa sospechosos son las mejores formas de minimizar el riesgo de un ataque de denegación de servicio.
Los Firewalls resultan muy útiles para evitar o reducir los accesos no autorizados, los ataques de denegación de servicio a nivel de red, y los ataques de suplantación de identidad, ventajosamente la propuesta del Cisco ASA 5540 como frontera con un doble Firewall IPTABLE para proteger la intranet nos ofrecen las seguridades necesarias contra estas amenazas, la idea es configurarlo correctamente.

3.1.6 Seguridad en la WEB

Empresas de diversa índole ya usan la Internet para comunicarse y el problema principal que surgió es la confiabilidad en que lo que se está comunicando no sea visto por personas que puedan hacer mal uso de dicha información, la UNL tiene que estar consciente de la importancia hoy en día de realizar trámites y negociaciones a través de la Internet, pero así mismo está consciente de la importancia de las seguridades en esa comunicación; hoy en día muchas instituciones realizan compras a través del internet pero el principal talón de Aquiles si lo podemos llamar así es la inseguridad que causa dar un número de tarjeta de crédito para pagar una transacción o el simple hecho de dar información personal que solo quisiera que lea el destinatario real.
A raíz de todo esto surgieron tecnologías que persiguen mejorar la seguridad de todas estas comunicaciones.

3.1.6.1 Seguridad en la Transmisión

La seguridad de este tipo se basa en el hecho de poder encriptar los mensajes que se envían por la red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.
Para llevar a cabo esta seguridad se crearon diversos protocolos basados en esta idea:

- SSH: Usado exclusivamente en reemplazo de telnet.
- SSL: Usado principalmente en comunicaciones de hipertexto pero con posibilidad de uso en otros protocolos.
- TSL: Es del mismo estilo del anterior.
- HTTPS: Usado exclusivamente para comunicaciones de hipertexto

3.1.6.2 SSH (Secure Shell)

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota. Usa Criptografía para seguridad en los datos.
SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL. Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el SSHD.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave pública al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

3.1.6.3 SSL (Secure socket Layer) y TLS (Transport Layer Secure)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL es una capa por debajo de HTTP y tal como lo indica su nombre esta a nivel de socket por lo que permite ser usado no tan solo para proteger documentos de hipertexto sino también servicios como FTP, SMTP, TELNET entre otros.

La idea que persigue SSL es encriptar la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de encriptación. El protocolo TLS está basado en SSL y son similares en el modo de operar.

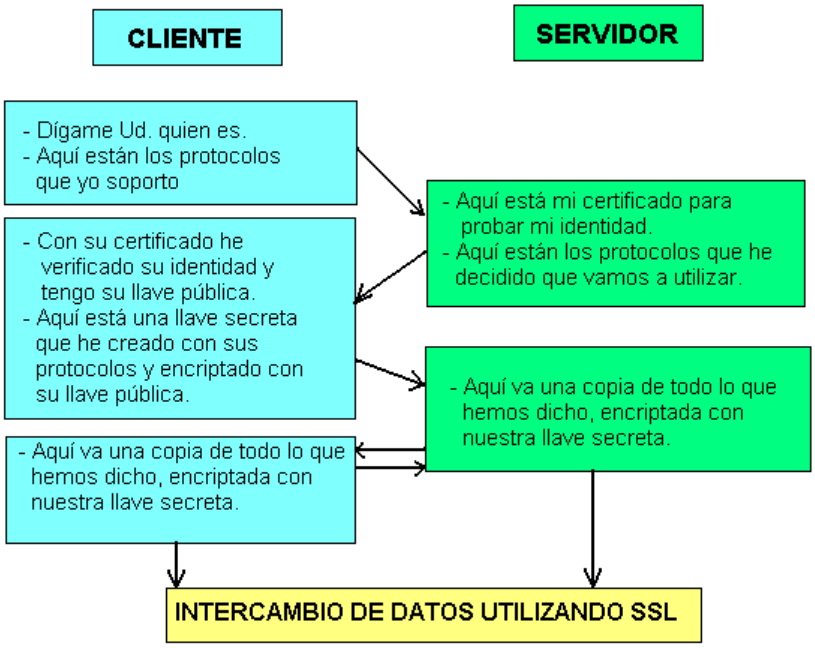


Fig. 35: Intercambio de datos utilizando SSL

3.1.6.4 OpenSSH y OpenSSL

En el caso de la propuesta que se está realizando en Seguridad Informática para la UNL, se maneja todo por Software Libre debido al no pago de licencias y a la disponibilidad del mismo.
Si vamos a utilizar OpenVPN para establecer enlaces seguros, es obvio que para manejar encriptación lo debemos realizar a través del protocolo OpenSSL.

3.1.6.5 GnuTLS (GNU Transport Layer Security Library)

Es una implementación de software libre de los protocolos SSL y TLS. Su propósito es ofrecer una Interfaz de programación de aplicaciones ó API (del inglés Application Programming

Interface) para aplicaciones que permite usar el protocolo de comunicaciones seguras sobre la capa de transporte de red.

3.1.7 Uso de Protocolos Seguros en Redes

La seguridad informática definitivamente es la parte fundamental para el buen manejo y flujo de la información, es ahí en donde en redes informáticas hablamos de protocolos en cada una de las capas del modelo TCP/IP que nos ayuden a manejar esa seguridad en la UNL. Protocolos que nos ofrecen seguridad y que incluyen servicios de: Manejo de claves, Confidencialidad, Privacidad, No Repudio, Integridad, autenticación y autorización. A continuación se presenta una tabla con protocolos seguros que trabajan en los diferentes niveles del modelo TCP/IP.

NIVELES	VENTAJAS	DESVENTAJAS	PROTOCOLOS
APLICACIÓN	Se puede extender la aplicación para brindar servicios de seguridad sin tener que depender del S.O	los mecanismos de seguridad deben ser diseñados para cada aplicación	Kerberos, PGP,SSH,OpenSSH S/MIME,SET, IPSec(ISAKMP),RADIUS, TACACS, OpenVPN
	Facilita el servicio no repudio.	Mayores probabilidades de	

		cometer errores	
TRANSPORTE	No se requieren modificaciones por aplicación.	Mantener el contexto del usuario es complicado	SSL, TSL, OpenSSL
		TLS requiere modificar las aplicaciones	
RED	Disminuye el flujo excesivo de negociación de claves	Dificil de manejar el no repudio	IPSec (AH,ESP), NLSP, PPTP,L2TP, OpenVPN
	Las aplicaciones no requieren modificación alguna		
	Permite crear VPNs e intranets.		
ENLACE DE DATOS	Más rápido	No son soluciones confiables	ATM, SILS, CHAP, PAP,MSCHAP, EAP,LEAP,PEAP
		Funcionan bien en enlaces dedicados	
		Deben tener	

		conexión física	

Tabla 6: Protocolos en los niveles OSI – TCP/IP[21]

[21] Seguridad del Centro de Datos de la Empresa Municipal ETAPA

FASE 4: REQUERIMIENTOS EN EQUIPAMIENTO

4.1 CARACTERÍSTICAS Y COSTO DE LOS EQUIPOS UTILIZADOS PARA EL MANEJO DE LA SEGURIDAD INFORMÁTICA DESDE EL DATA CENTER DE LA UNL.

En este punto se detallará las características de los equipos que considero se deben implementar en el Data Center de la Universidad Nacional de Loja para que brindar la seguridad requerida.

4.1.1 Firewall HW

CISCO ASA5540-AIP20-K9 		
CANTIDAD	MODELO	PRECIO
2	CISCO ASA 5540 IPS Edition Bundle – security appliance – with Cisco Advanced Inspection and Prevention Security Series Module 20 (AIP – SSM - 20).	$ 16.995.00
TOTAL		**$ 33.990.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Dimensions	1.75" Height x 17.50" Width x 13.20"	

	Depth
Firewall Protection	Intrusion Prevention Antivirus Worm Scanning Access Control Malware Protection
Flash Memory	128 MB
Input Voltage	110 V AC 220 V AC
License Type	ASA 5500 Encryption License ASA 5500 VPN Base License VMS 5 Device Basic License
Interfaces/Ports	4 x RJ-45 10/100/1000Base-T 1 x RJ-45 10/100Base-TX 2 x USB USB 2.0 1 x RJ-45 Console Management 1 x RJ-45 Auxiliary Management
Power Source	Power Supply
Standard Memory	1 GB
Virtualization	500 IPSec VPN Peer 500 Web VPN Peer 280000 Concurrent Session 20000 Concurrent Session 100 2 Security Context 50 Security Context
Form Factor	Rack-mountable
Number of Ports	5
Software Included	ASA 5500 Series Software v7.0

	ASA 5500 Series AIP Software 5.0 for Security Service Module Cisco VPN Client Software
Processor	Intel Pentium 4 2 GHz
Certifications & Standards	USB 2.0 **IEEE:** IEEE 802.3 IEEE 802.3u IEEE 802.3ab IEEE 802.1q **Safety:** UL 1950 CSA C22.2 No. 950 EN 60950 IEC 60950 AS/NZS3260 TS001 **Electromagnetic Compatibility (EMC):** CE marking FCC Part 15 Class A AS/NZS 3548 Class A VCCI Class A EN55022 Class A CISPR22 Class A EN61000-3-2 EN61000-3-3
Status Indicators	**Front Panel LEDs:** Power Status Active

	VPN Flash **Rear Panel LEDs:** MGMT indicator LEDs Network interface LEDs
Frequency	47 Hz to 63 Hz
Management	Web-based management application Cisco Adaptive Security Device Manager
Temperature	32F (0C) to 104F (40C) Operating -13F (-25C) to 158F (70C) Non-operating
Standard Warranty	1 año

Tabla 7: Características y Costo del Firewall HW

4.1.2 Servidor para Firewall SW

IBM HS21 BLADE SERVER		
		
CANTIDAD	MODELO	PRECIO
2	IBM HS21 BLADE SERVER para chasis	$ 1.395.00
TOTAL		**$ 2.790.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Familia de Procesadores	Intel Xeon	

Procesador	Intel Dual-Core Xeon 5150
Bus del Sistema	1333 MHz
Caché	4MB
Capacidad del disco	160 GB
Memoria interna	2 GB
Puertos	2 RJ45
Peso	5400 g
Tamaño	Altura 245mm, Ancho 29mm y Profundidad 446mm
Cracteristica de red	Gigabit Ethernet
Adaptador de Memoria gráfica	16 MB
Sistemas Operativos que soporta	Microsoft Windows Server 2003 Enterprise 64-bit Extended, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Enterprise Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 Web Edition, Red Hat Enterprise Linux AS 4, Red Hat Enterprise Linux AS 4 for Intel x86/ AMD64/ EM64T,

	Red Hat Enterprise Linux ES 4 for Intel x86/ AMD64/ EM64T, Red Hat Enterprise Linux WS 4 for Intel x86/ AMD64/ EM64T, SuSE Linux Enterprise Server 9 for x86/AMD64/Intel EM64T

Tabla 8: Características y Costo del Firewall SW

4.1.3 Switch Core

CISCO CATALYST 4506-E		
		
CANTIDAD	MODELO	PRECIO
1	Cisco Catalyst 4506-E - Switch - 6U - rack-mountable WS-C4506-E	$ 25.580.00
TOTAL		**$ 25.580.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Tipo	Montable en bastidor 6U	
Dimensiones	Ancho 44cm, Profundidad 31.7cm, Altura 44.1cm	
Cantidad de puertos	24 puertos 10/100 Fast Ethernet	

	12 puertos 10/100/1000 Base - TX 10 puertos SFP
Velocidad de transferencia de datos	100 Mbps
Protocolo de Interconexión de datos	Ethernet, Fast Ethernet
Protocolo de direccionamiento	OSPF, RIP, IS-IS, BGP, EIGRP, IGMPv2. HSRP, IGMP, direccionamiento IP estático, IGMPv3
Características	Diseño Modular, Conmutación Layer 4, Conmutación Layer 3, Conmutación Layer 2, alimentación mediante Ethernet (PoE), Soporta ARP, soporta VLAN
Cumplimiento de normas	IEEE 802.3, IEEE802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE802.3af, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE802.1x, IEEE 802.1s
Método de Autenticación	SSH, RADIUS, TACACS+, SSH2
Fuente de alimentación	Redundante interna
Voltaje	CA 120/230 V (50/60Hz)
Temperatura máxima	40 ℃

Tabla 9: Características y Costo del Switch Core

4.1.4 Switch para Distribución

CATALYST 3560 SW 24 PTS 10 100 + 2 PTS SFP		
		
CANTIDAD	MODELO	PRECIO
5	CATALYST 3560 SW 24 PTS 10/100 + 2 PTS SFP, STANDARD IMAGE	$ 1.350.00
TOTAL		**$ 6.750.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Tipo	Switch Montable en bastidor	
Dimensiones	Ancho 40cm, Profundidad 55cm, Altura 23cm	
Información Técnica	Cisco Catalyst 3560 24 10/100 + 2 SFP Standard Image. Capacidad duplex, conmutación Layer 3, auto-sensor por dispositivo, Encaminamiento IP, soporte de DHCP, negociación automática, enlace ascendente automático, RIP básico y ruteo estático.	
Cantidad de puertos	24 Ethernet 10/100 2 SFP-based Gigabit Ethernet 1 RJ-45 Consola Gestión	
Velocidad de transferencia de datos	10/100 Mbps	

Protocolo de Interconexión de datos	Ethernet, Fast Ethernet
Protocolo de administración remota	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c
Protocolos	LACP, DHCP, DTP, PAgP, RSTP, HSRP, UDLD, RIP v1.0, RIP v2.0, PIM-SM, PIM-DM, DVMRP, STP, MSTP, ARP, TCP/IP, TACACS+, RADIUS, TFTP, NTP, SSH, SNMP, Telnet
Estándares que cumple	IEEE 802.3, IEEE 802.3U, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Fuente de alimentación	Integrada
Voltaje	100-240 VAC (autoranging), 1.3-0.8A, 50-60 Hz
Consumo	45W
Garantía	2 años

Tabla 10: Características y Costo del Switch de Distribución 24 p 10/100, 2p SFP

CISCO WS-C3560G-24TS-S +4 pts SFP		
CANTIDAD	MODELO	PRECIO
6	WS-C3560G-24TS-S 10/100/1000 + 4 PTS SFP Gigabit Ethernet	$ 3.550.00
TOTAL		**$ 21.300.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Tipo	Switch Montable en bastidor	
Dimensiones	4,39cm Altura x 44,45cm Anchura x 37,85cm Profundidad	
Cantidad de puertos	24 Ethernet 10/100/1000 3 SFP-based Gigabit Ethernet 1 RJ-45 Consola Gestión	
Velocidad de transferencia de datos	10/100/1000 Mbps Half/Full-duplex	
Protocolo de Interconexión de datos	Ethernet, Fast Ethernet	
Memoria	128MB DRAM 32MB Memoria Flash	
Protocolos	RIP, WCCP, LACP, DHCP, DTP, PAgP, RSTP, HSRP, UDLD, RIP v1.0, RIP v2.0, OSPF, IGRP, EIGRP, BGP v4, PIM-SM, PIM-DM, DVMRP, STP, MSTP, ARP,	

	TCP/IP, TACACS+, RADIUS, TFTP, NTP, SSH, SNMP, Telnet
Estándares que cumple	IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x, IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p Prioridades CoS, IEEE 802.1Q VLAN, IEEE 802.3 10BASE-T especificación, IEEE 802.3u 100BASE-TX especificación, IEEE 802.3ab 1000BASE-T especificación, IEEE 802.3z 1000BASE-X especificación
Fuente de alimentación	Integrada
Voltaje	100 V AC a 240 V AC Auto Rango, 50 Hz o 60 Hz
Consumo	50W máx 100W
Garantía	2 años

Tabla 11: Características y Costo del Switch de Distribución 24 p 10/100/1000, 4p SFP

4.1.5 Servidores para la Seguridad Informática

4.1.5.1 Servidor para OpenLDAP

IBM HS21 BLADE SERVER


CANTIDAD	MODELO	PRECIO
1	IBM HS21 BLADE SERVER para chasis	$ 1.890.00
TOTAL		**$ 1.890.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Familia de Procesadores	Intel Xeon	
Procesador	Intel Quad Core Xeon E5420, 2.5 GHz	
Bus del Sistema	1333 MHz	
Caché	12MB	
Capacidad del disco	160 GB	
Memoria interna	4 GB	
Puertos	2 RJ45	
Peso	5400 g	
Tamaño	Altura 245mm, Ancho 29mm y Profundidad 446mm	
Cracteristica de red	Ethernet, Fast Ethernet, Gigabit Ethernet	
Adaptador de Memoria gráfica	16 MB	
Sistemas Operativos que soporta	Microsoft Windows Server 2003 Enterprise 64-bit Extended, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Enterprise Edition, Microsoft Windows Server 2003 R2	

	Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 Web Edition, Red Hat Enterprise Linux AS 4, Red Hat Enterprise Linux AS 4 for Intel x86/ AMD64/ EM64T, Red Hat Enterprise Linux ES 4 for Intel x86/ AMD64/ EM64T, Red Hat Enterprise Linux WS 4 for Intel x86/ AMD64/ EM64T, SuSE Linux Enterprise Server 9 for x86/AMD64/Intel EM64T

Tabla 12: Servidor para OpenLDAP

4.1.5.2 Servidores para RADIUS Y OpenVPN

IBM HS21 BLADE SERVER		
		
CANTIDAD	MODELO	PRECIO
2	IBM HS21 BLADE SERVER para chasis	$ 1.395.00
TOTAL		**$ 2.790.00**
ESPECIFICACIONES	CARACTERÍSTICAS	
Familia de Procesadores	Intel Xeon	

Procesador	Intel Dual-Core Xeon 5150
Bus del Sistema	1333 MHz
Caché	4MB
Capacidad del disco	160 GB
Memoria interna	2 GB
Puertos	2 RJ45
Peso	5400 g
Tamaño	Altura 245mm, Ancho 29mm y Profundidad 446mm
Cracteristica de red	Gigabit Ethernet
Adaptador de Memoria gráfica	16 MB
Sistemas Operativos que soporta	Microsoft Windows Server 2003 Enterprise 64-bit Extended, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Enterprise Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 Web Edition, Red Hat Enterprise Linux AS 4, Red Hat Enterprise Linux AS 4 for Intel x86/ AMD64/ EM64T,

	Red Hat Enterprise Linux ES 4 for Intel x86/ AMD64/ EM64T, Red Hat Enterprise Linux WS 4 for Intel x86/ AMD64/ EM64T, SuSE Linux Enterprise Server 9 for x86/AMD64/Intel EM64T

Tabla 13: Servidor para RADIUS Y OpenVPN

4.1.5.3 Costo del Equipamiento

COSTO DEL EQUIPAMIENTO PARA LA SEGURIDAD INFORMÁTICA		
CANTIDAD	CARACTERÍSTICAS DEL EQUIPO	PRECIO
2	CISCO ASA 5540 IPS Edition Bundle – security appliance – with Cisco Advanced Inspection and Prevention Security Series Module 20 (AIP – SSM - 20).	$ 33.990.00
2	IBM HS21 BLADE SERVER para chasis	$ 2.790.00
1	Cisco Catalyst 4506-E - Switch - 6U - rack-mountable WS-C4506-E	$ 25.580.00
5	CATALYST 3560 SW 24 PTS 10/100 + 2 PTS SFP, STANDARD IMAGE	$ 6.750.00
6	WS-C3560G-24TS-S 10/100/1000 + 4 PTS SFP Gigabit Ethernet	$ 21.300.00

1	Servidor IBM HS21 BLADE SERVER para chasis	$ 1.890.00
2	Servidores IBM HS21 BLADE SERVER para chasis	$ 2.790.00
TOTAL		**$ 95.090.00**

Tabla 14: Costo del Equipamiento

FASE 5: DESARROLLO DEL MANUAL DE POLÍTICAS

5.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA MANEJADAS DESDE EL INSTITUTO DE INFORMÁTICA DE LA UNL.

5.1.1 SEGURIDAD ORGANIZACIONAL

5.1.1.1 POLÍTICAS GENERALES DE SEGURIDAD

Estas políticas son establecidas basándose en la Norma ISO/IEC 27000 - Tecnología de la Información – Técnicas de Seguridad – La Seguridad de la Información de Gestión de Sistemas – Fundamentos y Vocabulario, específicamente en el conjunto de normas ISO/IEC 27001 - ISO/IEC 27006 incluida también la ISO/IEC 27033: Tecnología de la información – Técnicas de Seguridad - Seguridad en Redes.

Del Departamento de Redes del Instituto de Informática.

Art. 1. Normar el correcto uso de los servicios de Internet y correo electrónico en la UNL.
Art. 2. Establecer las medidas y mecanismos de control, monitoreo y seguridad, tanto para los accesos a páginas o sitios de Internet, como para los mensajes de correo con contenidos u orígenes sospechosos.
Art. 3. Que las conexiones a Internet cuenten con elementos de prevención, detección de intrusos, filtros contra virus, manejo de contenidos, entre otros, que afectan la integridad de los sistemas y la información institucionales.

Art. 4. Reducir el tráfico de mensajes, paquetes o transacciones no permitidos, que saturan la infraestructura de telecomunicaciones y generan actividad innecesaria en los servidores.

Art. 5. De acuerdo a la demanda de servicios, establecer prioridades, dando la más alta a las actividades consideradas esenciales para fomentar la educación y la investigación, objetivo primordial de la UNL.

Art. 6. Controlar, suspender o revocar los códigos de acceso a cualquier usuario que haga mal uso de los recursos, viole las políticas de seguridad o interfiera con los derechos de otros usuarios.

Art. 7. Contratar enlaces o servicios de conectividad a Internet, vía terceros, por lo que queda restringido a cualquier otra área de la Institución obtener y utilizar enlaces y servicios que permitan la interconexión de las redes de la UNL hacia el exterior. El Instituto de Informática a través del departamento de Redes es la única autorizada dentro de la UNL para realizar o autorizar ese tipo de contrataciones, esto podrá hacerlo atendiendo a necesidades especiales por cuenta de las áreas, certificando la incorporación de las medidas de control y seguridad en los enlaces.

Art. 8. Establecer las normas de construcción y arquitectura de los sitios de Intranet, que optimicen el acceso a los servicios y la información disponible para los usuarios.

Art. 9. Administrar y asignar todas las direcciones IP de la UNL, así como los dominios asignados a la misma.

Art. 10. Establecer las medidas y mecanismos de Seguridad para el ingreso al Data Center de la UNL.

Art. 11. Velar por el buen funcionamiento de los equipos que se encuentran en el Data Center.

De los administradores de red.

Art. 1. Configurar los servidores, tanto de la intranet como los públicos.
Art. 2. Instalar y actualizar los antivirus y sistemas operativos, así como tener al día en los en servidores asignados, las actualizaciones y Parches de programas institucionales licenciados y autorizados.
Art. 3. Llevar un registro y control de las direcciones IP de los equipos conectados a la red con acceso a Internet y la información de los usuarios, así como notificar al Departamento de Redes de las altas y bajas de usuarios para los servicios de correo electrónico e Internet.
Art. 4. Proporcionar al Departamento de Redes la documentación actualizada de la red local: planos de cableado, ubicación del equipo y relación de las asignaciones de direcciones IP.
Art. 5. Administrar los servicios locales de red como son www, correo electrónico, servidor de FTP y servidores de aplicaciones en red.
Art. 6. Solucionar fallas menores como son: cables desconectados, pérdida de suministro de energía eléctrica en los equipos de datos, desconfiguración de las computadoras de los usuarios o direcciones IP repetidas.
Art. 7. Monitorear el tráfico de la red y presentar informes del mismo al Departamento de Redes.

Art. 8. Supervisar el cumplimiento de las políticas y lineamientos institucionales.

Del Departamento de Soporte Técnico.

Art. 1. Brindar mantenimiento preventivo y/o correctivo únicamente al equipo que cuente con número de inventario, o se encuentre en comodato, debiendo en este último caso enviar al Instituto de Informática una copia del contrato correspondiente.
Art. 2. Realizar respaldos diarios de la información contenida en los servidores del Instituto.

Del Personal.

Art. 1. El empleado no tiene ningún derecho sobre la información que procese dentro de las instalaciones de la red institucional de la UNL.
Art. 2. La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito laboral.
Art. 3. El usuario se norma por las disposiciones de seguridad informática que propone el Instituto de Informática.
Art. 4. Conocer y obedecer las políticas de seguridad establecidas en el presente documento, las cuales, una vez aprobadas se publicarán para su divulgación en la página institucional de la UNL (www.unl.edu.ec).

Capacitación de usuarios.

Art. 1. El Instituto de Informática a través del Departamento de Redes capacitará a los usuarios informáticos en cuestiones de seguridad informática, basándose en lo establecido en el presente documento.
Art. 2. El Instituto de Informática proporcionará las fechas en que se impartirán las capacitaciones.
Art. 3. El material de apoyo (manuales, guías, etc.) será entregado minutos antes de iniciar la capacitación.

5.1.1.2 CLASIFICACIÓN Y CONTROL DE ACTIVOS

Responsabilidad por los activos.

Art. 1. Los titulares y administradores de los centros de trabajo de la UNL, son responsables de los activos que se encuentran bajo su resguardo.
Art. 2. Los jefes de cada departamento de la UNL, son responsables de mantener o proteger los activos de mayor importancia.

Clasificación de la información.

Art. 1. Cada jefe de departamento dará importancia a la información en base al nivel de clasificación que demande el activo.
Art. 2. La información pública puede ser visualizada por cualquier persona dentro o fuera de la institución

Art. 3. La información confidencial es propiedad absoluta de la UNL, el acceso a ésta es permitido únicamente a personal autorizado.

Art. 4. Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

Art. 5. El Instituto de Informática tendrá la responsabilidad de priorizar una situación de la otra en cuanto a los problemas en las estaciones de trabajo.

Art. 6. El Instituto de Informática implementará un Plan de Contingencia que indique claramente, qué hacer en caso de presentarse una situación extraordinaria en la parte Informática.

Art. 7. En situaciones de emergencia que impliquen áreas de atención al usuario entre otros, se dará prioridad en el siguiente orden:

a) Área financiera y de personal
b) Área educativa y de investigación
c) Área administrativa

Art. 8. El Plan de Contingencia se elaborará tomando en cuenta aspectos basados en situaciones pasadas, y enmarcarlo en la pro actividad de situaciones futuras.

5.1.1.3 RESPUESTA A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

Art. 1. Los respaldos de información deberán ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la institución.

Art. 2. Los respaldos se utilizarán únicamente en casos especiales, ya que su contenido es de suma importancia para la institución.
Art. 3. El Instituto de Informática debe contar con respaldos de información importante que manejen los servidores ante cualquier incidente.

5.1.2 SEGURIDAD LEGAL

5.1.2.1 DERECHOS DE PROPIEDAD INTELECTUAL

Art. 1. La UNL se reserva el derecho de respaldo, a usuarios académicos, administrativos o trabajadores ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.
Art. 2. Todo el software comercial que utilice la UNL, deberá estar legalmente registrado en los contratos de arrendamiento o adquisición, con sus respectivas licencias y facturas de compra.
Art. 3. La adquisición de software por parte del personal que labore en la UNL, no expresa el consentimiento de la institución, la instalación del mismo, no garantiza responsabilidad alguna para la UNL, por ende la institución no se hace responsable de las actividades de sus empleados.
Art. 4. Todo el software que se desarrolle en el Departamento de Software del Instituto de Informática será propiedad exclusiva de la UNL.
Art. 5. El software comercial licenciado adquirido por la UNL, es propiedad exclusiva de la institución.

Art. 6. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.
Art. 7. Los contratos con terceros en la gestión o prestación de un servicio, deberán especificar las medidas necesarias de seguridad, nivel de prestación del servicio y/o personal involucrado en tal proceso.
Art. 8. La adquisición del software comercial o libre, deberá ser gestionada con las autoridades correspondientes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

5.1.2.2 REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO

Art. 1. La DSI, podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado, será reportado conforme a lo indicado en las Políticas de Seguridad.

5.1.3 SEGURIDAD LÓGICA

5.1.3.1 CONTROL DEL ACCESO A USUARIOS DE LA RED DE DATOS DE LA UNL

Art. 1. La documentación de seguridad será resguardada por el Departamento de Redes, esto incluye folletos, guías, formularios, controles, etc.
Art. 2. La elaboración de la documentación relacionada con formularios, guías, etc., será elaborada por el Departamento de Redes.
Art. 3. El personal encargado de brindar los servicios de comunicaciones, no está autorizado a brindar ninguna clase de servicios, mientras no se haya seguido el procedimiento establecido para ello.

5.1.3.2 ADMINISTRACIÓN DEL ACCESO A USUARIOS A LOS SERVICIOS INFORMÁTICOS DE LA UNL

Art. 1. El acceso a los sistemas y servicios de información es permitido únicamente a los usuarios que dispongan de los permisos necesarios para su ejecución para ello tendrán que utilizarse servicios de autenticación.
Art. 2. El usuario deberá proveer toda la información necesaria para poder brindarle los permisos necesarios para la ejecución de los servicios de la red institucional de la UNL.
Art. 3. Se brindará a los usuarios el acceso a los servicios de correo electrónico e Internet de la UNL, siempre que cumplan con el procedimiento establecido.
Art. 4. El usuario de correo electrónico e Internet, deberá limitarse a atender los requerimientos de la Institución, en el desempeño de las funciones encomendadas a su puesto y apegándose a la normatividad establecida.
Art. 5. Las claves de acceso son personales e intransferibles

Art. 6. Las contraseñas o password asignados a los usuarios, deberán ser de 6 caracteres como mínimo y 8 como máximo, debiendo combinarlo con una letra mayúscula al inicio y un carácter especial al final.

Art. 7. La contraseña (password) de acceso, es de exclusiva responsabilidad del usuario a quien se le otorgó, por lo que no deberá publicarlo o tenerlo en lugar visible para que otra persona lo pueda manipular o hacer mal uso del equipo o información.

Art. 8. Es responsabilidad del usuario cambiar periódicamente su contraseña, de acuerdo a la criticidad de la información, procurando no reutilizar las últimas 4 contraseñas. En caso de no saber cómo realizar el cambio, el Departamento de Redes le brindará la asesoría necesaria.

Art. 9. El usuario es responsable de no dejar sesiones activas en su estación de trabajo cuando se ausente de su escritorio o sitio de trabajo. Por lo cual, es recomendable que una vez concluida su jornada laboral, apague su equipo para evitar que personas no autorizadas tengan acceso a él.

Art. 10. Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor, y en todo caso, deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra Institución.

Art. 11. En caso de necesitar bajar archivos o imágenes de la red, éstos deberán ser de un tamaño pequeño, a fin de no causar mucho tráfico y por consiguiente lentitud para los demás usuarios.

Art. 12. Deberá bajar periódicamente la información del servidor de correos a su equipo asignado para liberar la capacidad del servidor de correos.
Art. 13. Respetar los derechos de otras personas, tanto de propiedad intelectual como de equipo.
Art. 14. Deberá utilizar únicamente la cuenta que le ha sido asignada para tener acceso a sistemas y recursos.
Art. 15. Evitar el envío de archivos confidenciales a través del correo electrónico a menos que se utilicen técnicas de criptografía.

Normativa del uso de correo electrónico.

Art. 1. El Departamento de Redes es la única instancia facultada para autorizar el servicio de acceso a internet y correo electrónico.
Art. 2. El Departamento de Redes asignará y/o renovará claves de acceso a correo electrónico e Internet, de acuerdo con el procedimiento establecido y comprometiendo al usuario a cumplir con los lineamientos.
Art. 3. Se asignarán cuentas de correo electrónico por departamento, creándose la cuenta con las iniciales del mismo. Ejem. drii@unl.edu.ec
Art. 4. Las cuentas personales se asignarán únicamente con el Visto Bueno del Titular del Centro de Trabajo.
Art. 5. Queda prohibido enviar información por correo electrónico, cuentas FTP, o cualquier medio electrónico, clasificada como confidencial o que sin serlo, el usuario no tenga atribuciones que permitan su uso y divulgación, atenten contra los derechos de autor, sea falsa, difamatoria u ofensiva.

Art. 6. Queda prohibido el uso de seudónimos y envío de mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
Art. 7. Queda prohibido el envío interno o hacia el exterior, de correos *spam* de cualquier índole. Se consideran correos *spam* aquellos no relacionados con las funciones específicas a los procesos de trabajo.
Art. 8. Se realizará un monitoreo periódico sobre el uso de los correos, a fin de dar de baja aquellas cuentas que no sean utilizadas. Adicionalmente a esto, se llevará a cabo una depuración de forma semestral.
Art. 9. Es responsabilidad del titular de Centro de Trabajo que firma la solicitud, comunicar al Departamento de Redes cualquier circunstancia que implique la necesidad de eliminar el acceso solicitado o de modificarlo, ya sea porque el usuario deje de pertenecer a su área, se ausente por comisión, licencia o incapacidad, o por el mal uso que se haga del servicio.

Usos aceptables de los servicios de Internet.

Art. 1. La comunicación entre académicos y personas relacionadas con labores administrativas, siempre y cuando exista un intercambio mutuo y en condiciones recíprocas.
Art. 2. Comunicación e intercambio con la comunidad académica de otras instituciones, con el fin de tener acceso a los últimos avances relacionados con la especialidad del personal.

Acceso a sitios y contenidos no autorizados.

Art. 1. Esta totalmente prohibido cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

Art. 2. Para garantizar la seguridad de la información y el equipo informático, el Departamento de Redes establecerá filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad; por lo tanto, se prohíbe:

- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, o interferir con el trabajo de los demás, provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de la UNL.
- Utilizar los recursos de la UNL para el acceso no autorizado a redes y sistemas remotos.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas.
- Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja los derechos de los demás.
- Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.

- Utilizar los servicios de red para ver publicaciones de pornografía.
- Utilizar los servicios de red para enviar archivos que sean confidenciales.
- Utilizar los servicios para accesar a páginas de radio o TV en línea y de videos como YouTube.
- Los servicios bancarios y servicios personales que se ofrecen vía Internet, podrán utilizarse en forma mesurada.

5.1.3.3 CONTROL DE ACCESO A LA RED

Art. 1. El Departamento de Redes diseñará los mecanismos necesarios para proveer acceso a los servicios de la red institucional de la UNL.

Art. 2. Los mecanismos de autenticación y permisos de acceso a la red, deberán ser evaluados y aprobados por el Departamento de Redes.

Art. 3. El Departamento de Redes, hará evaluaciones periódicas a los sistemas de red, con el objetivo de eliminar cuentas de acceso sin protección de seguridad y componentes de red comprometidos.

Art. 4. El Departamento de Redes, verificará que el tráfico de red sea estrictamente normal, la variación de este sin ninguna razón obvia, pondrá en marcha técnicas de análisis concretas.

Art. 5. Se utilizarán mecanismos y protocolos de autenticación como claves privadas, autenticación usuario/contraseña.

Art. 6. Los dispositivos de red, estarán siempre activos y configurados correctamente para evitar anomalías en el tráfico y seguridad de información de la red institucional.

5.1.3.4 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Art.1. Para prevenir contaminaciones por virus informático, los usuarios de la UNL sólo utilizarán el software que haya sido valorado y asignado por el Instituto de Informática.

Art. 2. Los usuarios de equipo de cómputo de la UNL, deberán verificar que la información y los medios de almacenamiento, considerando al menos discos flexibles, CDs, Flash, Discos Externos, etc; estén libres de cualquier tipo de código malicioso, para lo cual deberán ejecutar el software antivirus autorizado e instalado por el Instituto de Informática.

Art. 3. Todos los archivos de computadora que sean proporcionados por personal interno o externo, considerando bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, deberá verificarse que no contenga ningún tipo de virus antes de su ejecución.

Art. 4. Ninguna persona de la UNL, deberá intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Menos aún, probarlos en cualquiera de los ambientes o plataformas de la UNL.

Art. 5. Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la previa autorización del Instituto de Informática.

Art.6. Cualquier usuario que sospeche de alguna infección por virus en su equipo de cómputo, deberá notificarlo

inmediatamente al Departamento de Soporte Técnico del Instituto de Informática para su erradicación.

Art. 7. Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Instituto de Informática en: antivirus, *outlook, office*, navegadores u otros programas.

CONCLUSIONES

- Para brindar seguridad informática desde el nuevo Data Center de la Universidad Nacional de Loja, se debe pensar en un cambio de la infraestructura física y lógica que opera actualmente, para ello se debe concientizar a las autoridades de la importancia de conseguir recursos para proyectos de este tipo, que garanticen el mejoramiento en el acceso a la información.

- Dentro del Análisis de la Situación Actual me di cuenta que el personal de los centros de cómputo y encargados de las redes, no son profesionales de la rama de la Informática, por lo que muy poco se aporta para el mejoramiento en la seguridad informática y lo que se aporta es por conocimientos de auto aprendizaje o empíricos de los encargados.

- El Data Center que maneja actualmente la Universidad Nacional de Loja carece totalmente de una adecuada infraestructura que garantice la puesta en marcha de un plan de mejoramiento de la seguridad física y lógica.

- Para el manejo de la seguridad informática en la UNL se debe recurrir a la aplicación de normas, como la ISO/IEC 27000 reconocidas internacionalmente y que muchas organizaciones a nivel mundial hacen uso de ella.

- Para brindar mayor seguridad a la intranet se debe utilizar doble Firewall uno externo y otro interno, procurando utilizar

de diferentes fabricantes si es HW o combinar HW con SW para hacerle más difícil al intruso el acceso a la red.

- Es importante que en el nuevo Data Center de la UNL se maneje redundancia en zonas críticas como Cortafuegos, debido a la importancia que este genera para el acceso a la información.

- Es una buena alternativa por cuestiones de costos utilizar herramientas y protocolos Open Source para brindar seguridad informática como: OpenVPN, IPTable, OpenSSH, OpenSSL, Squid, Dansguardian.

- Una solución adecuada y a bajo costo es la utilización de un servidor RADIUS y un OpenLDAP para el manejo de autenticación y autorización al ingreso a los servicios de la red institucional.

- La Utilización de dispositivos o equipos para ofrecer seguridad informática no es suficiente, esta debe ir acompañada de un monitoreo permanente del administrador de la red y de la aplicación de las políticas en seguridad informática que ponga en vigencia la institución.

RECOMENDACIONES

- La Universidad Nacional de Loja debe incluir dentro de sus políticas institucionales la seguridad informática aplicando normas internacionales debidamente probadas y certificadas para su utilización.

- Para el manejo de la Seguridad Informática en la UNL se debe establecer un grupo de talentos humanos capacitados para implementar esta propuesta y otras propuestas más que puedan dar solución a problemas en cuanto al acceso a la información se refiere.

- La Universidad Nacional de Loja debería dar mayor importancia al mejoramiento de los servicios informáticos en la institución, adquiriendo equipos adecuados para el manejo de los mismos, tomando en cuenta la propuesta realizada.

- Se debe desarrollar un plan de mejora de la seguridad Informática y de la Información, el mismo que dé cómo resultado un manual de políticas aplicando la Norma ISO/IEC 27000 la cual propone el manejo de Tecnología de la Información, Técnicas de Seguridad, La Seguridad de la Información de Gestión de Sistemas utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

- Se debe establecer un plan de capacitación y concientización de todos los miembros de la institución (Docentes, Administrativos, Trabajadores y Alumnos), de la importancia de cumplir con las políticas establecidas en

Seguridad Informática y de las Sanciones impuestas al incumplirlas.

- El Departamento de Redes del Instituto de Informática debería implementar un esquema para la Asignación dinámica de VLANs para los usuarios de la red, lo que garantizará acceder a los servicios basados en su perfil de usuario en cualquier equipo de la red ingresando sus credenciales.

- La utilización de herramientas y protocolos de software libre para establecer seguridad informática es una buena alternativa para el caso de instituciones que dependen del estado para la asignación de presupuesto para sus proyectos.

- La UNL tendría que migrar la red principal a fibra óptica así como lo plantea esta propuesta y todo el cableado a Cat6, con ello evitaremos la utilización de transceiver y tendríamos a estos dispositivos y a los que posee cada área para enlace inalámbrico, como redundancia o respaldo en caso suceda alguna eventualidad con la red principal.

BIBLIOGRAFÍA

Seguridad Informática http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, actualizado a Mayo 2008.

Monografías, Evaluación Seguridad de un Sistema de Información, www.monografia.com/trabajos/seguinfo/seguinfo.shtml, actualizado a 2006.

Libros networking, Mis libros de networking: 10 pasos para asegurar un dispositivo CISCO IOS, http://librosnetworking.blogspot.com/, actualizado a marzo 24 2006.

Norma ISO-IRAM-IEC 17799, http://seginfo.tripod.com/files/17799a.pdf, actualizado a Julio 2009

Norma ISO-IRAM-IEC 17799, http://es.wikipedia.org/wiki/Iso_17799, Información de toda la norma, actualizado a Septiembre 2008.

Resumen de toda la Norma ISO/IEC 27000 - Tecnología de la Información – Técnicas de Seguridad – La Seguridad de la Información de Gestión de Sistemas – Fundamentos y Vocabulario, http://www.iso27000.es, http://blog.tataki.es/2008/05/29/iso-27000-introduccion-y-estado-actual.

Conceptos Generales de los Centros de Procesamiento de Datos, http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos, http://es.wikipedia.org/wiki/Centro_de_respaldo

Cisco, Security Considerations for the Intranet Data Center, http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/ns376/networking_solutions_package.html, actualizado a Marzo 2006.

Cisco, Data Center Security Topologies, http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/ns376/networking_solutions_package.html, actualizado a Marzo 2006.

Gestión de Riesgo en la Seguridad Informática, Análisis y Clasificación del Riesgo, http://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Tipos de Ataques e Intrusos en las Redes Informáticas, **Alvaro Gómez Vieites,** Profesor de la Escuela de Negocios Caixanova, http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

Información sobre la Zona Desmilitarizada, cual es su estructura, http://www.solusan.com/que-es-una-dmz.html

Información sobre el Protocolo Autenticación, Autorización y Contabilización, Características, Lista de protocolos AAA, http://es.wikipedia.org/wiki/Protocolo_AAA

Información sobre el protocolo RADIUS, Características, Historia y Estándares que utiliza, http://es.wikipedia.org/wiki/RADIUS

Información acerca de las Listas de Control de Acceso, Caracteristicas, http://es.wikipedia.org/wiki/Lista_de_control_de_acceso, http://www.dsi.uclm.es/asignaturas/42550/PDFs/PRACTICA4.pdf

Empresa que tiene la patente para dar Certificados Digitales en algunos países de Suramérica incluido el Ecuador, http://www.verisign.com/mx/affiliate/index.html

Características de equipamiento, Firewall ASA 5540, Switch 3560, http://www.cisco.com/

Metodología para el Desarrollo de políticas y Procedimientos en Seguridad Informática, http://www.monografias.com/trabajos11/seguin/seguin.shtml, Diciembre 2006

GLOSARIO DE TÉRMINOS

IRAM: Instituto Argentino de Normalización y Certificación

ISO: Organización internacional para la Estandarización

SGSI: Sistema de Gestión de la Seguridad de la Información

ARP: (Address Resolution Protocol) Protocolo de Resolución de Dirección

ICMP: (Internet Control Message Protocol) Protocolo de Mensajes de Control de Internet

SMTP: (Simple Mail Transfer Protocol) Protocolo Simple de Transferencia de Correo

ISP: (**I**nternet **S**ervice **P**rovider) Proveedor de Servicios de Internet

PPP: (Point-to-point Protocol) Protocolo Punto a Punto

AAA: (**A**uthentication, **A**uthorization and **A**ccounting) Autenticación, Autorización y Contabilización o Auditoría

DSL: (***D****igital* ***S****ubscriber* ***L****ine*)Linea de Abonado Digital

ADSL: (***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*) Línea de Abonado Digital Asimétrica

PAP: (Password Authentication Protocol) Protocolo de Autenticación mediante Contraseña

EAP: (Extensible Authentication Protocol) Protocolo de Autenticación Extensible

ACL: (Access Control List) Lista de Control de Acceso

VLAN: (Virtual Local Area Network) Red de Área Local Virtual

ARP: (**A**ddress **R**esolution **P**rotocol) Protocolo de Resolución de Dirección

VPN: (**V**irtual **P**rivate **P**etwork) Red Privada Virtual

MD2: (Algoritmo de Resumen del Mensaje 2) El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el ordenador (128 bits o 16 bytes) y añadiéndole un checksum.

MD5: (Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

SHA: (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas.

DES: (Data Encryption Standard) es un algoritmo de cifrado, es decir, un método para cifrar información.

3DES: Hace triple cifrado del DES.

AES: (Advanced Encryption Standard), también conocido como Rijndael, es un esquema de cifrado por bloques

DHCP: (Dynamíc Host Confíguration Protocol) Protocolo de Configuración de Host Dinámico

RADIUS: (Remove Authentication Dial In User Service) protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP

IDS: (Intrusion Detection System) Sistema de Detección de Intrusos

SSH: (**S**ecure **SH**ell) Interprete de Ordenes Segura

SSL: (**Secure Sockets Layer**) Protocolo de Capa de Conexión Segura

TLS: (**Transport Layer Security**) Seguridad de la Capa de Transporte

LDAP: (*Lightweight Directory Access Protocol*) Protocolo Ligero de Acceso a Directorios

IPsec : (**Internet Protocol security**) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

EAP: (**Extensible Authentication Protocol**) Protocolo de Autenticación Extensible

ANEXOS

ANEXO 1

Análisis de los resultados obtenidos en las encuestas realizadas a los responsables de los centros de cómputo de la Universidad Nacional de Loja

Aquí se planteó una encuesta acerca de la seguridad informática aplicada al personal de los centros de cómputo de las siguientes Áreas y Departamento:

- Jefatura de Informática
- Área de Energía, Industrias y Recursos Naturales no Renovables
- Área Jurídica, Social y Administrativa
- Área Agropecuaria y de Recursos Naturales Renovables
- Área de la Educación, el Arte y la Comunicación
- Área de la Salud Humana

Obteniendo los siguientes resultados:

1. **¿Cree usted que la seguridad informática en una institución es vital para el resguardo de la información de la misma?**

ALTERNATIVAS	FRECUENCIA	%
Si	10	100
No	0	0
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 100% de los encuestados dicen que la seguridad informática es vital para el reguardo de la información, por lo tanto están consientes de eso.

2. ¿Desde dónde cree usted que se debe realizar el manejo de la seguridad informática?

ALTERNATIVAS	FRECUENCIA	%
Los Centros de Cómputo	2	20
Jefatura Informática	1	10
Data Center	6	60
No se tiene específico	1	10
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 60% de los encuestados dicen que el manejo de la seguridad informática se la debe hacer desde un Data Center, el 20% manifiesta que desde los centros de cómputo, el 10% dice que desde la jefatura de informática y un 10% restante manifiesta que no se tiene específico desde donde se maneja.

3. ¿De quién depende la responsabilidad de la seguridad informática en la Institución?

ALTERNATIVAS	FRECUENCIA	%
Auditoría Interna	0	0
Jefatura Informática	9	90
Departamento de Finanzas	0	0
No se tiene específico formalmente	1	10
TOTAL	**10**	**100**

De esta pregunta se puede concluir que el 90% de los encuestados dicen que la responsabilidad de la seguridad informática en la Institución recae en la jefatura Informática y que el 10% restante no tienen específico formalmente. Ninguno de los encuestados responde que el manejo de la seguridad informática en la Institución este dada por auditoría Interna y por el Departamento de finanzas

4. **¿El presupuesto de la Institución incluye aspectos de seguridad informática?**

ALTERNATIVAS	FRECUENCIA	%
Si	1	10
No	9	90
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 90% de los encuestados dicen que el presupuesto de la Institución no incluye aspectos de seguridad informática y el 10% restante dicen que si incluye.

5. **¿En qué se centra la seguridad informática en la Institución? (Elija todas las que se apliquen).**

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Protección de la red	7	26,92
Protección de los datos críticos de la Institución	8	30,77
Proteger los datos de los estudiantes	6	23,07
Desarrollo y afinamiento de seguridad de las aplicaciones	4	15,38
Otras	1	3,85
TOTAL	**26**	**100**

De lo anterior se puede concluir que el 30.77% de los encuestados opina que la seguridad informática se centra en la protección de los datos críticos de la institución, el 26.92% responde la seguridad informática se centra en la protección de la red, el 23.07% restante contesta que la seguridad informática se centra en proteger los datos de los estudiantes, el 15.30% contesta que la seguridad informática se centra en el desarrollo y afinamiento de seguridad de las aplicaciones y el 3,85% opina que existen otros campos en los cuales se debe centrar la seguridad informática como:

- Protección de contenidos

6. ¿Qué casos de violación de seguridad tuvieron lugar en la Institución? (Elija todas las respuestas aplicables).

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Manipulación de aplicaciones de Software	0	0
Accesos no Autorizados	5	20,8
Virus	9	37,5
Robo de datos	1	4,16
Monitoreo no autorizado de tráfico	3	12,5
Negación del Servicio	5	20,8
Pérdida de Integridad	1	4,16
Pérdida de Información	0	0
Ninguno	0	0
Otros	0	0
TOTAL	**24**	**100**

De lo anterior se puede concluir que el 37.5% de los encuestados opina que las violaciones de seguridad se deben a los Virus, el 20.8% responde que las violaciones de seguridad se deben a accesos no autorizados, el 20.8% contesta que se deben a la negación del servicio, el 12.5% dice se debe al monitoreo no autorizado del tráfico, el 4.16% considera que se deben al robo de datos, el 4.16% piensa que se deben a la pérdida de la Integridad. Ninguno de los encuestados responde que las violaciones de seguridad se deben a la manipulación de aplicación de software, a la pérdida de la información, ninguna y otra.

7. ¿Cuántas intrusiones o incidentes de seguridad identifico en promedio durante el periodo anterior?

ALTERNATIVAS	FRECUENCIA	%
Ninguna	5	50
Entre 1-3	2	20
Entre 4-7	2	20
Más de 7	1	10
No sabe	0	0
No responde	0	0
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 50% de los encuestados opina que no se dieron incidentes de seguridad en el período pasado, el 20% responde que en el período pasado se dieren entre 1-3 incidentes de seguridad, el 20% contesta que en el período pasado se dieren entre 4-7 incidentes de seguridad, el 10% dice que en el período pasado se dieren entre más de 7 incidentes de seguridad. Ninguno de los encuestados responde que no saben si se dieron incidentes de seguridad en el período pasado.

8. Una vez que ocurre la violación de seguridad esta se notifica a:

ALTERNATIVAS	FRECUENCIA	%
Asesor Legal	0	0
Autoridades Locales	0	0

Jefatura de Informática	7	70
Ninguna, no se denuncia	2	20
Otro	1	10
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 70% de los encuestados opinan que las violaciones de seguridad se notifican al Departamento de Informática, el 20% que no se notifican a nadie o no se denuncian, Ninguno de los encuestados responde que las violaciones de seguridad que se notifican al Asesor legal o a las Autoridades locales. El 10% contesta opina que existen otros departamentos a los cuales denuncian las violaciones de seguridad como:

- El coordinador administrativo

9. ¿Cuántas pruebas de seguridad realiza la Institución para valorar el estado de seguridad informática?

ALTERNATIVAS	FRECUENCIA	%
Una al año	4	40
Entre 2 y 4 al año	0	0
Más de 4 al año	1	10
Ninguna	5	50
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 50% de los encuestados opina que no se realizan pruebas de seguridad en la Institución, el 40% responde que las pruebas de seguridad en la Institución se dan una vez al año, el 10% contesta que se dan más de cuatro al año. Ninguno de los encuestados responde que las pruebas de seguridad en la Institución se den entre dos y cuatro al año.

10. ¿Cuál de los siguientes mecanismos utiliza actualmente la Institución para proteger sus Sistemas de Información? (Elija todas las aplicables).

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Smart Cards	0	0
Biometría	1	2,08
Antivirus	9	18,75
Autenticación, Autorización	3	6,25
Filtro de paquetes	3	6,25
Firewalls Hardware	5	10,42
Firewalls Software	5	10,42

Firmas digitales/certificados digitales	2	4,2
Redes privadas virtuales	4	8,33
Proxies	10	20,83
Sistema de detección de intrusos	1	2,08
Monitoreo	4	8,33
Ninguno	0	0
Otros	1	2,08
TOTAL	**48**	**100**

De lo anterior se puede concluir que el 20.83% de los encuestados opina que la institución utiliza a los proxies como mecanismo para proteger sus sistemas de información, el 18.75% responde que la institución utiliza a los antivirus como mecanismo para proteger sus sistemas de información, el 10.42% contesta que la institución utiliza los firewalls Hardware, el 10.42% dice que la institución utiliza los firewalls software, el 8.33% piensa que la institución utiliza a las redes privadas virtuales como mecanismos para proteger sus sistemas de información, el 8.33% considera que la institución utiliza al monitoreo, el 6.25% cree que la institución utiliza a la Autenticación Autorización, el 6.25% opina que la institución utiliza al filtro de paquetes, el 4.2% responde que la institución utiliza las firmas digitales/certificados digitales como mecanismos para proteger sus sistemas de información, el 2.08% contesta que la institución utiliza la biometría, el 2.08% dice que la institución utiliza los sistemas de detección de intrusos. Ninguno de los encuestados responde que la Institución utiliza a los Smart Card como mecanismo para proteger sus sistemas de información. El 2.08% piensa que la institución debe utilizar otros mecanismos para proteger sus sistemas de información como:

- Iptables
- Hosts.allow
- Hosts.deny

Lo que si nos damos cuenta es que el personal informático en la institución no se pone de acuerdo en que se utiliza como mecanismos para proteger sus sistemas de información por lo tanto eso nos da un indicador de desconocimiento de la realidad informática en la UNL.

11. ¿La Institución cuenta con políticas de seguridad de redes?

ALTERNATIVAS	FRECUENCIA	%
No se tiene políticas de seguridad definidas	4	40
Actualmente se encuentra en desarrollo	3	30
Existe políticas formales, escritas documentadas e informadas a todos	3	30
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 40% de los encuestados opina que la institución no tiene políticas de seguridad definidas, el 30% responde que las políticas de seguridad actualmente se encuentran en desarrollo y el 30% contesta que existen políticas formales, escritas documentadas e informadas a todos en la Institución; esto nos da a entender que también existe desconocimiento.

12. ¿Cuáles de los siguientes es obstáculo principal para lograr una adecuada seguridad informática en la Institución?

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Inexistencias de políticas de seguridad	4	12,5
Falta de tiempo	3	9,37
Falta de formación técnica	4	12,5
Falta de apoyo de directivos	3	9,37
Falta de colaboración entre Áreas	3	9,37
Complejidad Tecnológica	1	3,12
Poco entendimiento de seguridad Informática	2	6,25
Falta de recursos	5	15,62
Falta de personal	7	21,87
Ninguno	0	0
TOTAL	**32**	**100**

De lo anterior concluiré que el 21.87% de los encuestados opina que la falta de personal es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 15.62% responde que la falta de recursos, el 12.5% contesta que la inexistencia de políticas, el 12.5% dice que la falta de formación técnica es obstáculo principal, el 9.37% piensa que la falta de tiempo, el 9.37% considera que la falta de apoyo de directivos, el 9.37% cree que la falta de colaboración entre Áreas, el 6.25% opina que el poco entendimiento de seguridad informática, el 3.12% responde que la complejidad tecnológica. Ninguno de los encuestados responde que ninguno de los obstáculos anteriores sea principal para lograr una adecuada seguridad informática en la Institución.

13. ¿De las siguientes actividades de seguridad cuáles son realizadas en la Institución y cuáles son realizadas por personal externo?

Esta pregunta consta de dos partes, pero debido a lo que se refiere con personal externo todas las respuestas son cero, solo se hace el cuadro de lo referente a la Institución, además es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Integración y pruebas de los planes de recuperación de información	1	5,26
Divulgación de aspectos relacionados con la seguridad	0	0
Manejo de incidentes y análisis de vulnerabilidades	1	5,26
Evaluación de seguridad	2	10,52
Seguimiento y monitoreo de actividades	3	15,79
Administración de seguridad	4	21,05
Configuraciones técnicas	8	42,11
TOTAL	19	100

De lo anterior se puede concluir que el 38.88% de los encuestados opinan que las configuraciones técnicas son actividades realizadas por la institución, el 22.22% contesta que la administración de seguridad, el 16.66% dice que el seguimiento y monitoreo de actividades, el 11.11% piensa que la evaluación de seguridad, el 5.55% considera que la integración y pruebas de los planes de recuperación de información, el 5.55% cree que el manejo de incidentes de seguridad y análisis de vulnerabilidades. Ninguno de los encuestados responde que la divulgación de aspectos relacionados con la seguridad sea una actividad realizada por la institución. Ninguno de los encuestados describe que las actividades antes mencionadas sean realizadas por personal externo a la institución.

14. ¿Con que frecuencias se hacen las revisiones de seguridad de activos de información?

ALTERNATIVAS	*FRECUENCIA*	*%*
Anual	*0*	*0*
Semestral	*2*	*20*
Eventual	*4*	*40*
Nunca	*4*	*40*
TOTAL	*10*	*100*

De lo anterior se puede concluir que el 40% de los encuestados opinan que las revisiones de seguridad de activos de información se hacen eventualmente, el 40% responde que no se hacen nunca y el 20% contesta que se hacen semestralmente. Ninguno de los encuestados opina que las revisiones de seguridad de activos de información se hagan anualmente.

15. Dentro de la Institución, ¿Cuáles de los siguientes aspectos son de mayor preocupación en el área de seguridad?

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Informática móvil	1	4
Memoria extraíble	6	24
Redes Inalámbricas	10	40
Telefonía voz sobre IP	1	4
Servidores	7	28
Ninguno	0	0
Otros	0	0
TOTAL	**25**	**100**

De lo anterior se puede concluir que el 40% de los encuestados opina que las redes inalámbricas es el aspecto de mayor preocupación en el área de seguridad, el 28% contesta que los servidores, el 24% dice que las memorias extraíbles, el 4% piensa que la informática móvil, el 4% considera que la telefonía voz sobre IP. Nadie de los encuestados considera que ninguno de los anteriores sea el aspecto de mayor preocupación en el área de seguridad o que existan otros aspectos.

16. ¿Cree usted que es necesario la implementación de un Data Center en la UNL con toda la infraestructura adecuada que brinde seguridades tanto físicas como lógicas para el manejo de la información?

ALTERNATIVAS	FRECUENCIA	%
Si	10	100
No	0	0
TOTAL	**10**	**100**

De lo anterior se puede concluir que el 100% de los encuestados dicen que es necesaria la implementación de un Data Center con toda la infraestructura adecuada, por lo tanto están consientes de eso.

Análisis de los resultados obtenidos en las entrevistas realizadas a los responsables de los centros de cómputo de la Universidad Nacional de Loja

Aquí se planteó una entrevista acerca de la seguridad informática aplicada al personal de los centros de cómputo de los siguientes departamentos:

- Jefatura de Informática
- Área de Energía, Industrias y Recursos Naturales no Renovables
- Área de la Educación, el Arte y la Comunicación
- Área de la Salud Humana

Cabe mencionar que en el Área Jurídica, Social y Administrativa no se realizo dicha entrevista, debido a que no había una persona encargada de forma general de los centros de cómputo y los responsables de dichos centros eran personas que no conocían de la materia por eso se limitaron a no dar la entrevista.

Además en el Área Agropecuaria y de Recursos Naturales Renovables tampoco se realizo la entrevista, debido a que el encargado del centro de cómputo no se encontraba en la ciudad y no se realizo dicha entrevista.

De las entrevistas realizadas se obtuvieron los siguientes resultados:

1. **¿Qué entiende usted sobre Seguridad Informática?**

ALTERNATIVAS	FRECUENCIA	%
Conoce bastante	3	60
Conoce poco	1	20
No conoce	1	20
TOTAL	**5**	**100**

De lo anterior se puede concluir que el 60% de los entrevistados si conoce sobre lo que es la seguridad informática, el 20% conoce poco acerca de lo que se refiere a la seguridad informática y el otro 20% de los entrevistados no conoce sobre dicho tema.

2. ¿Qué medidas implementaría usted para tener una mayor seguridad de los datos tanto inalámbrica como alámbricamente?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
VPN	2	22,2
Servidor Radius	2	22,2
Cisco Pix	1	11,1
Monitoreo Correctivo y Preventivo de la red	1	11,1
Software con licencia	1	11,1
Servidores (web y proxy) de buena calidad	1	11,1
Crear esquemas de las redes existentes	1	11,1

TOTAL	**9**	**100**

De lo anterior podemos concluir que el 22% de los entrevistados afirman que las medidas a implementar para tener una mayor seguridad de los datos en la intranet son las VPN, el 22% contesta que los servidores radius son de importancia a implementar para la seguridad de la intranet, el 11% dice que los Cisco Pix, el 11% piensa que el monitoreo correctivo y preventivo de la red, el 11% considera que el Software con licencia, el 11% aseveran que los servidores web y proxy, y 11% afirma que los esquemas de seguridad son de importancia a implementar para la seguridad de la intranet.

3. ¿Qué tipo de mecanismos de seguridad informática se ejecutan en la actualidad?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Firewalls	1	12,5
Acceso web (Protocolos SSL[22] en el SGA[23])	1	12,5
Encriptación wep	1	12,5
Iptables	1	12,5
Host-deny	1	12,5
Monitoreo y gestión de redes	1	12,5
Mac Address	1	12,5
No existen	1	12,5
TOTAL	**8**	**100**

De lo anterior se puede concluir que el 12,5% de los entrevistados afirman que el firewall es un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% contesta que los Accesos web servidores son un mecanismo de seguridad que se ejecuta en la actualidad, el

[22] *SSL: Secure Socket Layer*

[23] SGA: Sistema de Gestión Académica de la Universidad Nacional de Loja

12,5% dice que la encriptación web, el 12,5% piensa que los Iptables son un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% considera que los host-denny son un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% aseveran que el monitoreo y gestión de redes es un mecanismo de seguridad, el 12,5% afirma que las MAC Address son un mecanismo de seguridad que se ejecuta en la actualidad y por último un 12.5% niega la existencia de un mecanismo de seguridad que se ejecute en la actualidad, esto nos da la idea que las personas que trabajan en la parte informática en la UNL no conocen de la realidad de las seguridades existentes.

4. ¿Qué opina acerca del control de acceso (Autenticación, Autorización) en redes de datos?

ALTERNATIVAS	FRECUENCIA	%
Conoce bastante	3	60
Conoce poco	1	20
No conoce	1	20
TOTAL	**5**	**100**

De lo anterior se puede concluir que el 60% de los entrevistados si conoce sobre lo que es el control de acceso en redes de datos utilizando AAA, el 20% conoce poco y el otro 20% de los entrevistados no conoce sobre dicho tema.

5. ¿Considera usted que la seguridad en la red inalámbrica y alámbrica, implementada en la Universidad Nacional de Loja es segura?

ALTERNATIVAS	FRECUENCIA	%
SI	1	20
NO	4	80
TOTAL	**5**	**100**

De lo anterior se puede concluir que el 20% de los entrevistados considera que la seguridad en la red inalámbrica y alámbrica, implementada en la Universidad Nacional de Loja si es segura y el otro 80% de los entrevistados afirman que no lo es, eso marca un precedente para trabajar sobre este tema

6. ¿Qué sugerencias ayudarían a mejorar la seguridad en la red de datos de la Universidad Nacional de Loja?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

ALTERNATIVAS	FRECUENCIA	%
Administración permanente de los historiales de los sistemas	1	7,6
Implementación de políticas de seguridad a nivel de usuario final	2	15,3
Inversión en equipos para la seguridad	2	15,3
Capacitación en seguridades LAN-WAN-WLAN	2	15,3
Que exista VPN en cada área	1	7,6
Que exista software libre para la administración de redes	2	15,3
Que exista en mecanismo de autenticación como servidor radius	1	7,6
Que exista manuales de distribución de la red en cada área.	1	7,6
Administración permanente de la red	1	7,6
TOTAL	**13**	**100**

De lo anterior se puede concluir que el 7,6% de los entrevistados afirman que se deberían implementar una Administración permanente de los historiales de los sistemas para mejorar la seguridad de la red, el 12,5% contesta que se deberían implementar políticas de seguridad a nivel de usuario final para mejorar la seguridad de la red, el 12,5% dice que se deberían realizar una Inversión en equipos para la seguridad de la red, el 12,5% piensa que se deberían implementar capacitaciones en seguridades LAN-WAN-WLAN para mejorar la seguridad de la red, el 12,5% considera que se deberían implementar VPN en cada área, el 12,5% aseveran que se deberían implementar software libre para la administración de redes, el 12,5% afirma que se deberían implementar un mecanismo de autenticación como servidor radius para mejorar la seguridad de la red, un 12% menciona que se deberían implementar manuales de distribución de la red en cada área y por último un 12.5% sugiere que se deberían implementar una administración permanente de la red para mejorar la seguridad de la misma.

ANEXO 2

Fotografías de la Situación Actual del Centro de Datos de la Universidad Nacional de Loja

Foto 1: Administración Central

Foto 2: Jefatura Informática

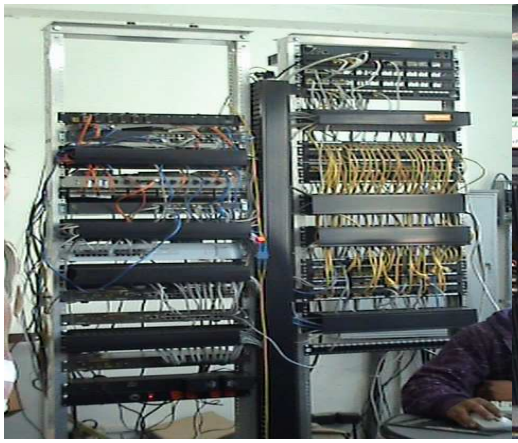


Foto 3: Data Center1

Foto 4: Servidores1

Foto 5: Seguridad Eléctrica

Foto 6: Servidores2

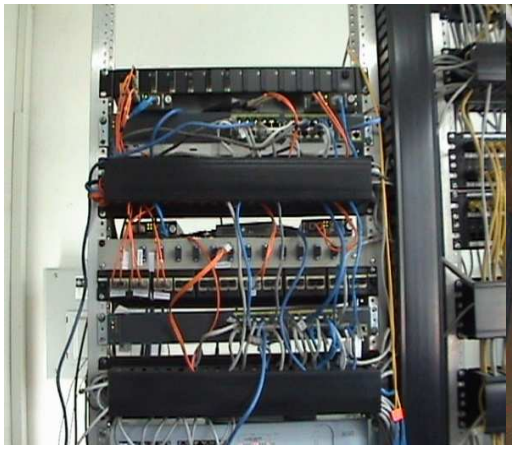


Foto 7: Conexiones de Fibra

Foto 8: Firewall

Foto 9: Proxy

Foto 10: DHCP

Foto 11: Data Center 2

Foto 12: DHCP

ANEXO 3

Diseños para la construcción del instituto de informática de la Universidad Nacional de Loja

Foto 1: Instituto de Informática (Vista Exterior)

Foto 1: Instituto de Informática (Vista Exterior Frontal)

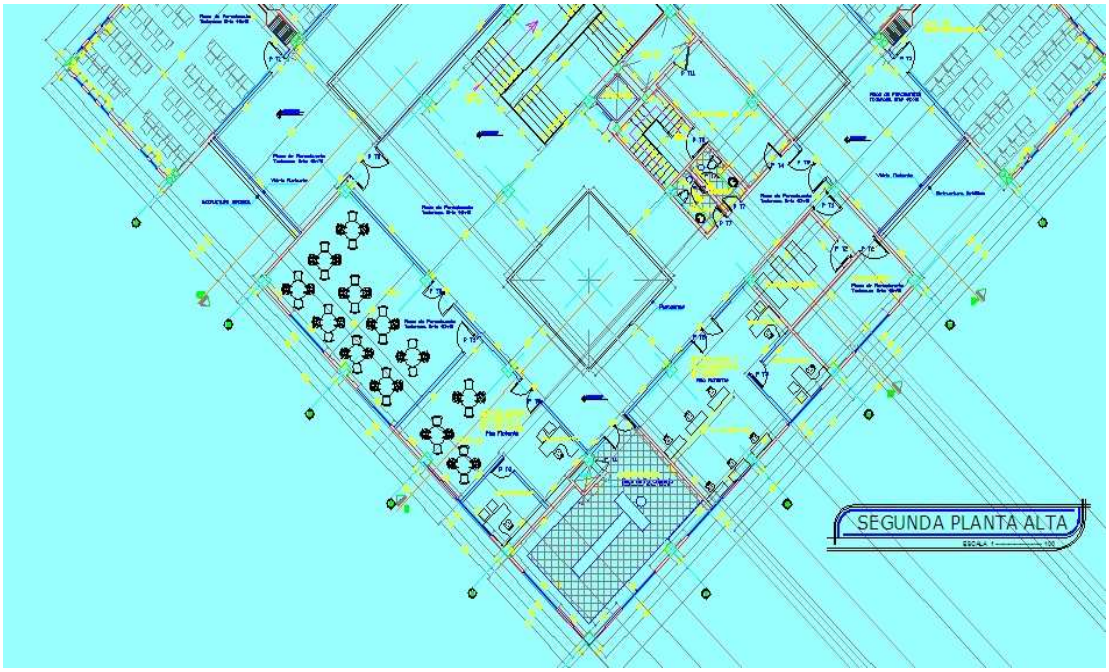


Foto 2: Instituto de Informática (Segunda Planta)

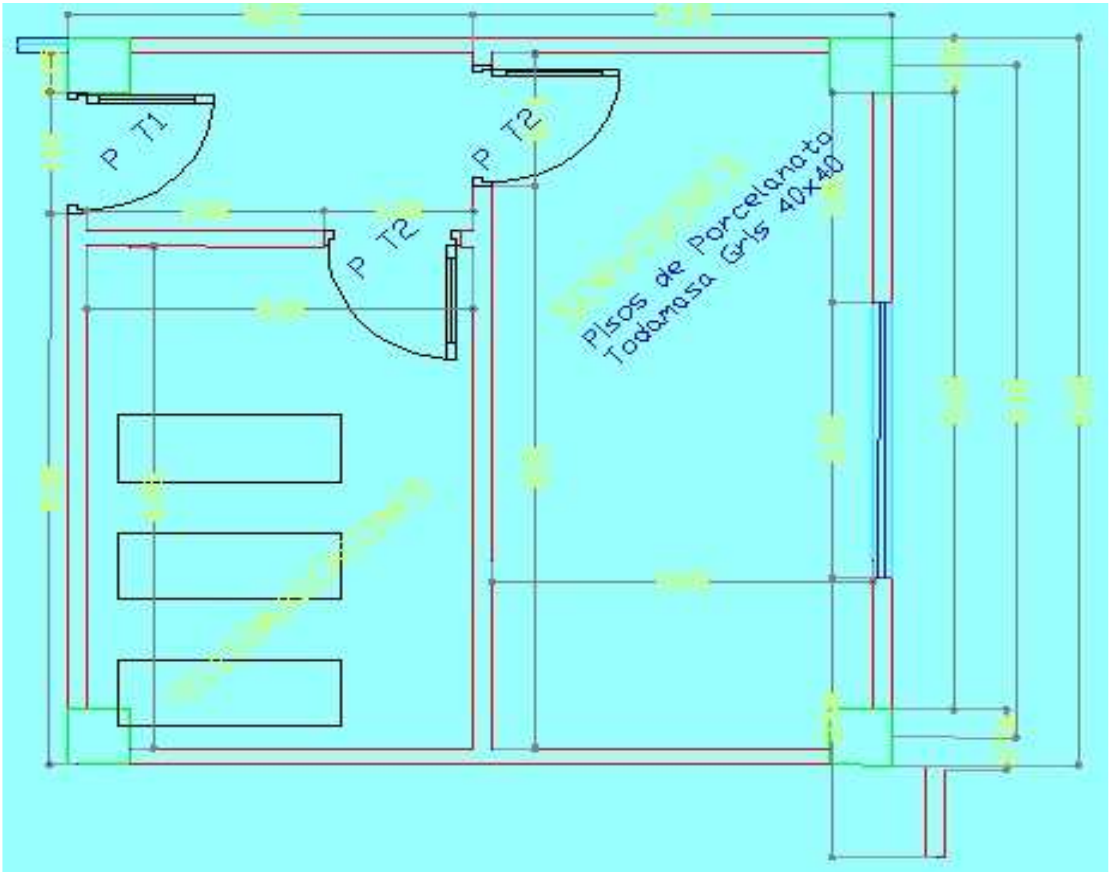


Foto 3: Data Center UNL