UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO DIRIGIDO

"GESTIÓN DE LA RED DE DATOS EN LA DIRECCIÓN DE INFORMACIÓN ACADÉMICA DE LA U.A.P."

TRABAJO DIRIGIDO PRESENTADO PARA OBTENER EL TÍTULO ACADÉMICO DE LICENCIADO EN INGENIERÍA DE SISTEMAS

POSTULANTE: Univ. Marco Antonio Montevilla Ruiz

TUTOR: M.Sc. Ing. Freddy Morales Blanco

ASESOR: Ing. Abel Huaygua Chalco

Cobija - Pando – Bolivia

2016

AGRADECIMIENTOS

A Dios por darme la vida, salud y la sabiduría para realizar mis sueños, a mis padres y hermanos por su apoyo en el trascurso de mi carrera, a mis amigos por acompañarme en los buenos y malos momentos de mi vida y a todos mis Docentes del Área de Ciencias y Tecnología, Gracias…

DEDICATORIA

A Dios por darme la vida, para realizar mi Carrera Universitaria, a mis padres y a mi hermana Cinthia por su apoyo incondicional y tener la confianza en mí, a mi hijita hermosa por ser el angelito que me cuida y guía mis pasos.

A todos mis docentes del Área de Ciencias y Tecnología por haberme transmitido sus conocimientos.

RESUMEN

Con los avances de las tecnologías de información y comunicación, crece la necesidad de compartir información y recursos, razón por la cual la implementación de redes para solucionar estas necesidades se vuelve algo cotidiano. Lo cual hace presente la gestión de redes.

La gestión de redes abarca hoy en día muchos aspectos, que pueden resumirse o sintetizarse en tareas, para conseguir niveles de trabajo y de servicio adecuados a los objetivos de una organización.

El presente trabajo dirigido consiste en la gestión de la red de datos en la Dirección de Información Académica de la Universidad Amazónica de Pando (U.A.P.), el cual tiene el objetivo, mejorar la gestión de la Red de Datos en la ya mencionada Dirección. Debido a las necesidades presentada en las unidades de la dirección de información académica, para tener una mejor gestión en la red de datos se realizaron las diferentes actividades: se realizó un análisis inicial de la misma la cual ayudo a obtener los requerimientos de los usuarios para así en base a eso realizar los diseños lógico y físico de la red de datos cumpliendo normas y estándares de cableado estructurado, del mismo modo se brindó asistencia técnica contante en el trascurso del desarrollo del Trabajo Dirigido todo esto se llevó acabo utilizando la metodología "Modelo Funcional Para la Administración de Redes".

La gestión de la red de datos mejoró significativamente, permitiendo tener un mejor flujo de información sin muchos cortes, del mismo modo permitió mejorar la seguridad física como lógica, la misma nos lleva a las conclusiones que se debe realizar la adquisición de más equipos de seguridad y realizar la implementación del cableado acorde a los diseños propuestos.

ABSTRACT

With the advances of information and communication technologies, the need to share information and resources grows, which is why the implementation of networks to solve these needs becomes a daily occurrence. This makes network management present.

Network management today encompasses many aspects, which can be summarized or synthesized into tasks, to achieve levels of work and service adequate to the objectives of an organization.

The present work consists of the management of the data network in the Academic Information Department of the Amazonas University of Pando (U.A.P.), which has the objective of improving the management of the Data Network in the aforementioned Directorate. Due to the needs presented in the units of the academic information management, in order to have a better management in the data network the different activities were carried out: an initial analysis of the same was done, which helped to obtain the users' requirements for So based on that make the logical and physical designs of the data network complying with norms and standards of structured cabling, in the same way provided constant technical assistance in the course of the development of the Directed Work all this was carried out using the methodology "Model Functional for Network Administration ".

The management of the data network improved significantly, allowing a better flow of information without many cuts, likewise allowed to improve physical security as logic, it leads us to the conclusions that must be made to acquire more security equipment and implement the wiring according to the proposed designs.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I

1.MARCO INTRODUCTORIO

1.1. ANTECEDENTES

La Universidad Amazónica de Pando, fue creada mediante Decreto Supremo N° 20511 del 21 de septiembre de 1984 y sancionada mediante Ley de la Nación N° 653 de 18 de Octubre de 1984 según (UAP, Universidad Amazonica de Pando, 2016). Actualmente Universidad Amazónica de Pando, tiene como Magnífico Rector al Ing. Ludwing Arcienega Baptista y como Vicerrector al Lic. José Luis Segovia Saucedo; ofertando estudios académicos superiores a nivel licenciatura, de las seis Áreas Académicas los cuales son: Ciencias de la Salud, Ciencias Biológicas y Naturales, Ciencias y Tecnología, Ciencias Jurídicas y Políticas, Ciencias Sociales y Humanísticas, Ciencias Económicas y Financieras. Asimismo, oferta estudios superiores a nivel Técnico Superior.

La Dirección de Información Académica de la Universidad Amazónica de Pando (UAP[1]), se inicia el 2003 donde se presenta un proyecto denominado "Proyecto de Organización de la Dirección de Información Académica (DIA[2])", cuya misión es promover, orientar y administrar, la información académica de estudiante y docentes en la UAP en forma transparente, eficiente y oportuna a través de nuevas tics. Este proyecto se pone en ejecución el mismo año, la cual cuenta con las siguientes Unidades, trámites e informaciones, archivo académico universitario, sistemas académicos universitario.

Hoy por hoy existe la Unidad de Sistemas de Información y Comunicación (USIC[3]) dependiente de la Dirección Administrativa Financiera la cual dentro de sus Divisiones está la División de Redes de Datos e Internet quien es el ente encargado de Administrar toda la red de datos de nuestra Superior Casa de Estudios, es así que en coordinación con dicha unidad se realizar el presente Trabajo Dirigido.

[1] Universidad Amazónica de Pando
[2] Dirección de Información Académica
[3] Unidad de Sistemas de Información y Comunicación

La metodología que se recurrirá para el siguiente trabajo dirigido es, Modelo funcional para la administración de redes, basada en modelos funcionales estándares de la ITU[4] y de la ISO[5].

En el presente Trabajo Dirigido se ha tomado en cuenta los siguientes trabajos relacionados en el campo de estudio:

(Huaygua, 2005). En el trabajo de grado "Administración de la red de datos e internet (DIA)", el mismo tiene como objetivo mejorar la administración de la red de datos y el servicio de internet del predio central de la UAP, la misma da soluciones a los problemas de la Red e implementa políticas del uso de la red y el uso de Internet, así mismo realiza la implementación de un Servidor Proxy en la sala de Internet del Campus Universitario de la UAP.

(Ledezma, 2012). Hace mención en proyecto de internet como una red de redes, es decir, una red que no solo interconecta computadoras, sino que interconecta redes de computadoras entre sí, es una de las herramientas con mayor capacidad de información y así el servicio de Internet mejora con la administración de la red de datos e Internet, regulando el ancho de banda, restringiendo página web, monitoreo y control del uso de internet.

(Zenteno, 2009). Hace referencia en el trabajo de grado "Servidor de Administración de ancho de banda en la Universidad Amazónica de Pando", el mismo realiza la implementación de una aplicación MikroTik que permita gestionar el ancho de banda, es así que se optimizó los recursos del internet a través de la utilización del wed-proxy, y el modelo de cola, en la cual ayudó en políticas de bloqueos de tráficos a páginas y paquetes al igual a descargas de ciertos archivos.

[4] Unión Internacional de Telecomunicaciones
[5] Organización Internacional para la Estandarización

(Calizaya, 2012). Hace referencia en el trabajo de grado “Administración de la Red de Datos e Internet en el Predio Central de la U.A.P”, la misma dio solución a problema de la Red aplicando políticas de bloqueo de páginas e implementando el servicio de HotSpot para el ingreso por autenticación a la zona Wifi de la UAP.

(Fong, 2015).En el trabajo de grado Implementación de una red de datos del laboratorio del programa de ingeniería de sistemas en el área de ciencia y tecnología de la Universidad Amazónica de Pando, la misma con la implementación logro la interconexión de los equipos para tener un mejor flujo de información y recursos.

Cabe mencionar que cada uno de los trabajos mencionados ayudaron para tomar decisiones puntuales para mejorar la gestión de la Red de Datos de la Dirección de Información Académica, de misma forma servirá de referencia de los aportes que realizaron cada uno de los autores ya mencionados.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Descripción del Problema

En el Campus Universitario de la Universidad Amazónica de Pando, Predio en el cual desempeña sus funciones la Dirección de Información Académica (DIA), se encarga de ofrecer las actividades de administración académica a la comunidad universitaria, la misma tiene algunas privaciones en su administración, no cuenta con un adecuado acceso, la falta de administración en la seguridad, monitoreo, soporte técnico, los cortes frecuentes de los servicios, equipos en mal estados y otros obsoletos, no cumple con las normas y estándares en sus cableado de red, la mismas dificultan a la hora de cumplir sus funciones cotidianas.

Estas causas mencionadas anteriormente provocan efectos como ser: La pérdida de información a la hora de transferir la información entre equipos ,insatisfacción del servicio por parte de los usuarios, de tal manera que los usuarios tienen constante reclamos por pérdida

o lentitud de los servicios prestados, los funcionarios no pueden realizar sus actividades laborales a nivel deseado lo cual con lleva al desempeño laboral a un nivel no esperado, la demora en el tiempo a la hora de la atención a la comunidad universitaria.

1.2.2. Formulación del Problema

Debido a los problemas mencionados se plantea el siguiente problema principal:

"Gestión inadecuada en la Red de Datos en la Dirección de Información Académica de la U.A.P."

1.3. OBJETIVOS

1.3.1. Objetivo General

Mejorar la gestión de la Red de Datos en las unidades de la Dirección de Información Académica de la U.A.P. utilizando la metodología "Modelo Funcional para la Administración de Redes", para así proporcionar un buen servicio.

1.3.2. Objetivos Específicos

Los objetivos específicos que nos llevaran a alcanzar el objetivo general son:

- ✓ Analizar la situación actual de la red, realizar entrevistas y una encuesta al personal técnico y de planta de la unidad, para conocer los requerimientos.
- ✓ Diseñar la red de datos basado en los requerimientos y la metodología empleada, cumpliendo así sus normas y estándares para tener resultados efectivos y eficientes.
- ✓ Brindar soporte técnico informático vía asistencia técnica a las unidades de la dirección académica para mejorar en su desempeño de las mismas.

- ✓ Gestionar la Seguridad de la red de datos, basándonos en la metodología utilizada, para optimizar el funcionamiento de la misma.

1.4. ALCANCES

De acuerdo al ámbito geográfico, el alcance del trabajo dirigido contempla la Dirección de Información Académica de la Universidad Amazónica de Pando, en la cual se realizara las siguientes actividades:

- Diseño lógico y físico de la red de datos.
- Servicio técnico informático a las unidades de la dirección de información académica.
- Explotar políticas de seguridad, Servicios de seguridad y mecanismos de seguridad a nivel lógico y físico.
- Se realizará el soporte técnico en algunos casos en coordinación con el administrador de redes de datos del Campus Universitario de la UAP dependiente de la USIC.
- Las actividad a realiza solo contempla la Dirección de Información Académica.

1.5. METODOLOGÍA Y HERRAMIENTAS UTILIZADAS

La metodología empleada en el siguiente Trabajo Dirigido es "Modelo Funcional para la Administración de Redes", esta metodología es recomendable en trabajos dirigidos puesto que es un cargo en base a funciones, las mismas se explican a continuación:

Existen diversos modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN[6]de la ITU como el modelo OSI-NM[7], estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

[6] Serie de recomendaciones M.3000 de la ITU-T. http://www.itu.int
[7] El modelo de interconexión de sistemas abiertos

Esta metodología divide la administración de una red en áreas funcionales que son cinco y son las siguientes: (configuración, fallas, rendimiento, contabilidad y seguridad) cada proceso tiene sus propias actividades. En base al trabajo dirigido se considera tres de las cinco áreas funcionales de la metodología que ayudaran a alcanzar la solución a la problemática planteada las cuales son: (configuración, fallas y seguridad) cada actividad de la metodología tiene por objetivo depender con los objetivos específicos.

1.6. ORGANIZACIÓN DEL DOCUMENTO

Describe el contenido del resto de documento, resumiendo el propósito y contenido de cada uno de los siguientes capítulos, hasta el capítulo de las conclusiones.

- **Capítulo I:** Establece la parte introductoria del Trabajo Dirigido donde se describe la introducción, el problema, los objetivos planteados, la metodología utilizada y alcances.
- **Capítulo II:** Se describe los fundamentos teóricos y conceptuales y las herramientas utilizadas en el desarrollo del presente Trabajo Dirigido.
- **Capítulo III:** En este capítulo se describe la metodología adoptada para el proceso del desarrollo del presente Trabajo Dirigido.
- **Capítulo IV:** En este capítulo se describe el marco contextual de la institución involucrada donde se realizara el presente Trabajo Dirigido.
- **Capítulo V:** En este capítulo se realiza la ejecución del proyecto en base a la metodología, sus etapas y actividades como ser: análisis, planeación y diseño de la Red de Datos, gestión de fallas, y gestión de la seguridad.
- **Capítulo VI:** En este capítulo se refleja y detalla las conclusiones y recomendaciones obtenidas del trabajo dirigido, en base a los objetivos planteados, alcances y las recomendaciones para la mejor gestión de la red de datos.

CAPITULO II

2.MARCO TEÓRICO

2.1. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

Según (ORTI, 2016) Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Las TIC son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido...).

En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas. (Cabero, 1998)

De acuerdo a los autores Ortí y Cabero las tecnologías de informacion y comunicación son un conjunto de tecnologías nueva que permiten el acceso a la información que giran en tres medios básicos: informática, microelectronica y telecomunicaciones; de forma que interactuan directamente entre ellas para asi conseguir nuevos conocimientos.

2.2. GESTION DE RED

La gestión de red trata sobre la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste.

Los objetivos principales de la gestión de red consisten en mejorar disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad.

Desde el momento en que las redes se consideran cada vez más una parte importante y estratégica de la empresa, industrias u otros tipos de instituciones y como resultado de la cada vez mayores dimensiones que están adoptando, resulta pues más importante su control y gestión con el fin de obtener mejor calidad de servicios posible.

Para proporcionar una calidad de servicio adecuada mediante la gestión de redes, se parte de unos recursos humanos que mediante una serie de herramientas aplican unas determinadas metodología a la red. Este texto versa sobre herramientas y métodos que se pueden emplear en la gestión de red. Las recomendaciones sobre esta temática proviene de diversos grupos de estandarización. Las más importantes, la ITU-T[8], han definido la red de gestión de las telecomunicaciones (TMN). Estas recomendaciones definen cinco áreas funcionales para la gestión de red, la de supervisión y fallos, configuración, tarificación, prestaciones y seguridad. (Barba Martí, 1999).

De acuerdo con (Magedanz, 1996) La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio.

[8] Sector de Normalización de las Telecomunicaciones de la UIT

2.2.1. Arquitectura de Gestión de Red

La gestión de red se suele centralizar en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la empresa en cuestión. Un centro de gestión de red dispone de tres tipos principales de recursos:

- Métodos de gestión. Definen las pautas de comportamiento de los demás componentes del centro de gestión de red ante determinadas circunstancias.
- Recursos humanos. Personal encargado del correcto funcionamiento del centro de gestión de red.
- Herramientas de apoyo. Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos

2.3. RED DE DATOS

Según se menciona en (wikitel, 2016) Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la conmutación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física.

Según (Merino, 2011-2014) Una red de computadoras también llamada red de ordenadores o red informática es un conjunto de equipos (computadoras y dispositivos), conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a una red se denomina un nodo

2.3.1. Red de Área Local (LAN)

De acuerdo a (Ecured, 2016) Una red de área local, red local es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos.

El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información; algunas de las ventajas de las red de área local, es que permite compartir Bases de datos (se elimina la redundancia de datos), Programas (se elimina la redundancia de Software) y Periféricos como puede ser un Módem, una Tarjeta RDSI, una Impresora, etc.

2.3.2. Red de Área Local Virtual (VLAN)

De acuerdo a (Cisco c. , 2016) Una Vlan[9] es un grupo de dispositivos en uno o más LANs que están configurados para comunicarse como si estuvieran conectados al mismo cable, cuando en realidad se encuentran en un número de diferentes segmentos de la LAN. Debido a que las VLAN se basan en conexiones lógicas en vez de físicas, son extremadamente flexible.

Las VLAN mejoran la seguridad de la red al aislar a los usuarios que tienen acceso a los datos y aplicaciones sensibles, además dividen la red en redes lógicas más pequeñas que dan resultado a una menor susceptibilidad a las tormentas de broadcast.

- **Funciones de las VLAN**
  - **Optimización del Ancho de Banda**: crean dominios de broadcast más pequeños.

[9] Red de Área Local Virtual

- **Seguridad:** permiten desarrollar un nivel de seguridad más alto, ya que no permiten que la información salga del mismo grupo de trabajo.
- **Balance de carga:** combinado con ruteo, determinan la mejor ruta hacia un destino.
- **Aíslan las fallas:** reducen el impacto de problemas en la red.

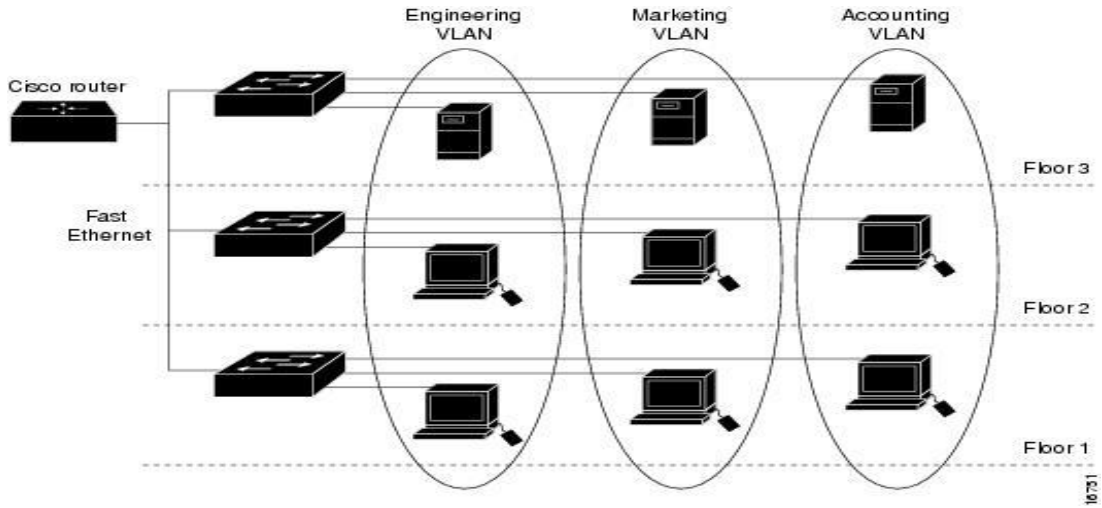


FIGURA 1: *Esquema de tres VLAN que crean redes lógicamente definidas*

Fuente*: (Cisco c. , 2016)*

2.3.3. Topología de Red

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las

interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma. Los diferentes tipos de topología son:

- Topología de bus
- Topología de estrella
- Topología en anillo
- Topología de árbol
- Topología de malla

➢ **Estrella Extendida**

Según (Tripod, 2016), una topología en estrella extendida es igual a la topología en estrella, con la diferencia que cada nodo que se conecta con el nodo central también es el centro de otras estrella , como se muestra en la figura 2, La ventaja es que hace que el cableado sea más corto y limita el número de dispositivos necesarios para interconectar cualquier nodo central Una topología en estrella extendida es muy jerárquica y se puede configurar (con el equipo apropiado) para "animar" a que el trafico permanezca local.

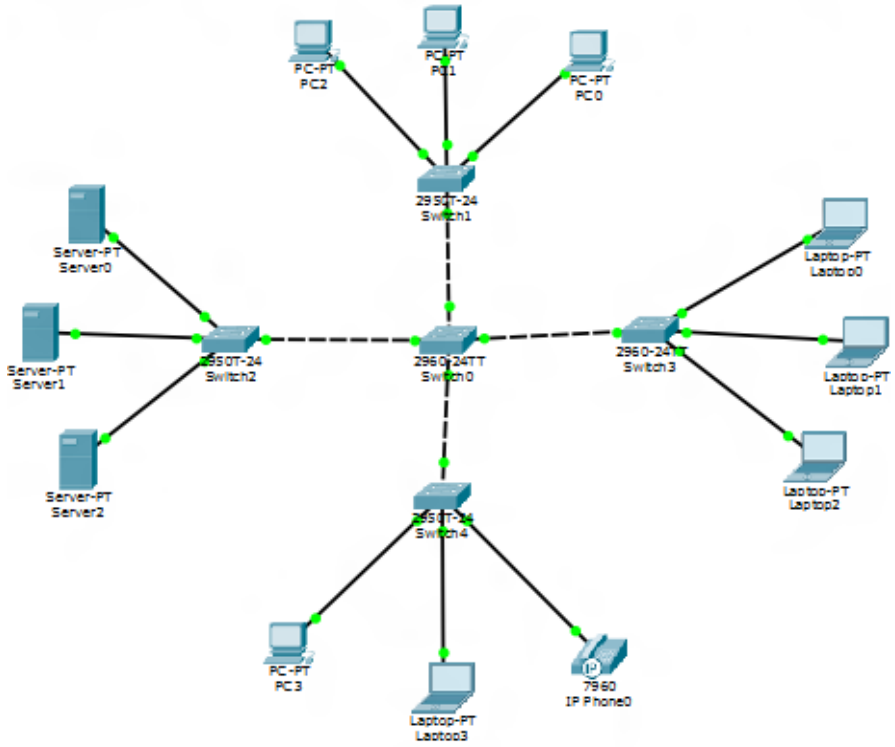


FIGURA 2: *Topología estrella extendida*

Fuente**:** *Elaboración propia*

2.4. CABLEADO ESTRUCTURADO CUMPLIENDO LOS ESTÁNDARES ANSI/TIA/EIA-568 Y ANSI/TIA/EIA-569.

Según (Porto A. G., 2011. Actualizado: 2014) Se conoce como cableado estructurado al sistema de cables, conectores**,** canalizaciones **y** dispositivo**s** que permiten establecer una infraestructura de telecomunicaciones en un edificio. La instalación y las características del sistema deben cumplir con ciertos estándares para formar parte de la condición de cableado estructurado.

Tal como es descrito por (raymundo, 2016) Es el conjunto de elementos pasivos, flexibles, genérico independiente, que sirve para interconectar equipos activos de diferentes o igual tecnología permitiendo la integración de los diferentes sistemas de control, comunicación y manejo de información, sean estos de datos, video, así como equipos de comunicación y otros sistemas.

2.4.1. Estándar ANSI/EIA/TIA-568

El estándar ANSI/TIA/EIA-568 y sus recientes actualizaciones especifican los requerimientos de un sistema integral de cableado, independiente de las aplicaciones y de los proveedores, para los edificios comerciales.

Se estima que la "vida productiva" de un sistema de cableado para edificios comerciales debe ser de 15 a 25 años. En este período, las tecnologías de telecomunicaciones seguramente cambien varias veces. Es por esto que el diseño del cableado debe prever grandes anchos de banda, y ser adecuado tanto a las tecnologías actuales como a las futuras.

Especificaciones del Estándar ANSI/EIA/TIA-568:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina, para distintas tecnologías de cables (cobre y fibra).
- Topología y distancias recomendadas.

- Parámetros de desempeño de los medios de comunicación (cables de cobre, fibra).

El estándar ANSI/EIA/TIA-568-C.1 identifica seis componentes funcionales:

- ✓ Instalaciones de Entrada (o “Acometidas”)
- ✓ Distribuidor o repartidor principal y secundarios
- ✓ Distribución central de cableado
- ✓ Distribuidores o repartidores Horizontales
- ✓ Distribución Horizontal de cableado
- ✓ Áreas de trabajo

2.4.2. Distribuidor o Repartidor Principal y Secundarios

La estructura general del cableado se basa en una distribución jerárquica del tipo “estrella”, con no más de 2 niveles de interconexión. El cableado hacia las “áreas de trabajo” parte de un punto central, generalmente la “Sala de Equipos”. Aquí se ubica el Distribuidor o Repartidor principal de cableado del edificio. Partiendo de éste distribuidor principal, para llegar hasta las áreas de trabajo, el cableado puede pasar por un Distribuidor o Repartidor secundario y por una Sala de Telecomunicaciones.

El estándar no admite más de dos niveles de interconexión, desde la sala de equipos hasta la sala de Telecomunicaciones. Estos dos niveles de interconexión brindan suficiente flexibilidad a los cableados de back-bone.

2.4.3. Distribuidores o Repartidores Horizontales

Los cables montantes (back-bone) terminan en los distribuidores o repartidores horizontales, ubicados en la Sala de Telecomunicaciones. Estos repartidores horizontales deben disponer de los elementos de interconexión adecuados para la terminación de los cables montantes (ya sean de cobre o fibra óptica).

Asimismo, a los repartidores horizontales llegan los cables provenientes de las "áreas de trabajo" (cableado horizontal, de allí su nombre de "repartidores horizontales"), el que también debe ser terminado en elementos de interconexión adecuado.

La función principal de los repartidores horizontales es la de interconectar los cables horizontales (provenientes de las áreas de trabajo) con los cables montantes (provenientes de la sala de equipos).

2.4.4. Distribución Horizontal de Cableado

Tal como es descrito por (Joskowicz, 2013) la norma ANSI/TIA/EIA-568 la define como la distribución horizontal es la parte del cableado de telecomunicaciones que conecta las áreas de trabajo con los distribuidores o repartidores horizontales, ubicados en el Armario o Sala de Telecomunicaciones.

La distribución Horizontal Incluye:

- Cables de distribución horizontal
- Conectores de telecomunicaciones en las áreas de trabajo (dónde son terminados los cables de distribución horizontal)
- Terminaciones mecánicas de los cables horizontales
- Cordones de interconexión ("Patch-cords") en el Armario o Sala de Telecomunicaciones.
- Puede incluir también "Puntos de Consolidación"

2.4.5. Topología de Distribución Horizontal

El cableado de distribución horizontal debe seguir una topología del tipo estrella, con el centro en el armario o sala de telecomunicaciones, y los extremos en cada una de las áreas de trabajo. Los conectores de telecomunicaciones en las áreas de trabajo deben ser conectados mediante un cable directamente al panel de interconexión ubicado en el armario de telecomunicaciones. No se admiten empalmes ni uniones, salvo en caso de existir un "punto de consolidación".

2.4.6. Distancia para el Cable de Distribución Horizontal

La distancia máxima para el cable de distribución horizontal es de 90 m, medida en el recorrido del cable, desde el conector de telecomunicaciones en el área de trabajo hasta el panel de interconexión en el armario de telecomunicaciones.

Los cordones de interconexión ("patch-cords") utilizados en las áreas de trabajo y en el armario de telecomunicaciones no deben ser más largos que 10 m en conjunto (completando una distancia de 100 m de "punta a punta". Se recomienda que los cordones de interconexión en cada extremo no superen los 5 m.

- **Cables Reconocidos para la Distribución Horizontal**
  - UTP o ScTP de 100 _ y cuatro pares
  - Fibra óptica multimodo de 50/125 μm
  - Fibra óptica multimodo de 62.5/125 μm

2.5. ESPACIOS Y CANALIZACIONES PARA TELECOMUNICACIONES

El estándar ANSI/TIA/EIA-569 provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios comerciales, la misma contempla diversas revisiones.

En Marzo de 2013 entró en vigencia la revisión “C” de la recomendación, conocida como ANSI/TIA/EIA-569-C donde se quita expresamente la referencia de “Edificios comerciales”.

El estándar identifica los siguientes componentes en la infraestructura edilicia[10]:

- Instalaciones de Entrada
- Sala de Equipos
- Canalizaciones de “Montantes” (“Back-bone”)
- Salas de Telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

2.5.1. Sala de Equipos

Se define como el espacio dónde se ubican los equipos de telecomunicaciones comunes al edificio. Los equipos de esta sala pueden incluir centrales telefónicas, equipos informáticos (servidores), Centrales de video, etc. Sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones.

En el diseño y ubicación de la sala de equipos, se deben considerar:

- Posibilidades de expansión. Es recomendable prever el crecimiento en los equipos que irán ubicados en la sala de equipos, y prever la posibilidad de expansión de la sala.
- Evitar ubicar la sala de equipos en lugar dónde puede haber filtraciones de agua, ya sea por el techo o por las paredes

[10] Referirse a todo aquello propio o vinculado a los edificios y también a la construcción

- Facilidades de acceso para equipos de gran tamaño.
- La estimación de espacio para esta sala es de 0.07 m^2 por cada 10 m^2 de área utilizable del edificio. En edificios de propósitos específicos, como ser Hoteles y Hospitales. En todos los casos, el tamaño mínimo recomendado de 13.5 m^2 (es decir, una sala de unos 3.7 x 3.7 m).
- Es recomendable que esté ubicada cerca de las canalizaciones "montantes" (back bone), ya que a la sala de equipos llegan generalmente una cantidad considerable de cables desde estas canalizaciones.
- Otras consideraciones deben tenerse en cuenta, como por ejemplo:
  - ✓ Fuentes de interferencia electromagnética
  - ✓ Vibraciones
  - ✓ Altura adecuada
  - ✓ Iluminación
  - ✓ Consumo eléctrico
  - ✓ Prevención de incendios

2.5.2. Canalizaciones de "Back-Bone"

Se distinguen dos tipos de canalizaciones de "back-bone": Canalizaciones externas, entre edificios y canalizaciones internas al edificio.

- **Canalizaciones Interna**

  Las canalizaciones internas de "backbone", generalmente llamadas "montantes" son las que vinculan las "instalaciones de entrada" con la "sala de equipos", y la "sala de equipos" con las "salas de telecomunicaciones".

Estas canalizaciones pueden ser ductos, bandejas, escalerillas porta cables, etc.

Es muy importante que estas canalizaciones tengan los elementos “cortafuegos “de acuerdo a las normas corporativas y/o legales. Las canalizaciones “montantes” pueden ser físicamente verticales u horizontales.

- **Canalizaciones Montantes Verticales**

Se requieren para unir la sala de equipos con las salas de telecomunicaciones o las instalaciones de entrada con la sala de equipos en edificios de varios pisos.

Generalmente, en edificios de varios pisos, las salas de telecomunicaciones se encuentran alineados verticalmente, y una canalización vertical pasa por cada piso, desde la sala de equipos.

Estas canalizaciones pueden ser realizadas con ductos, bandejas verticales, o escalerillas porta cables verticales. No se admite el uso de los ductos de los ascensores para transportar los cables de telecomunicaciones.

- **Canalizaciones Montantes Horizontales**

Si las salas de telecomunicaciones no están alineadas verticalmente, son necesarios tramos de “montantes” horizontales. Estas canalizaciones pueden ser realizadas con ductos, bandejas horizontales, o escalerillas porta cables. Pueden ser ubicadas sobre el cielorraso, debajo del piso, o adosadas a las paredes.

2.5.3. Salas de Telecomunicaciones

Las salas de telecomunicaciones se definen como los espacios que actúan como punto de transición entre las “montantes” verticales (back bone) y las canalizaciones de distribución horizontal. Estas salas generalmente contienen puntos de terminación e interconexión de cableado, equipamiento de control y equipamiento de telecomunicaciones (típicamente equipos, como por ejemplo switches). Se recomienda no compartir la sala de telecomunicaciones con equipamiento de energía.

Los tamaños recomendados para las salas de telecomunicaciones son las siguientes (se asume un área de trabajo por cada 10 m2):

Área utilizable	Tamaño recomendado de la sala de telecomunicaciones
500 m2	3 m x 2.2 m
800 m2	3 m x 2.8 m
1.000 m2	3 m x 3.4 m

***TABLA 1**: Tamaños recomendados para la sala de telecomunicaciones*

***Fuente:** (Joskowicz, 2013)*

2.5.4. Canalizaciones Horizontales

Las "canalizaciones horizontales" son aquellas que vinculan las salas de telecomunicaciones con las "áreas de trabajo". Estas canalizaciones deben ser diseñadas para soportar los tipos de cables recomendados en la norma TIA-568, entre los que se incluyen el cable UTP de 4 pares, el cable STP y la fibra óptica.

- **Tipos de Canalizaciones**

  El estándar TIA-569 admite los siguientes tipos de canalizaciones horizontales:

  - Ductos bajo piso
  - Ductos bajo piso elevado
  - Ductos aparentes
  - Bandejas
  - Ductos sobre cielorraso

- Ductos perimetrales

➢ **Ductos Aparentes**

Ductos bajo piso Ductos bajo piso elevado Ductos aparentes Bandejas Ductos sobre cielorraso Ductos perimetrales no puede tener más de 30 m y dos codos de 90grados entre cajas de registro o inspección, el Radio de curvatura: Debe ser como mínimo 6 veces el diámetro de la canalización para cobre y 10 veces para fibra Si la canalización es de más de 50 mm de diámetro, el diámetro de curvatura debe ser como mínimo 10 veces el diámetro de la canalización

Los ductos aparentes pueden ser metálicos o de PVC, rígidos en ambos casos. No se recomiendan ductos flexibles para las canalizaciones horizontales. Las características de estos ductos y de su instalación deben ser acordes a los requisitos arquitectónicos y edilicios.

Se recomienda que no existan tramos mayores a 30 metros sin puntos de registro e inspección, y que no existan más de dos quiebres de 90 grados en cada tramo.

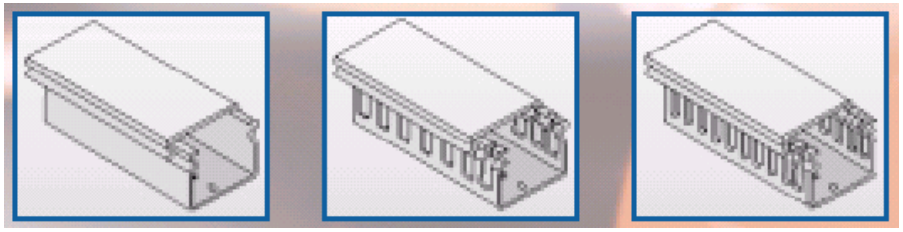


FIGURA 3: *Ductos aparentes de PVC*

Fuente: *(Joskowicz, 2013)*

➢ **Secciones de las Canalizaciones**

Las secciones de las canalizaciones horizontales dependen de la cantidad de cables que deben alojar y del diámetro externo de los mismos. En el diseño se debe recordar que cada área de trabajo debe disponer por lo menos de dos cables UTP (típicamente de diámetro entre 4.5 y 5.5 mm). Asimismo se debe tener en cuenta el crecimiento futuro, dejando espacio en las canalizaciones para cables adicionales.

- **Distancias a Cables de Energía**

La ANSI/EIA/TIA-569 establece las canalizaciones para los cables de telecomunicaciones deben estar adecuadamente distanciadas de las canalizaciones para los cables de energía.

- Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
- Cables de corriente alterna
- Mínimo 13 cm. para cables con 2KVA o menos
- Mínimo 30 cm. para cables de 2KVA a 5KVA
- Mínimo 91cm. para cables con más de 5KVA
- Luces fluorescentes y balastros (mínimo 12 centímetros). El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cms.)
- Equipo de soldadura
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).

2.5.5. Áreas de Trabajo

Son los espacios dónde se ubican los escritorios, boxes, lugares habituales de trabajo, o sitios que requieran equipamiento de telecomunicaciones.

Las áreas de trabajo incluyen todo lugar al que deba conectarse computadoras, teléfonos, cámaras de video, sistemas de alarmas, impresoras, relojes de personal, etc.

Si no se dispone de mejores datos, se recomienda asumir un área de trabajo por cada 10 m^2 de área utilizable del edificio. Esto presupone áreas de trabajo de aproximadamente 3 x 3 m. En algunos casos, las áreas de trabajo pueden ser más pequeñas, generando por tanto mayor densidad de áreas de trabajo por área utilizable del edificio.

Se recomienda prever como mínimo tres dispositivos de conexión por cada área de trabajo. En base a esto y la capacidad de ampliación prevista se deben prever las dimensiones de las canalizaciones.

2.6. SEGURIDAD INFORMATICA

De acuerdo con (Aida Noemy Domingo Sales, 2012) La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida)**.** Para ello existen una serie de estándares, protocolos, métodos, regias, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

2.6.1. Seguridad en Redes

En redes de computadoras, como en otros sistemas, su propósito es de reducir riesgos a un nivel aceptable, con medidas apropiadas. La seguridad comprende los tópicos siguientes:

- **Identificación:**(ID) es la habilidad de saber quién es el usuario que solicita hacer uso del servicio.
- **Autentificación:** Es la habilidad de probar que alguien es quien dice ser; prueba de identidad. Por ejemplo un password secreto que solo el usuario debe conocer.
- **Control de Acceso:** una vez que se sabe y se puede probar que un usuario es quien es, es sistema decide lo que le permite hacer.
- **Confidencialidad:** Es la protección de la información por la que garantiza que esta accesible únicamente a personal autorizado, para que no pueda ser vista ni entendida por personal no autorizado.
- **Integridad:** Es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.
- **No repudiación:** La no repudiación es la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que él enviador del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales.

2.6.2. OBJETIVOS DE LA SEGURIDAD

Generalmente, la seguridad informática consiste en garantizar que el material *y* los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Según (e-ducativa.catedu.es, 2016) El objetivo principal de la seguridad informática es garantizar que los recursos y la información estén protegidos y para protegerlo son necesarios conseguir los siguientes aspectos:

- **Integridad**.- sólo los usuarios autorizados podrán modificar la información.
- **Confidencialidad**.- sólo los usuarios autorizados tendrán acceso a los recursos y a la información que utilicen.
- **Disponibilidad**.- la información debe estar disponible cuando se necesite.
- **No repudio.-** el usuario no puede refutar o negar una operación realizada.

2.6.3. Seguridad Física y Lógica

- **Seguridad Física**

  De acuerdo con (e-ducativa.catedu.es, 2016) La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.

  Según se menciona en (uv.es, 2016) Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

  Se refiere a todos aquellos elementos de control tangibles que de una u otra forma limitan el seceso a un recurso o la ejecución de una tarea. Ejemplo de seguridad física lo constituyen una puerta, un vigilante, un detector de humo, cámaras de seguridad.

- **Seguridad Lógica**

  Tal como es descrito por (e-ducativa.catedu.es, 2016) La seguridad lógica de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y al información contenida en él.

De acuerdo a (Borghello, 2000 - 2009) Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.".

Es decir que la Seguridad Lógica consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.”

2.7. SERVICIO TÉCNICO INFORMÁTICO

Según (sales, 2016) El servicio técnico informático que brinda su ayuda físicamente. Responden a los usuarios de sus organizaciones y ejecutan automáticamente los programas de diagnóstico para resolver problemas. Además, pueden escribir manuales y capacitar en el uso de hardware y software nuevos mediante el soporte informático. Estos trabajadores, también, supervisan el funcionamiento diario de los sistemas informáticos de su empresa, la resolución de problemas técnicos con redes de área local (LAN), redes de área amplia (WAN), y otros sistemas. A continuación encontrará algunas ventajas que ofrece este servicio:

- Ofrece varias modalidades para acomodarse a sus necesidades.
- Maximiza los recursos de su computadora.
- Provee un servicio intuitivo y seguro.
- Brinda una respuesta rápida y segura a su problema.

2.8. FIREWALL

Según (Cisco, 2016) Un cortafuego (firewall en inglés) es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos.

FIGURA 4: *Principio fundamental del Firewall*

Fuente: *(CiscoASA, 2015)*

2.8.1. Sistema de Prevención de Intrusos(IPS)

Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS fueron inventados de forma independiente por Jed Halle y Vem Paxon para resolver ambigüedades en la monitorización pasiva de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las

tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Tiempo después, algunos IPS fueron comercializados por la empresa One Secure, la cual fue finalmente adquirida por NetScreen Technologies, que a su vez fue adquirida por Juniper Networks en 2004. Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación.

El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como o IDS (tradicionalmente colocado como un rastreador de puertos en la red).

El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc.). (Seguridad, 2016)

- **Ventajas**
  - Protección preventiva antes de que ocurra el ataque
  - Defensa completa (Vulnerabilidades del Sistema Operativo, Puertos, Trafico de IP, códigos maliciosos e intrusos)
  - Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
  - Fácil instalación, configuración y administración
  - Es escalable y permite la actualización de dispositivos a medida que crece la empresa

- **Características de un IPS**
  - Capacidad de reacción automática ante incidentes
  - Aplicación de nuevos filtros conforme detecta ataques en progreso.
  - Mínima vigilancia

- Disminución de falsas alarmas de ataques a la red
- Bloqueo automático frente a ataques efectuados en tiempo real
- Optimización en el rendimiento del tráfico de la red

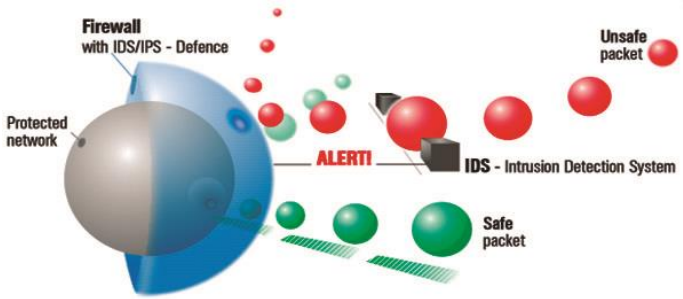


FIGURA 5: *Esquema de funcionamiento de IPS*

Fuente: *(trendcorp, 2014)*

2.8.2. Dispositivo de Seguridad Cisco SA 540

Es un dispositivo que constituye soluciones de seguridad "todo en uno" ideales para empresas en crecimiento. La combinación de Internet de alta seguridad, de los servicios inalámbricos, de las conexiones de sitio a sitio y del acceso remoto, con los servicios de firewall y las capacidades de seguridad para el sistema de prevención de intrusiones, el correo electrónico y el contenido, este dispositivos de Cisco SA 540 proporcionan a las empresas en crecimiento la certeza de que su red cuenta con la protección adecuada. (Cisco, 2010)

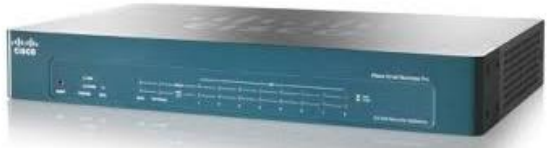


FIGURA 6: *Dispositivo de seguridad Cisco SA 540*

Fuente: *(Cisco, 2010)*

- **Funciones**
  - Un firewall con inspección de estado de paquetes integrado y el sistema de prevención de intrusiones proporcionan protección de clase empresarial contra visitantes o tráfico no deseado y ataques maliciosos.
  - El perímetro de red sin protección (DMZ[11]) aloja con un alto nivel de seguridad servidores de archivos, servidores web y otros servidores accesibles a través de Internet sin exponer la red de área local interna de la empresa a ninguna amenaza.
  - Su galardonada tecnología contra virus, software espía, correos electrónicos no deseados y ataques de suplantación de identidad utiliza ocho técnicas diferentes de inspección para evaluar la dirección IP del emisor y explorar el contenido del correo electrónico, haciendo uso de más de 3 millones de patrones diferentes de virus y más de 400.000 patrones de software espía para optimizar la precisión.
  - Los bloques de filtrado de Web y de URL reconocen los sitios web maliciosos mientras limitan el uso de Internet del empleado a sitios web apropiados o relacionados con su trabajo.
  - La conectividad Gigabit Ethernet en todos los puertos brinda el rendimiento máximo de la red.
- **Ventajas**

[11] Zona desmilitarizada o red perimetral

- Mejora la productividad de los empleados, ya que bloquea correos electrónicos no deseados y software espía, además de impedir la inadecuada navegación por Internet.
- Mejora la capacidad de recuperación de la empresa, ya que evita la alteración de servicios y aplicaciones fundamentales por violaciones a la seguridad o interrupciones en la red, gracias a un firewall de clase empresarial, seguridad avanzada contra correo no deseado y amenazas de Internet, y capacidad de doble conexión WAN.
- Aumenta la eficacia operativa al evitar que los recursos de soporte de TI se destinen a la eliminación de software espía y malicioso.
- Aumenta la movilidad y capacidad de respuesta de los empleados, ya que permite el acceso remoto a través de una red privada virtual con un alto nivel de seguridad.
- Reduce los riesgos de violaciones a la seguridad, ya que realiza un exhaustivo control de acceso e incluye un completo conjunto de servicios de protección contra amenazas.

CAPITULO III

3.MARCO METODOLÓGICO

3.1. MODELO FUNCIONAL PARA LA ADMINISTRACIÓN DE REDES

Se describe una metodología de redes de datos basada en modelos funcionales estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

3.2. ADMINISTRACIÓN DE LA CONFIGURACIÓN

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

3.2.1. Planeación y Diseño de la Red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser
    - Multicast,
    - Voz sobre IP (VoIP),
    - Calidad de servicio (QoS), etc.

Algunas necesidades cuantitativas pueden ser

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a Gigabit Ethernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red
c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.
e) Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

3.2.2. Selección de la Infraestructura de Red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

3.2.3. Instalaciones y Administración del Software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

a) Instalaciones de Hardware

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.
- Documentar el cambio para futuras referencias.

b) Administración del Software.

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

- Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de tftp.

3.2.4. Provisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

- Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

3.2.5. Políticas y Procedimientos Relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

3.3. ADMINISTRACIÓN DEL RENDIMIENTO

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

3.3.1. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) Utilización de enlaces

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) Utilización de procesamiento

Es importante conocer la cantidad de procesador que un servidor esta consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

3.3.2. Análisis.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) Utilización elevada.

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b) Tráfico inusual.

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) Elementos principales de la red.

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) Calidad de servicio.

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

3.3.3. Interacción con otras Áreas

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

3.4. ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- Localización de fallas. Determinar el origen de una falla.
- Pruebas de diagnóstico. Diseñar y realizar pruebas que apoyen la localización de una falla.
- Corrección de fallas. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- Administración de reportes. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.
- Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

3.4.1. Monitoreo de Alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También

conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

- **Tipo de las Alarmas**
  - Alarmas en las comunicaciones. Son las asociadas con el transporte de la información, como las pérdidas de señal.
  - Alarmas de procesos. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.
  - Alarmas de equipos. Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
  - Alarmas ambientales. Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
  - Alarmas en el servicio. Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.
- **Severidad de las Alarmas.**
  - Crítica. Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

- Mayor. Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- Menor. Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.
- Indefinida. Cuando el nivel de severidad no ha sido determinado por alguna razón.

3.4.2. Localización de Fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

- **Pruebas de diagnóstico**

  Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- **Pruebas de conectividad física.**

  Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- **Pruebas de conectividad lógica.**

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

- **Pruebas de medición.**

  Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

3.4.3. Corrección de Fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- Reemplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- Aislamiento del problema. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- Redundancia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- Instalación de software. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

3.4.4. Administración de Reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

- **Creación de Reportes**

  Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte de be contener al menos la siguiente información:

  - El nombre de la persona que reportó el problema
  - El nombre de la persona que atendió el problema o que creó el reporte del mismo.
  - Información técnica para ubicar el área del problema
  - Comentarios acerca de la problemática.
  - Fecha y hora del reporte

- **Seguimiento a Reportes**

  La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc., y este debe poder ser consultada en cualquier momento por el administrador.

- **Manejo de Reportes**

  El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

- **Finalización de Reportes**

  Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

3.5. ADMINISTRACIÓN DE LA CONTABILIDAD

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

3.6. ADMINISTRACIÓN DE LA SEGURIDAD

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

3.6.1. Prevención de Ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

3.6.2. Detección de Intrusos

El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

3.6.3. Respuesta a Incidentes

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

3.6.4. Políticas de Seguridad

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

3.6.5. Servicios de Seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. Identifica el "que".

De acuerdo a la Arquitectura de Seguridad OSI, un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

3.6.6. Mecanismos de Seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

3.6.7. Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.
- Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.
- Implementar las política de seguridad mediante los mecanismos adecuados

3.7. HERRAMIENTAS

3.7.1. Smartpss

Sistema inteligente de Productos de Seguridad (SmartPSS) es un sistema de gestión donaciones de software que tengan acceso a todos los productos de seguridad Dahua. SmartPSS es ampliamente Se utiliza con la mayoría de los sistemas de vigilancia y de intercomunicación Dahua insmall al medio proyectos. SmartPSS mantiene la facilidad de uso fácil, así como una gran funcionalidad.

Vigilar, revisar material de archivo, búsqueda inteligente, alarmas inteligentes, seguimiento inteligente, cada funcionalidad está a su disposición de forma gratuita.

3.7.2. Packet Tracer

Cisco Packet Tracer es un potente programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red y preguntar "¿qué pasa si". Como parte integral de la experiencia de aprendizaje integral de la Academia de Redes, Packet Tracer proporciona capacidades de simulación, visualización, creación, evaluación y colaboración y facilita la enseñanza y aprendizaje de conceptos tecnológicos complejos.

Packet Tracer complementa el equipo físico en el aula permitiendo a los estudiantes crear una red con un número casi ilimitado de dispositivos, fomentando la práctica, descubrimiento y solución de problemas. El entorno de aprendizaje basado en la simulación ayuda a los estudiantes a desarrollar habilidades del siglo XXI como la toma de decisiones, el pensamiento creativo y crítico y la resolución de problemas. Packet Tracer complementa los currículos de Networking Academy, permitiendo a los instructores enseñar y demostrar fácilmente conceptos técnicos complejos y diseño de sistemas de redes.

El software Packet Tracer está disponible de forma gratuita solo a los instructores, estudiantes, ex alumnos y administradores de Networking Academy que sean usuarios registrados de Academy Connection.

3.7.3. Microsoft Visio

Microsoft Visio es un software de dibujo vectorial para Microsoft Windows. Microsoft compró la compañía Visio en el año 2000.

Las herramientas que lo componen permiten realizar diagramas de oficinas, diagramas de bases de datos, diagramas de flujo de programas, UML, y más, que permiten iniciar al usuario en los lenguajes de programación.

El navegador Internet Explorer incluye un visor de diagramas Visio, cuya extensión es vsd, llamado Visio Viewers.

Aunque originalmente apuntaba a ser una aplicación para dibujo técnico para el campo de Ingeniería y Arquitectura; con añadidos para desarrollar diagramas de negocios, su adquisición por Microsoft implicó drásticos cambios de directrices de tal forma que a partir de la versión de Visio para Microsoft Office 2003 el desarrollo de diagramas para negocios pasó de añadido a ser el núcleo central de negocio, minimizando las funciones para desarrollo de planos de Ingeniería y Arquitectura que se habían mantenido como principales hasta antes de la compra. Una prueba de ello es la desaparición de la función "property line" tan útil para trabajos de agrimensura y localización de puntos por radiación, así como el suprimir la característica de ghost shape que facilitaba la ubicación de los objetos en dibujos técnicos. Al parecer Microsoft decidió que el futuro del programa porque residía en el mundo corporativo de los negocios y no en las *mesas de dibujo* de Arquitectos e Ingenieros compitiendo con productos como AutoCad, DesignCad, Microstation, etc.

En sus orígenes aplicaba más al ramo de Ingeniería, pero hoy en día es fundamental en el análisis de procesos y operaciones en las empresas.

CAPITULO IV

4.MARCO INSTITUCIONAL

4.1. UNIVERSIDAD AMAZÓNICA DE PANDO

Según (UAP, 2016), La Universidad Amazónica de Pando, fue creada mediante Decreto Supremo N° 20511 del 21 de septiembre de 1984 y sancionada mediante Ley de la Nación N° 653 de 18 de Octubre de 1984. Además, menciona que El Estatuto Orgánico de la UAP fue aprobado en la VI Conferencia Nacional de Universidades en octubre de 1997 y por el Congreso Nacional de Universidades el mes de mayo de 1999, ambos eventos realizados en la ciudad de Trinidad – Beni.

4.1.1. Historia de la Universidad Amazónica de Pando

La Universidad Amazónica de Pando, se encuentra ubicada en la ciudad de Cobija, capital del departamento Pando, en el extremo norte del territorio nacional, en plena región amazónica.

Las actividades académicas comenzaron oficialmente el 3 de diciembre de 1993, con dos Carreras: Licenciatura en Biología y Licenciatura en Enfermería.

Asimismo, En agosto de 1996 se incorporó la carrera de Informática a nivel de Técnico Superior. Posteriormente, consecuente con la política de diversificación de la oferta curricular, a partir de la gestión académica del 2000 se crearon los siguientes programas académicos:

a) Ingeniería Agroforestal, a Nivel de Licenciatura.
b) Derecho, con mención en derecho ambiental, a nivel de Licenciatura.
c) Construcción Civil, a nivel de Técnico Superior.
d) Pesca y Acuicultura, también a nivel de Técnico Superior.

Por otro lado, se aprobó el cambio del grado académico de la carrera de Informática a nivel de Licenciatura como Ingeniería Informática. En la gestión del 2001, se aprobó la apertura del Programa de Ciencias Económicas y Financieras, con las carreras de: Economía, Administración de Empresas y Contaduría Pública a nivel de Licenciatura. En la gestión del 2004 se aprobó la creación del Área de Ciencias Sociales con dos carreras: Ciencias de la Comunicación Social y Trabajo Social a nivel de Licenciatura, para su puesta en marcha se contó con el apoyo financiero de la Prefectura del Departamento Pando.

En la gestión académica 2006, se dio apertura a las carreras de Ingeniería civil e Ingeniería en Tecnología de la Madera a nivel licenciatura y la implementación del Centro Tecnológico Puerto Rico, con las carreras de Guardabosques, Pesca y Acuicultura y Sistemas de producción Agropecuaria, estas últimas a nivel de Técnico Superior. Finalmente, en la gestión académica 2007 se dio apertura a la Unidad Académica las Piedras, en el Municipio de Gonzalo Moreno, con las carreras de Turismo Sostenible y Administración de Empresas.

4.1.2. Misión Institucional

Institución Pública y Autónoma de Educación Superior, que forma profesionales idóneos, con excelencia académica, pensamiento crítico y compromiso social, que desarrolle la investigación científica y tecnología, promoviendo la interacción social, en un contexto de diversidad social e interculturalidad, para contribuir al desarrollo integral de nuestra amazonia.

4.1.3. Visión Institucional

En el año 2017 la Universidad Amazónica de Pando será una Universidad Autónoma, transparente, desconcentrada, incluyente, con libertad de pensamiento, comprometida con su población, que brinde profesionales de excelencia académica, investigación científica y tecnología pertinente hacia su entorno; enfocada en una gestión moderna y flexible basada en resultados, con todos sus programas acreditados, orientados al bienestar de la comunidad universitaria para contribuir al desarrollo integral de nuestra amazonia.

4.2. DIRECCIÓN DE INFORMACIÓN ACADÉMICA

La Dirección de Información Académica dependiente del Vicerrectorado es la instancia que presta servicios de apoyo logístico y administrativo de toda actividad académica y de información que se lleva a cabo en la Universidad Amazónica de Pando.

La dirección de información académica, se inicia el 2003 donde se presenta un proyecto denominado "Proyecto de Organización de la Dirección de Información Académica (DIA)", cuya misión es promover, orientar y administrar, la información académica de estudiante y docentes en la U.A.P en forma transparente, eficiente y oportuna a través de nuevas tics. Este proyecto se pone en ejecución el mismo año, la cual cuenta con cuatro unidades las cuales coadyuvan en la mejora del servicio, los cuales son: Unidad de Trámites y Registros (UTR), Unidad de Archivo Académico Universitario (UAAU), Unidad de Informaciones (UI) e Unidad de Sistemas Académicos (USA), cada uno de ellos son pilares fundamentales de las transformaciones y mejoras en los servicios académicos que brinda nuestra dirección.

4.2.1. Misión

Somos una dirección técnica de gestión de la información, que brinda un servicio eficiente a la comunidad universitaria y población en general, utilizando nuevas tecnologías de información y comunicación, para contribuir al desarrollo académico administrativo en la Universidad Amazónica de Pando.

4.2.2. Visión

Ser una dirección técnica transparente en la gestión de la información, que brinda un servicio óptimo con calidad, a la comunidad universitaria y población en general, utilizando modernas tecnologías de información y comunicación; siendo un referente institucional en la Universidad Amazónica de Pando y contribuyendo al desarrollo académico del sistema universitario nacional.

4.2.3. Objetivo

Mejorar continuamente y sistemáticamente los servicios académicos y de información con el uso de las modernas Tecnologías de la Información y Comunicación TIC, con el fin de fortalecer la gestión académica de la Universidad Amazónica de Pando.

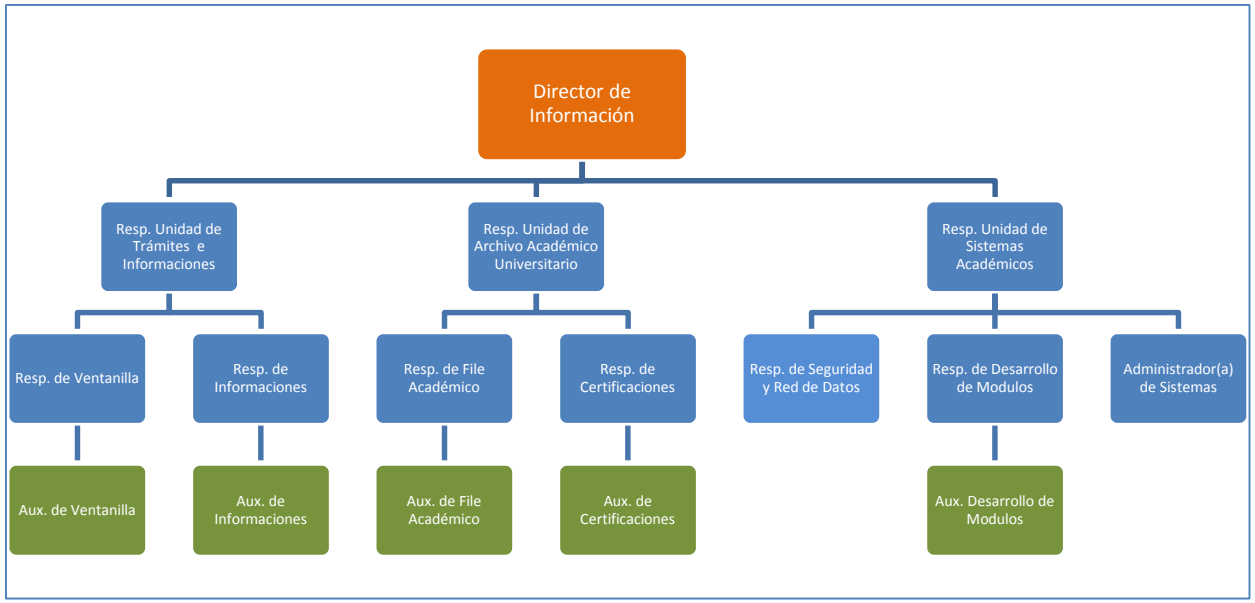


FIGURA 7: *Organigrama de la Dirección de Información Académica*

Fuente: *Dirección de Información Académica*

CAPITULO V

5.MARCO APLICATIVO

5.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN (AC)

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware.

5.1.1. Actividad AC 1: Planeación y Diseño de la Red

- **Etapa 1: Reunir las Necesidades de la Red**

Como parte de la planeación y diseño de la red de datos se vio en la necesidad de reunir las necesidades de la red, las mismas fueron tecnológicas, cuantitativas, para ello se realizó la determinación de la tecnología de la red de la Dirección de Información Académica, la cual será de tipo broadcast (radiodifusión).

Con respecto a las necesidades cuantitativas de la red se identificó la cantidad de nodos, conmutadores, tipo de hardware y Software requeridos en la Dirección de Información Académica, como se muestra en la tabla 2, del mismo modo se consideró la cantidad de nodos requeridos a futuro, considerando también los espacios de los conmutadores.

UNIDADES	CANTIDAD DE NODO PARA FUNCIONARIOS	CANTIDAD DE NODOS PARA EQUIPOS DE SEGURIDAD Y SERVIDORES	CANTIDAD DE NODOS A FUTURO	CANTIDAD DE CONMUTADOR	HARDWARE SOFTWARE REQUERIDO
Unidad de Trámites y Registros	5	3	2	1	Computadoras Cable UTP Cat. 6

Unidad de Informaciones	4	3	2		Windows Antivirus, adobe, office etc.
Unidad de Archivo Académico Universitario	8	3	2	1	Computadoras Tarjeta de red Cable UTP Cat. 6 Windows Antivirus, adobe, office etc.
Unidad de Sistemas Académicos	9	7	3	1	Servidor Computadora Firewall Cable UTP Cat. 6 Windows, Ubuntu Ubuntu server Antivirus, adobe, office etc.
Dirección de la DIA	4	2	2	1	Computadoras Cable UTP Cat. 6 Windows Antivirus, adobe, office etc.

TABLA 2: Necesidades de la tecnológicas y cuantitativas de la red.
Fuente: Elaboración Propia

La Dirección de Información Académica cuenta con una estructura de 4 ambientes que corresponden a cada una de sus Unidades, la misma consta de 26 equipos de computación distribuidos en cada uno de sus ambientes. Los mismos son utilizados por sus funcionarios de esta Dirección.

Cabe mencionar que las necesidades de la red ayudaron en el diseño y planeación de la nueva red de datos, del mismo modo se realizó el diagnóstico de la Red de Datos, ver detalle del diagnóstico en Anexo B. Este servicio de análisis y diagnóstico de redes permite

encontrar deficiencias en la red de datos y sus causas, u oportunidades de mejora, y formular acciones correctivas y de mejoramiento. Este servicio se complementa con el de optimización de la red, en donde se implementan estas acciones.

- **Etapa 2: Diseñar la topología de la red**

Esta etapa tiene como objetivo determinar la topología de red la misma se tomó las consideraciones del estándar ANSI/TIA/EIA-568, la misma establece las consideraciones a tomar para el cableado de distribución horizontal.

Para realizar esta actividad se hizo uso de la herramienta Packet Tracer, el mismo es un potente simulador de red.

- **Diseño de la Topológico Actual de la Red de Datos de la Dirección de Información Académica**

  El diseño de la Red de Datos de la Dirección de Información Académica actualmente está compuesto por 5 conmutadores[12] y un firewall Cisco SA 540 que tienen una conexión por cableado al área de trabajo, los cuales están distribuidos en los diferentes ambientes del predio de la Dirección de Información Académica como se muestra en la figura 8, el diseño y la cantidad de conmutadores en funcionamiento actual no satisface las necesidades de los usuarios, motivo que ha generado algunos percances, uno de ellos son los corte constantes de los servicios prestados por dicha Unidad.

[12] Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos.

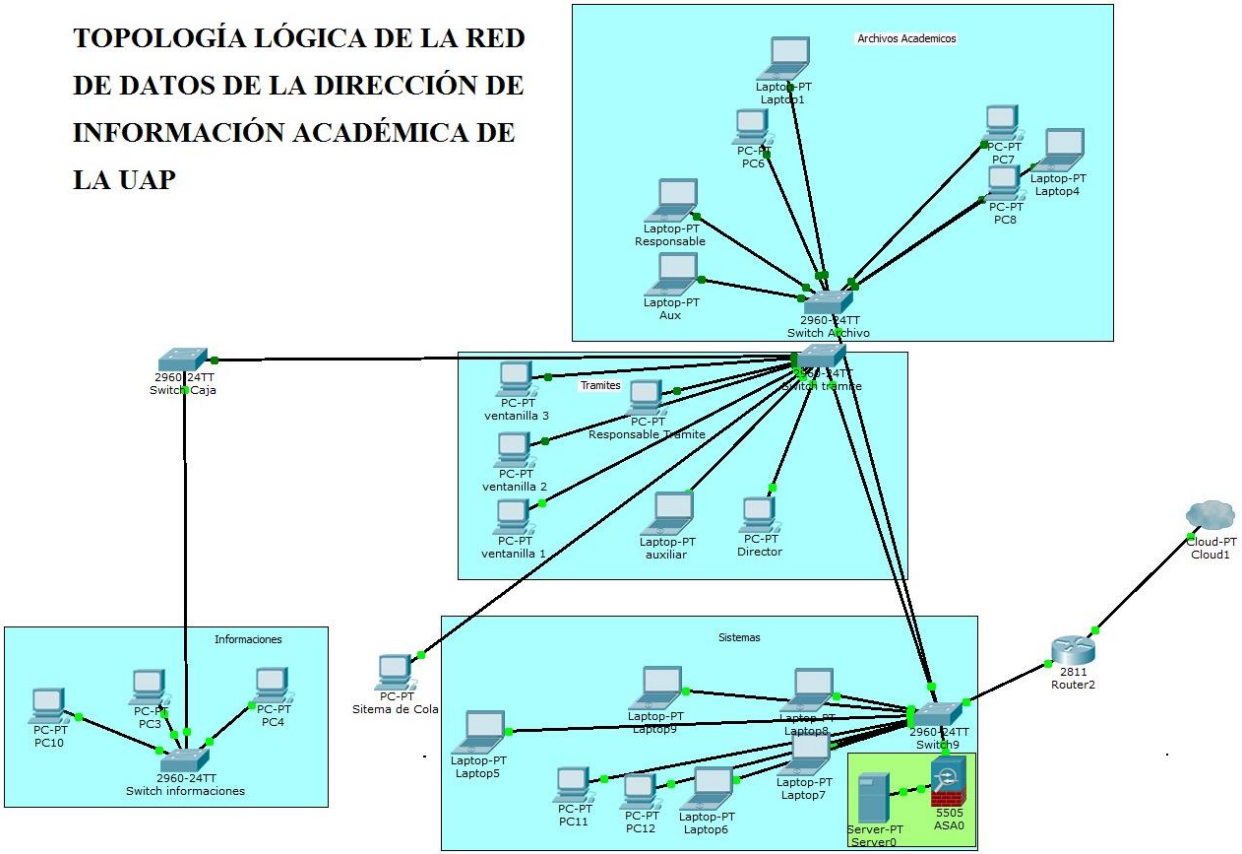


FIGURA 8: *Diseño lógico actual de la Red de Datos de la Dirección de Información Académica*
Fuente: *Elaboración propia*

- **Propuesta Topológica y Diseño Lógico de la Red de Datos de la Dirección de Información Académica**

Como parte de la gestión de la configuración y los percances ocurridos tales como: pérdidas de los servicios que se tiene en la Dirección de Información Académica, se determina diseñar un nuevo diseño lógico acorde a los estándares ANSI/TIA/EIA-568, la misma establece las consideraciones a tomar para el cableado de distribución horizontal la misma establece una topología es estrella.

Se realizó el diseño lógico de la red, haciendo uso de la herramienta Packet Tracer para el modelado de la red de datos y para la representación de las conexiones de cada nodo a los equipos de la red, para ello se utilizó la topología estrella extendida, donde cada equipo solamente tendrá un enlace de punto a punto dedicado con el conmutador, para la distribución de 4 conmutadores encada uno de los ambientes de la Dirección de Información Académica, cada conmutador consta de 24 puertos considerando el crecimiento de los usuarios.

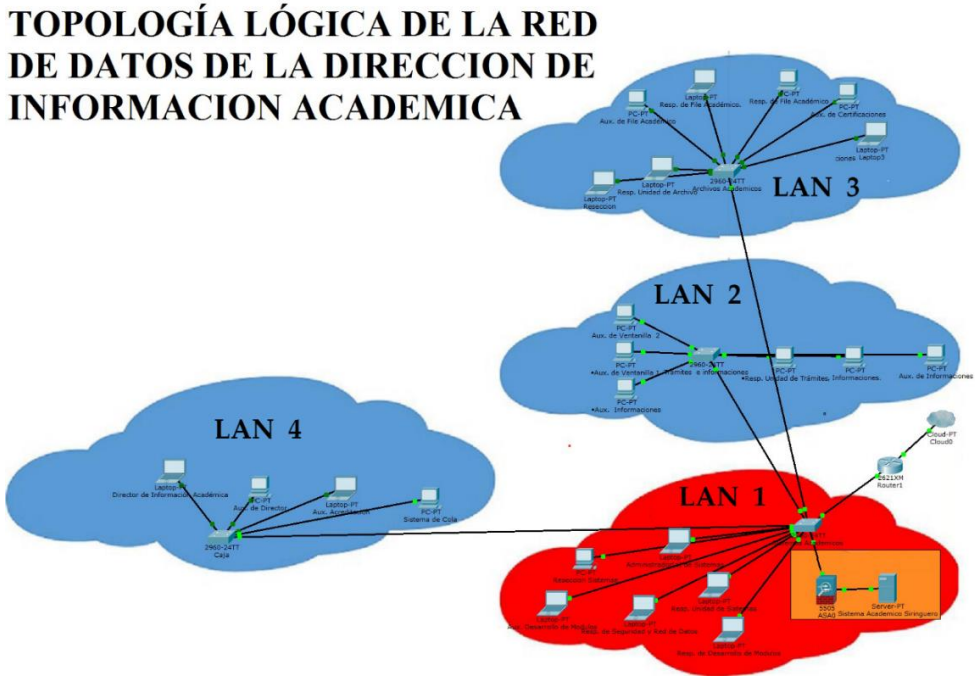


FIGURA 9: *Propuesta de Diseño Lógico de la Red de Datos de la Dirección de Información Académica*
Fuente: *Elaboración propia*

A continuación se puede observar las figuras más detalladas de con su respectiva configuración y nodos en cada Lan[13].

- **LAN 1: UNIDAD DE SISTEMAS ACADÉMICOS**

[13] Red de Área Local

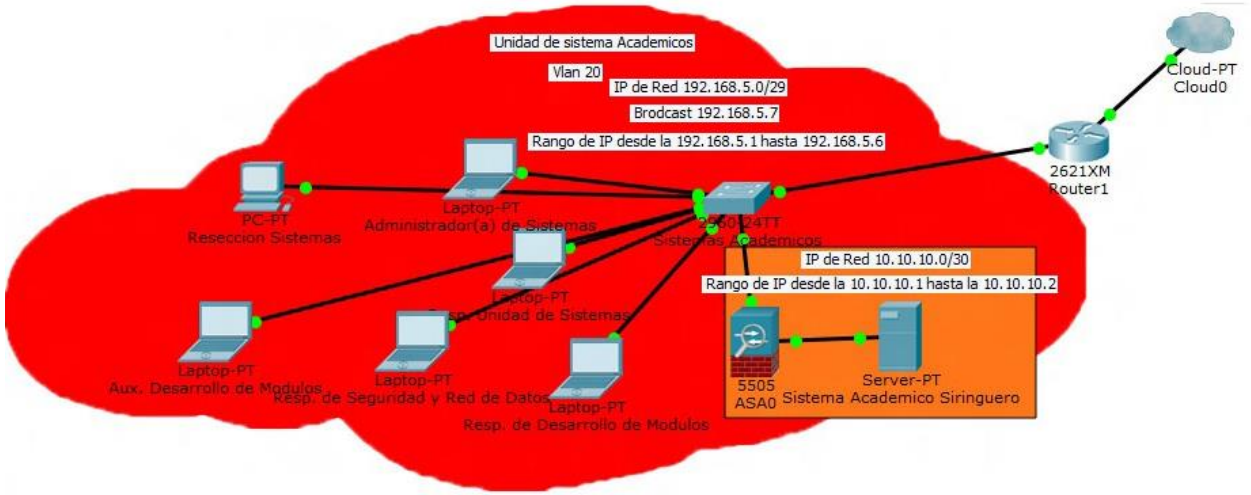


FIGURA 10: *Diseño lógico de la Lan 1 perteneciente a la Unidad de Sistemas Académicos del DIA.*
Fuente*: Elaboración propia*

Dentro de esta Lan 1 se puede apreciar que cuenta con otra Red interna la misma es una red perimetral o segura cuya función es proteger la red interna y los servicios que son brindados por ella, en este caso se cuenta con el Servidor del Sistema Siringuero integrado a esta red perimetral o DMZ[14], del mismo modo se puede apreciar la cantidad de nodos con la que cuenta en esta Lan.

Del mismo modo dentro de esta Lan se cuenta con una red de área virtual Vlan 20 la misma proporciona seguridad a la hora de la trasmisión de datos e información hacia el Servidor de la Unidad de Sistemas Académicos.

[14] Es seguridad es una zona desmilitarizada o red perimetral.

- **LAN N° 2,3 y 4**

Estas tres lan no tienen configuraciones adicionales, solo se propone que realicen un mejor orden en las configuraciones de direcciones IP, se puede observar la propuesta en las diferentes figuras, como también en la tabla 3.

Cada una de estas tres Lan corresponden a las diferentes Unidades del DIA tales como: Unidad de Tramite y Registros, Unidad de Informaciones, Archivos Academicos, y a la direccion del DIA.

- **LAN 2:UNIDAD DE TRAMITE Y REGISTROS, UNIDAD DE INFORMACIONES**

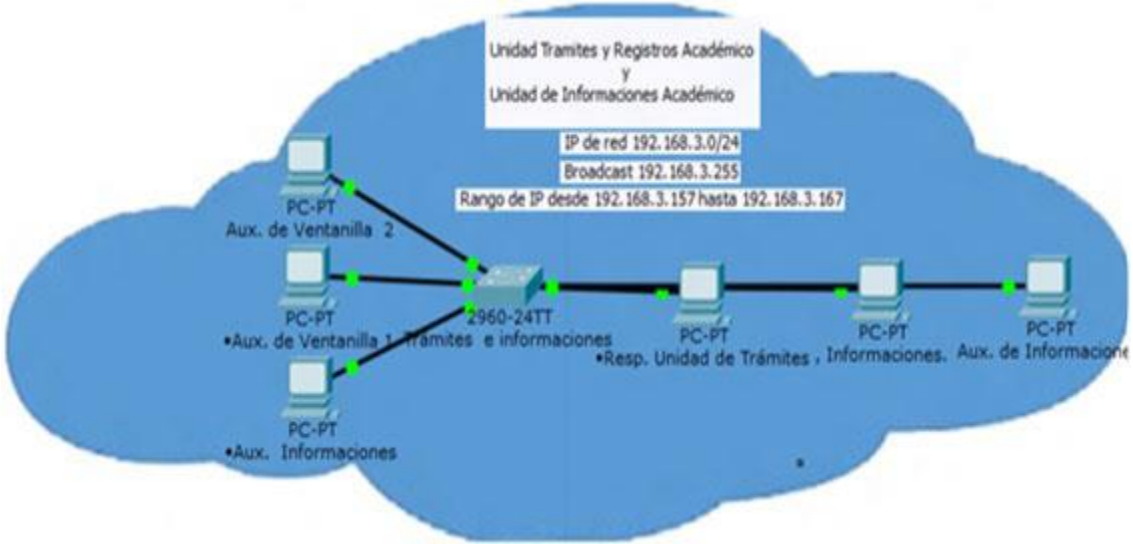


FIGURA 11: *Diseño lógico de la Lan 2 perteneciente a la unidad tramites y informaciones Académicos del DIA*
Fuente*: Elaboración propia*

- **LAN 3: UNIDAD DE ARCHIVOS ACADÉMICOS**

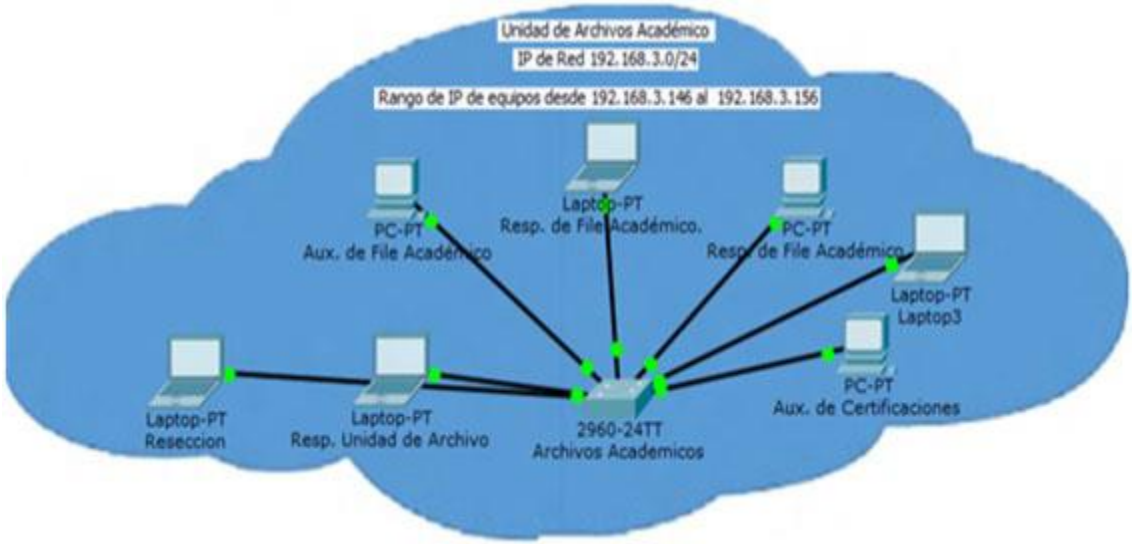


FIGURA 12: *Diseño lógico de la Lan 3 perteneciente a la Unidad de Archivos Académicos del DIA*
Fuente: *Elaboración propia*

- **LAN 4: DIRECCIÓN DEL DIA**

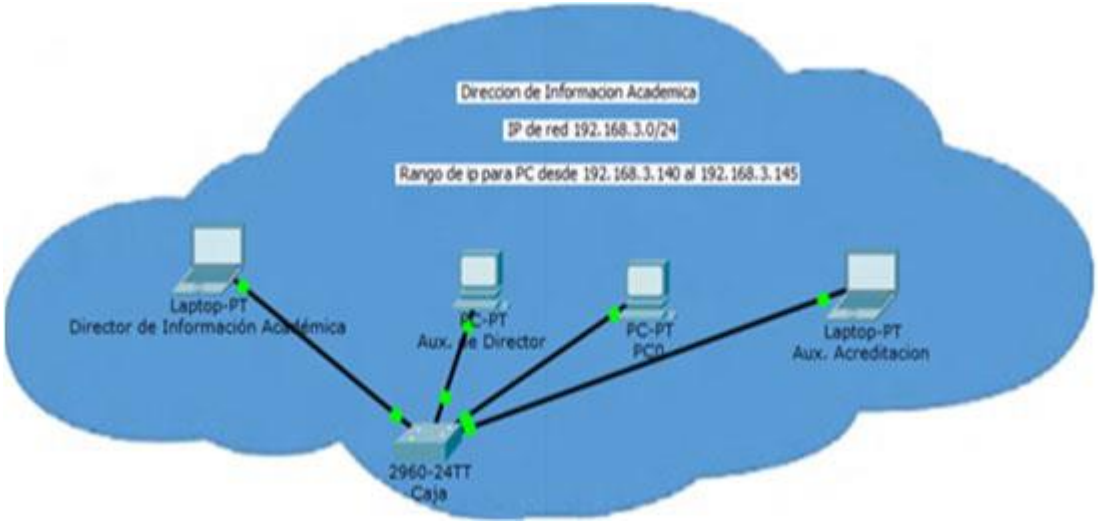


FIGURA 13: *Diseño lógico de la Lan 4 perteneciente a la Dirección del DIA*
Fuente*: Elaboración propia*

La configuración de las direcciones IP de los equipos en el transcurso del Trabajo Dirigido, se la realizó en coordinación con el administrador de la red de la Universidad Amazónica de Pando dependiente de la Unidad de Sistemas de Información y Comunicación (USIC), en la tabla 3 se muestra la propuesta de las configuraciones de las direcciones IP, la cual es para tener un mejor orden en la direcciones IP de cada unidad, como también para que se prevea las direcciones IP necesarias, tomando en cuenta el crecimiento de los usuarios en cada Unidad del DIA.

Nº	Detalle	Direcciones de IP`S	Puerta de enlace
1	Dirección de Información Académica	192.168.3.140 al 192.168.3.145	255.255.255.0
2	Unidad de Archivos Académico	192.168.3.146 al 192.168.3.156	255.255.255.0

3	Unidad Tramites y Registros Académico	192.168.3.157 al 192.168.3.167	255.255.255.0
4	Unidad de Sistemas Académico(Vlan)	192.168.5.1 al 192.168.5.6	255.255.255.248

TABLA 3: *Propuesta de orden de direcciones IP para la Dirección de Información Académica*
Fuente: *Elaboración propia*

- **Diseño Físico de la Red de Datos actual de la Dirección de Información Académica**

Como anteriormente se avía mencionado que la Dirección de Información Académica tenía algunos percances en el diseño lógico de la red de datos, de la misma forma sucede en el diseño físico, lo cual dificulta la conexión adecuada a cada uno de los equipos con los que se cuenta, cabe mencionar que la conexión actual no cumple las normas y estándares de cableado estructurado como se muestra en las figuras 14,15.

FIGURA 14: *Estado de la Red de Datos de la Dirección de Información Académica inicio*
Fuente: *Elaboración propia*

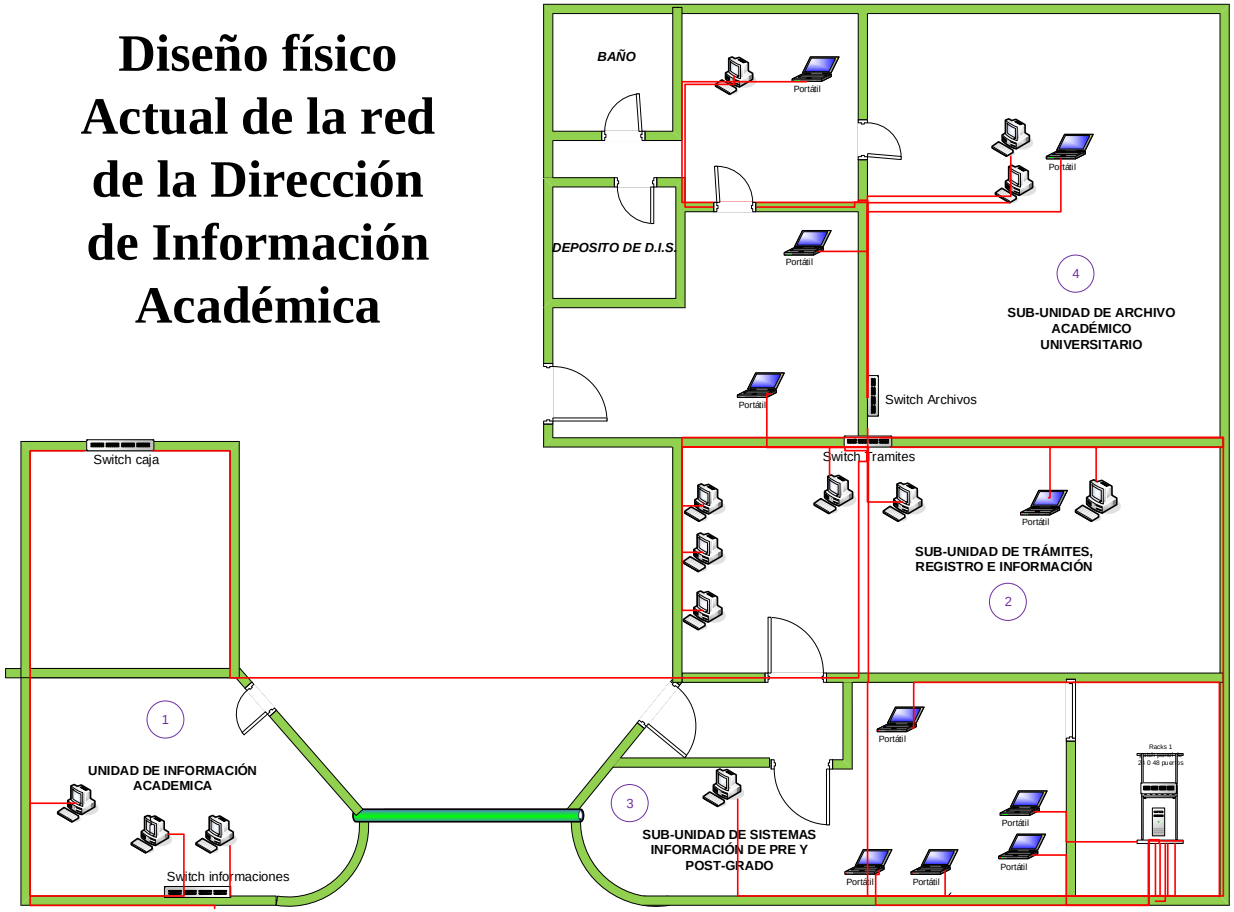


FIGURA 15: *Diseño físico Actual de la dirección de información Académica*
Fuente: *Elaboración propia*

- **Propuesta del Diseño Físico de la Red de Datos de la Dirección de Información Académica**

Para garantizar el mejor funcionamiento de la red de datos se vio por conveniente proponer reorganizar el cableado en los predios de la Dirección de Información Académica.

Para la propuesta del nuevo diseño físico de la red de datos se tomó en cuenta los requerimientos, el estándar ANSI/TIA/EIA-569 que provee especificaciones para el diseño de las instalaciones en estructuras edilicia para el cableado estructurado y lo plasmado en el diseño lógico, para ver las conexiones de cada uno de los equipos a los conmutadores con los que contará la nueva red de datos. El nuevo diseño físico de la red de datos estará conectado por cableado estructurado que cumple las normas y estándares internacionales, por el cual brindará una red óptima segura y confiable para la distribución de cada uno de los servicios, como se muestra en la figura 16.

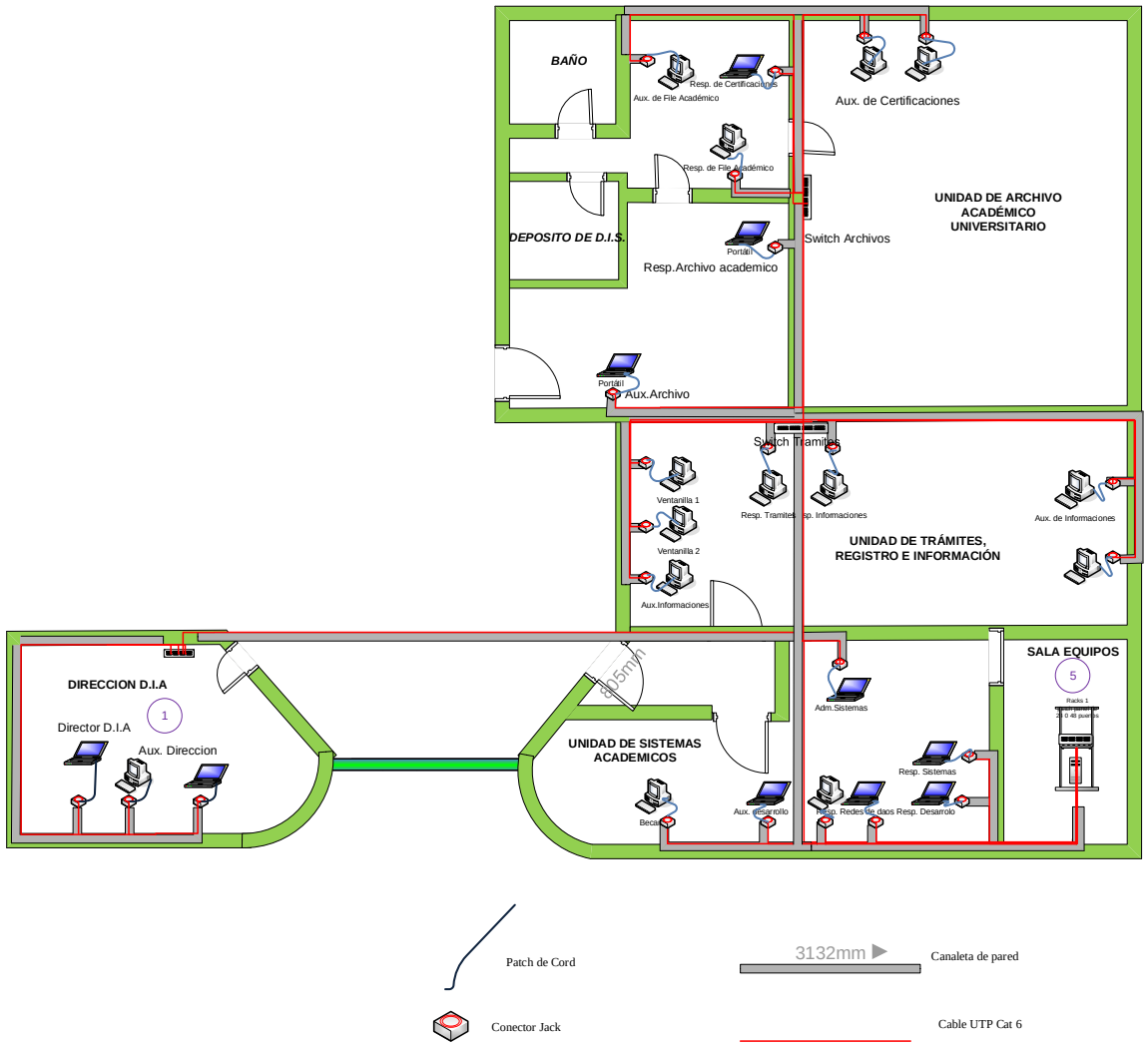


FIGURA 16: *Propuesta del diseño físico de la Red de Datos de la Dirección de Información Académica*
Fuente: *Elaboración propia*

La nueva estructura de la Red de Datos está basado en los requerimientos y normas internacionales, por las problemáticas presentadas se plantea la nueva estructura a base de 4 conmutadores y un firewall para la configuración de la red, y de la nueva Vlan que se realizó, a continuación se muestra de forma individual los diseños de cada Unidad con su respectiva cotización de materiales requerido para su implementación la cotización que se realizó individual por unidad no contempla la mano de obra la misma varia de entre los 70 bs a 105 bs por punto o nodo implementado, cual se realiza la estimación de nodos requeridos multiplicado por punto implementado..

- **Cotización de los dispositivos para la Red de Datos de la Dirección en General.**

  Se ha realizado la cotización del material requerido para la Red de Datos contemplando el material existente con el que cuenta la Dirección de Información académica, la misma reduce en los costos, en el caso que fuera un cableado de Red nueva los costos serían más elevados, la tabla 4 muestra los costos de cada dispositivo que se requiere para la implementación, cabe mencionar que la misma tabla no contempla el costo de la mano de obra, la misma los precio varían entre los 70 bs a 105 bs por punto puesto, la cual se requiere 30 puntos como mínimo contemplando el aumento de los usuarios.

Nº	Descripción	Cantidad	Costo Unitario	Total
1	Conector Jack Keystone Femea Cat-6 Certificado	30	18.34	550
2	Mini Rack 9u X 680mm 19 negro	3	720	2160
3	Organizador de Cable de 2U P/Rack	4	65	260
4	Patch Panel cat 6 de 24 Puertos	4	420	1680
5	Patch de Cord de 1 Mts cat 6	30	20.50	615
6	Switch de Cisco 28 Puerto	2	6595	13190
7	Patch Cord de 0,5 Mts para Terminación en Rack	30	17	510
8	Cable UTP Nexx Cat 6	2	2700	5400
9	Conector RJ-45	30	3.5	105
9	Canaleta de pared cat grande	1	80	80

10	Canaleta 20*10*2MT	90	5.83	519
Costo Total de la los materiales requeridos				**25069**

TABLA 4: *Cotización de los materiales de red*

Fuente: *Elaboración propia*

Como se puede observar en la siguiente figura más detalles del diseño físico de la red de datos de la Unidad de Sistemas Académico, Tramites y Registro y de Información Académico, Unidad de Archivos Académico, del mismo modo se muestran las tabla la cotización de dispositivos que se requerirá para la implementación en las tablas de cotización no contempla los costó de implementación de cada nodo, lo cual los precios pueden variar de 70 a 105 por nodo implementado.

- **Diseño físico y Tabla de Cotización de los dispositivos de la Red de Datos de la Unidad de Sistemas Académicos.**

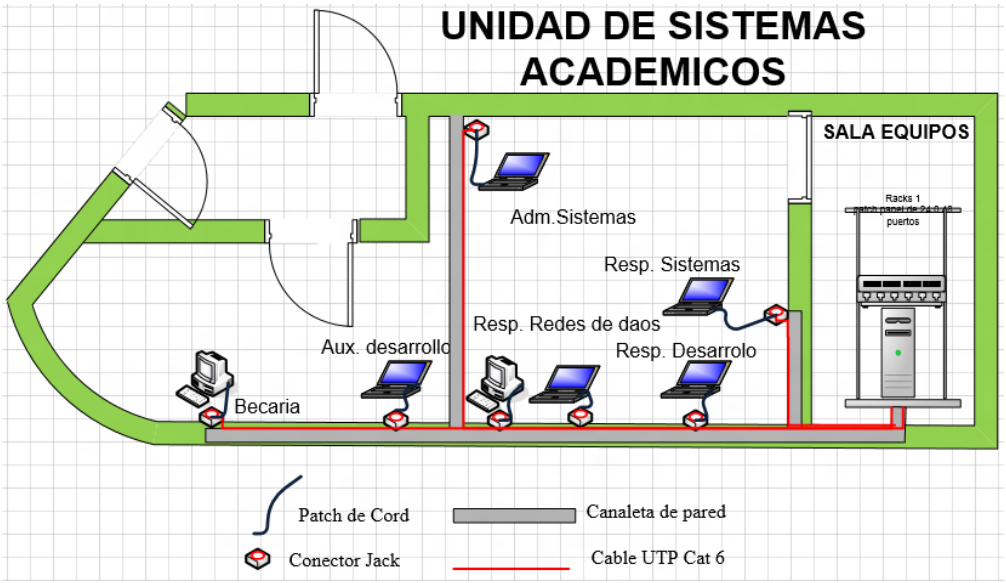


FIGURA 17: *Diseño físico de la Unidad de Sistemas Académicos*
Fuente*: Elaboración propia*

Nº	Descripción	Cantidad	Costo Unitario	Total
1	Conector Jack Keystone Femea Cat-6 Certificado	8	18.34	147
	Mini Rack 9u X 680mm 19 negro	Existente		
3	Organizador de Cable de 2U P/Rack	1	65	65
4	Patch Panel cat 6 de 24 Puertos	1	420	420
5	Patch de Cord de 1 Mts cat 6	10	20.50	205
6	Switch de Cisco 24 Puerto	Existente		
7	Patch Cord de 0,5 Mts para Terminación en Rack	10	17	170

8	Cable UTP Nexx Cat 6	75 Mts	9 el Mts	675
9	Conector RJ-45	15	3.5	53
9	Canaleta de pared cat grande	1	80	80
10	Canaleta 20*10*2MT	18	6	108
Costo Total de la los materiales requeridos			**1923**	

***TABLA** 5: Cotización de los dispositivos de la Red de Datos de la Unidad de Sistemas Académicos*
***Fuente**: Elaboración propia*

- **Diseño físico y Tabla de Cotización de los dispositivos de la Red de Datos de la Unidades de Trámites y Registro y de Información Académico**

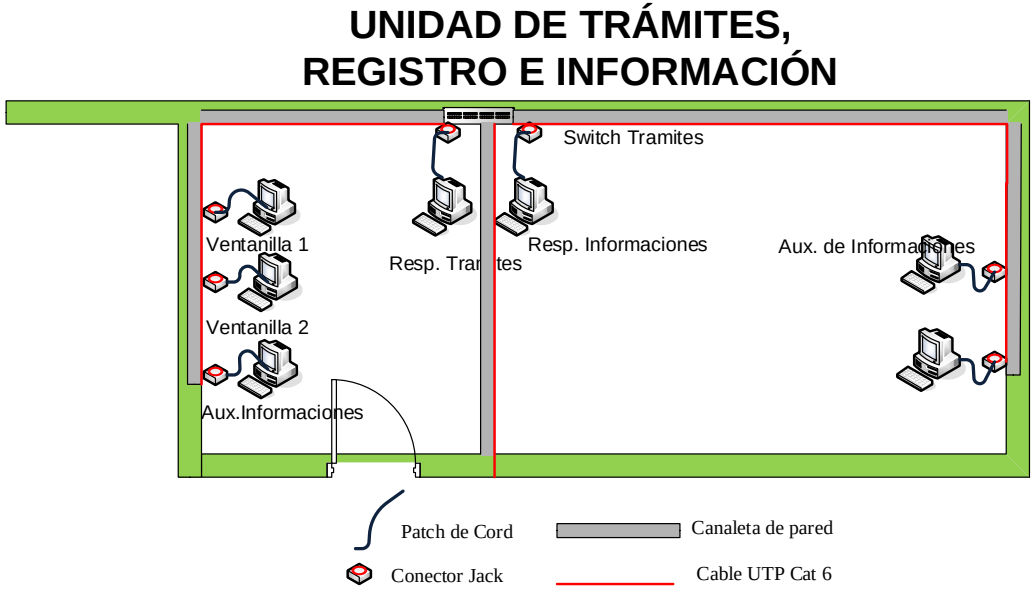


***FIGURA 18:** Diseño físico de la Unidades de Tramites y Registro y de Información Académico*
***Fuente:** Elaboración propia*

Nº	Descripción	Cantidad	Costo Unitario	Total
1	Conector Jack Keystone Femea Cat-6 Certificado	7	18.34	130
	Mini Rack 9u X 680mm 19 negro	1	720	720
3	Organizador de Cable de 2U P/Rack	1	65	65
4	Patch Panel cat 6 de 24 Puertos	1	420	420
5	Patch de Cord de 1 Mts cat 6	7	20.50	144
6	Switch de Cisco 24 Puerto	Existente		
7	Patch Cord de 0,5 Mts para Terminación en Rack	7	17	170
8	Cable UTP Nexx Cat 6	80 Mts	9 Mts	720
9	Conector RJ-45	10	3.5	35
9	Canaleta de pared cat grande	1	80	80
10	Canaleta 20*10*2MT	23	6	138
Costo Total de la los materiales requeridos				**2622**

TABLA 6: *Cotización de dispositivos de red de las unidades de trámites y registro y de información académico*
Fuente*: Elaboración propia*

➢ **Diseño físico y Tabla de Cotización de los dispositivos de la Red de Datos de Unidad de Archivos Académico**

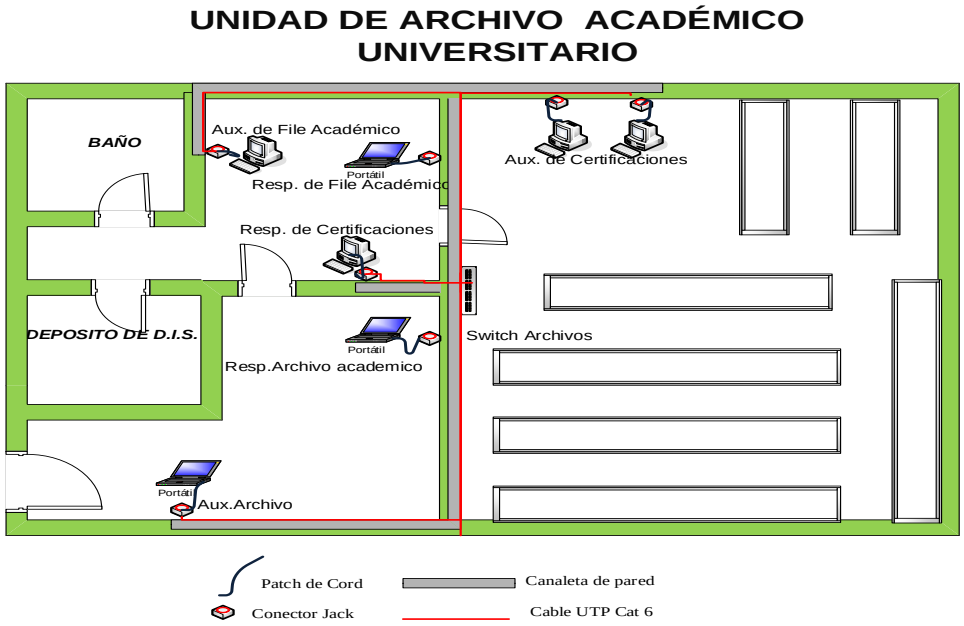


FIGURA 19: *Diseño físico de la Unidad de Archivos Académico*
Fuente*: Elaboración propia*

Nº	Descripción	Cantidad	Costo Unitario	Total
1	Conector Jack Keystone Femea Cat-6 Certificado	7	18.34	130
2	Mini Rack 9u X 680mm 19 negro	1	720	720
3	Organizador de Cable de 2U P/Rack	1	65	65
4	Patch Panel cat 6 de 24 Puertos	1	420	420
5	Patch de Cord de 1 Mts cat 6	7	20.50	144
6	Switch de Cisco 24 Puerto	1	6595	6595

7	Patch Cord de 0,5 Mts para Terminación en Rack	7	17	170
8	Cable UTP Nexx Cat 6	100 Mts	9 Mts	900
9	Conector RJ-45	10	3.5	35
9	Canaleta de pared cat grande	1	80	80
10	Canaleta 20*10*2MT	26	6	156
Costo Total de la los materiales requeridos				**9415**

TABLA 7: Cotización de Dispositivos para la Unidad de Archivos Académico
***Fuente**: Elaboración propia*

- **Diseño físico y Tabla de Cotización de los dispositivos de la Red de Datos de la Dirección del DIA**

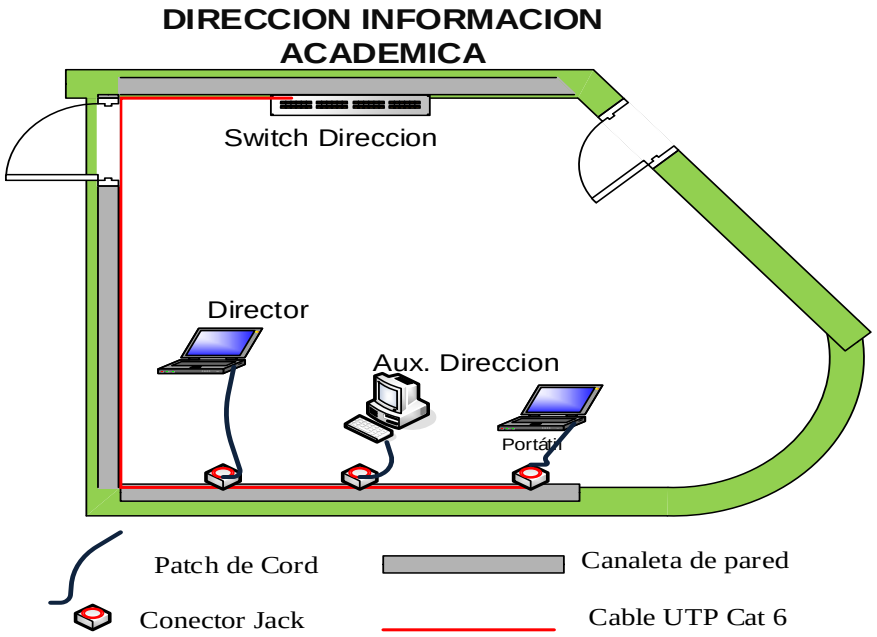


***FIGURA 20:** Diseño físico de la Dirección del DIA*

***Fuente**: Elaboración propia*

Nº	Descripción	Cantidad	Costo Unitario	Total
1	Conector Jack Keystone Femea Cat-6 Certificado	4	18.34	72
2	Mini Rack 9u X 680mm 19 negro	1	720	720
3	Organizador de Cable de 2U P/Rack	1	65	65
4	Patch Panel cat 6 de 24 Puertos	1	420	420
5	Patch de Cord de 1 Mts cat 6	4	20.50	82
6	Switch de Cisco 24 Puerto	1	6595	6595
7	Patch Cord de 0,5 Mts para Terminación en Rack	4	17	68
8	Cable UTP Nexx Cat 6	65 Mts	9 Mts	585
9	Conector RJ-45	5	3.5	18
9	Canaleta de pared cat grande	1	80	80
10	Canaleta 20*10*2MT	21	6	126
Costo Total de la los materiales requeridos				**8831**

***TABLA 8:** Cotización de los dispositivos de la Red de Datos de la Dirección del DIA.*
***Fuente**: Elaboración propia*

5.1.2. Actividad AC 2: Selección de la infraestructura de red.

La selección de la infraestructura de red está basada en los requerimientos y el diseño propuesto, se detallan en las tablas siguientes.

- **Infraestructura para la gestión de la Red de Datos de los usuarios**

Nº	Características	Detalle
1.	Laptop	Todos los modelos
2.	Computadora de escritorio	Todos los modelos

3.	Disco duro	80 GB o superior
4.	Procesador	Intel(R), APUs de AMD, dual Core o superior
5.	Memoria RAM	2,00 GB o superior
6.	Tarjeta de red	Integrada

TABLA 9: *Características de la computadora de escritorio – Laptop*

Fuente: *Elaboración propia*

- **Infraestructura para mejorar la gestión y el funcionamiento de la red de datos.**

Nº	Características	Detalle	Cantidad
1	Firewall (Existente)	Cisco SA 540	01
2	Switch de 28 puertos (Existente)	Cisco SG 300	02
3	Switch de 24 puertos(nuevo)	Cisco	02
4	Cable UTP (Caja de 300m) (nuevo)	Categoría 6	01
5	Conectores RJ45(nuevo)		50
6	jack rj45 (nuevo)	Categoría 6	30

TABLA 10: *Material disponible y nuevo que se requiere para mejorar la Red de Datos*
Fuente: *Elaboración propia*

5.1.3. Actividad AC 3: Instalaciones y Administración del Software y Hardware.

Como parte de esta actividad de la Administración de la configuración, la Dirección de Información Académica, se administró el Firewall Cisco SA 540, y los conmutadores Cisco administrables bajo las siguientes configuraciones que se muestra en las siguientes tablas:

CONFIGURACIÓN EN FIREWALL CISCO SA 540	DESCRIPCIÓN	DETALLE
INTERFAZ Y PUERTO	Configuración de la interfaz con el IP Address de la Red de área local virtual (Vlan) y su puerto respectivo en el Firewall	Configuración de las interfaces, definiendo el puerto 8 para la nueva red de área local virtual (Vlan) con la siguiente dirección de IP/address 192.168.5.0/29. Nombre de la Vlan Sistemas Numero o id de la Vlan 20
NAT	Network Address Translación, permite el enrutamiento de IP`S.	Para realizar el enrutamiento de la nueva Vlan con la red del Servidor.

TABLA 11: Configuración en Firewall Cisco SA 540para la administración de la Red de Dato
***Fuente**: Elaboración Propia*

La tabla 11 detalla la configuración de la implementación de una nueva red de área local virtual Vlan 20 la cual se denominó Vlan Sistemas, la misma contribuye en la seguridad de trasmisión de datos e información y en el acceso remoto al Sistema Académico Siringuero de los funcionarios de la Unidad de Sistemas, dependiente de la Dirección de Información Académica, la figura 21muestra lo plasmado en la tabla.

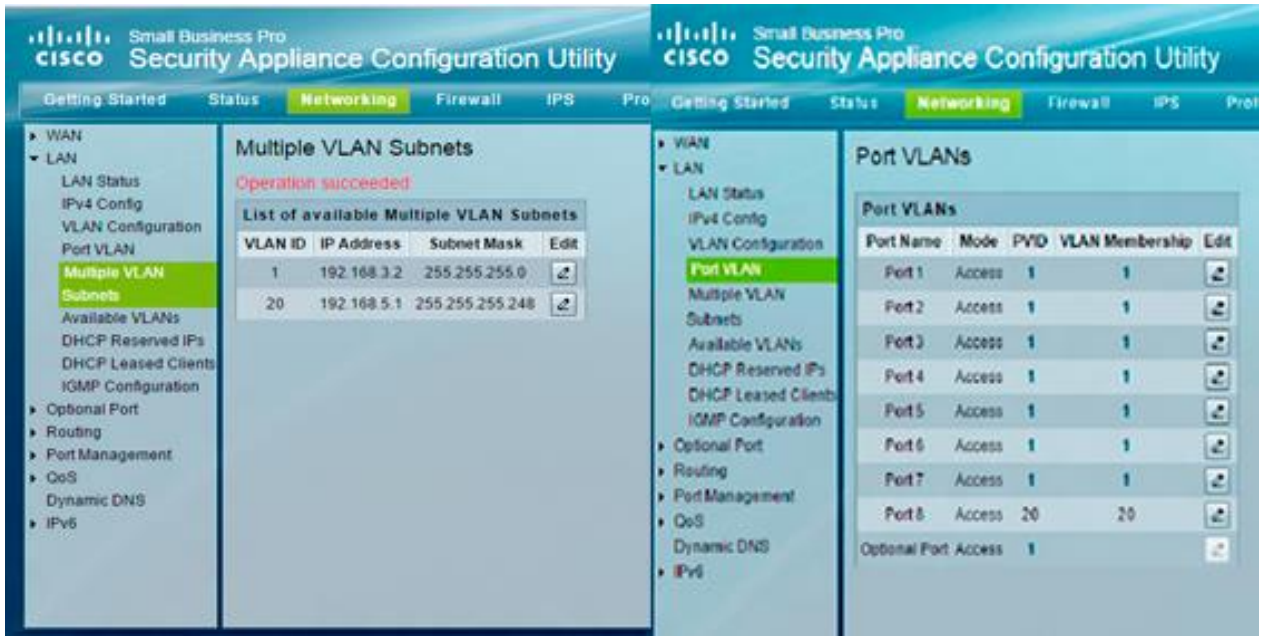


FIGURA 21: *Configuración de nueva Vlan y su asignación de IP y su respectivo puerto*
Fuente: *Recuperación de imagen del Firewall Cisco SA 540*

CONFIGURACIÓN EN EL CONMUTADOR (Switch)	DESCRIPCIÓN	DETALLE
PUERTOS	Configuración de numero o id, su nombre y sus puertos de la nueva red de área local virtual (Vlan) en el	Configuración del id o número y nombre fue igual a la de la configuración firewall la misma fue id 20 nombre sistemas la diferencia es en la configuración de los puertos los mismos fueron

	respectivo conmutador(Switch)	1,2,3,12,13,14,15 para la nueva red de área local virtual (Vlan)

TABLA 12: *Configuración de la nueva Vlan en el conmutador principal*
Fuente: *Elaboración propia*

Como se puede apreciar en la tabla anterior se realizó la configuración del conmutador principal que se ubica en la sala de equipos, correspondiente para la nueva Vlan 20 denominada Vlan sistemas, la misma permitirá tener un mejor control y seguridad a nivel de puertos, que solo los equipos que pertenecen a la Unidad de Sistemas tendrán acceso físicos a los puertos asignados como se muestra en la figura 22.

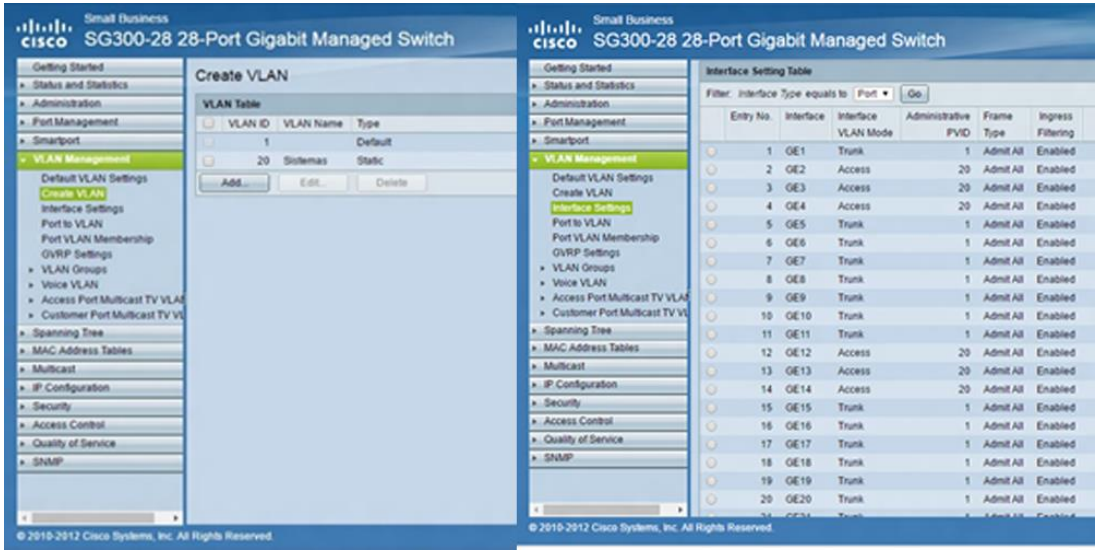


FIGURA 22: *Configuración de puertos respectivos para la Vlan en el conmutador principal*
Fuente: *Recuperación de imagen del conmutador principal*

Cabe mencionar que la nueva red de área local virtual está configurada para poder tener acceso a las otras redes, tal como a la red del servidor, caso contrario lo que no pasa con las otras redes no tienen acceso a la nueva red de área local, esto es para proteger los datos que circula hacia el servidor, del mismo modo la nueva red de área local virtual cuenta con seguridad a nivel de puertos la cual ase más segura la red de la Unidad de Sistemas Académicos.

Del mismo modo se realizó la instalación de software SmarttPss como se muestra en la figura 13 el mismo se utilizó para el monitoreo de las cámaras de Seguridad IP, ver detalles en el Anexo D

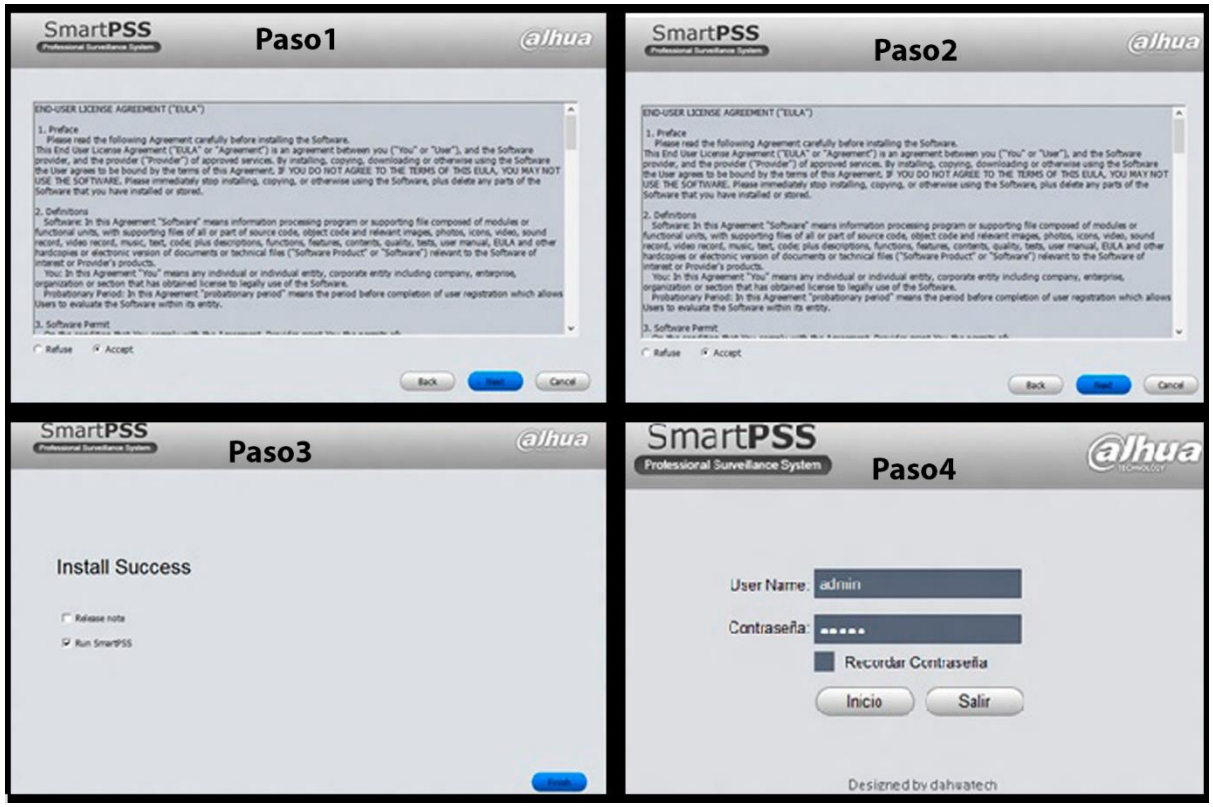


TABLA 13: *Instalación de Software SmartPSS*
Fuente: Elaboración propia

- **Configuración del protocolo TCP/IP en los equipos informáticos de los usuarios de la Unidad de Sistemas Académicos.**

  Para la configuración del protocolo TCP/IP se siguió los siguientes criterios que se detalla en la Tabla 14.

Nº	Descripción	Detalle

1	Dirección IP	192.168.5.x, perteneciente a la clase c donde x es el número de la nueva dirección IP que se asigna cada vez que solicita un usuario.
2	Gateway o puerta de enlace	La puerta de enlace asignada es la dirección IP 192.168.5.1
3	Mascara de red	255.255.255.248 = 29 la red esta sub dividida.
4	Broadcast	192.168.5.7 es la trasmisión que realiza o todos los nodos.
5	Cantidad de hosts	La cantidad de equipos es 6 puesto que esta sub dividida la red

TABLA 14: *Descripción de la configuración del protocolo TCP/IP*
Fuente*: Elaboración propia*

5.2. ADMINISTRACIÓN DE FALLAS(AF)

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en el servicio de Internet y la red de datos. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

La gestión de fallas también llamado Servicio Técnico Informático en el Trabajo Dirigido (Gestión de la Red de Datos en la Dirección de Información Académica de la U.A.P), fue una actividad constante durante la ejecución del Trabajo Dirigido, para lo cual se gestionaron los siguientes procesos establecidos por la metodología en la administración de fallas.

1. Localización de Fallas

2. Corrección de Fallas.

5.2.1. Proceso AF 1: Localización de Fallas

Este elemento de la localización de fallas es importante para identificar las causas que han originado una falla. De acuerdo a modelo funcional para la administración de redes que utiliza la prueba de diagnóstico, que presenta algunas pruebas de diagnóstico para localizar las fallas las mismas son: pruebas de conectividad física, Prueba de conectividad lógica y la prueba de medición.

Como parte de la prueba de diagnóstico se describirá algunas pruebas que se realizaron en el trascurso del desarrollo del Trabajo Dirigido, las mismas se realizaron cuando se recibía una alerta acorde a la solicitud de requerimientos de que ocurría algún problema en la red en alguna de las Unidades de la Dirección de Información Académica. La siguiente figura muestra el formulario de solicitud requerimiento.

	FORMULARIO SOLICITUD DE REQUERIMIENTO DE SISTEMA SIRINGUERO	Código: DIA-USA-FOR-001 Versión: v.01 Vigencia: 2015-12-11 Página 1 de 1

DATOS GENERALES DEL SOLICITANTE			
De	Lic. Mayerlin Moreno Lima	Para	Ing. Freddy Morales Blanco
Cargo	Resp. Informaciones	Cargo	Resp. Unidad de Sistemas Académicos
Dirección o Unidad	Dirección de Información Académica	Dirección o Unidad	Dirección de Información Académica
Fecha	18/04/2016		
		#cite (solo para u.s.a)	

DESCRIPCIÓN DE REQUERIMIENTOS GENÉRICOS		
N°	Requerimientos	Opción
1	Asignación de usuario y contraseña	
2	Desarrollo y mantenimiento de módulos del Sistema Siringuero	
3	Modificación y/o rectificación de datos en el Sistema Siringuero	
4	Revisión de cámaras de seguridad en los predios del Vice-Rectorado	
5	Capacitación a los usuarios administrativos, docentes y estudiantes del Sistema Siringuero	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIONES Y/O COORDINACIONES		
Nro.	Requerimiento	Opción
6	Parámetros de programación, impresión de actas, registro de notas.	
7	Apoyo técnico para manejo del Sistema Siringuero	
8	Otros… ……..	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIÓN INFORMACIÓN ACADÉMICA		
Nro.	Requerimiento	Opción
9	Mantenimiento y conectividad de redes de datos	✓
10	Apoyo técnico para manejo del Sistema Siringuero	
11	Creación de nuevos planes de estudios	
12	Creación de cursos extracurriculares y trámites que no se encuentran en el Sistema Siringuero.	
13	Servicio de sistemas de colas, asignación de nuevas ventanillas y cajas	
15	Habilitación de cupos en Sistema Siringuero para habilitación de postulantes	
14	Otros	
Otros requerimientos que no estén contemplados en el formulario Especificar: Backup de Computadoras		✓

UNIDAD DE SISTEMAS ACADÉMICOS
COBIJA 18 ABR 2016
Hora: 12:05 Firma:
Universidad Amazónica de Pando

DESCRIPCION DE REQUERIMIENTO
En esta sección pueden describir el requerimiento o adjuntar documentos

Lic. Mayerlin Moreno Lima
RESP. INFORMACIONES
Universidad Amazónica de Pando
Usuario Solicitante

UNIVERSIDAD AMAZÓNICA DE PANDO
UNIDAD DE INFORMACIONES
COBIJA - BOLIVIA

Lic. Richard Rojas Lopez
JEFE UNIDAD DE TRAMITES
RESP. SIS. E INFORMACIONES
Universidad Amazónica de Pando
Jefe Inmediato Superior

FIGURA 23: *Formulario de solicitud de Requerimiento de mantenimiento de la Red.*
Fuente: Elaboración propia

- **Pruebas de Conectividad Física.**

  La prueba de conectividad consiste en la verificación de los medios de transmisión que se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio de transmisión.

- **Pruebas de Conectividad Lógica.**

  Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto, a continuación se describirá las pruebas de conectividad lógica realizadas las mismas son: Prueba de configuración IP, prueba de conexión.

  - **Prueba de configuración de configuración IP**

    Para realizar la prueba de configuración de configuración IP se realzaba haciendo uso de símbolo de sistema que tienen incorporado los sistemas operativos, la misma trabaja con línea de comandos, lo primero que se realizaba es verificar la configuración IP del equipo. Una forma es insertar la línea de comando ipconfig, que permite saber cuál es la configuración IP del equipo. El resultado de este comando proporciona las IP que tiene cada interfaz, luego se verifica la interfaz de Ethernet conectada a la red de área local si corresponde o no a la red con la que se cuenta.

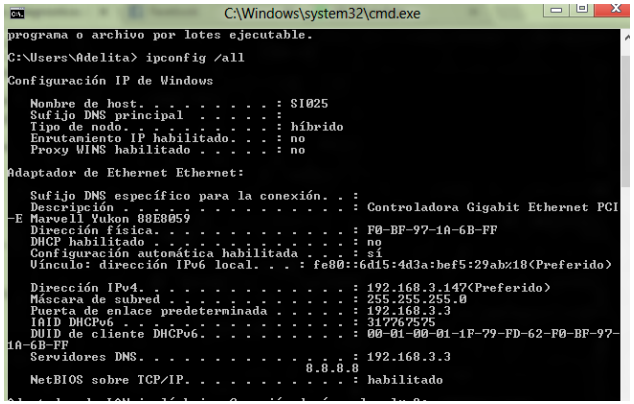


FIGURA 24: *Verificación de configuración de la interfaz Ethernet con el comando ipconfig /all*
Fuente: *Recuperación de imagen de la consola de cmd de Windows*

- **Prueba de la conexión**

Para realizar esta prueba se debe probar que la red de datos funcione de manera adecuada, existe una utilidad muy práctica que se suministra como una prestación estándar con la mayoría de los sistemas operativos. Se trata de los comando ping y tracert**.** Los comandos ping y tracert permiten enviar paquetes de datos a los equipos de la red y evaluar el tiempo de respuesta, además se obtiene una estadística de la latencia de red de esos paquetes.

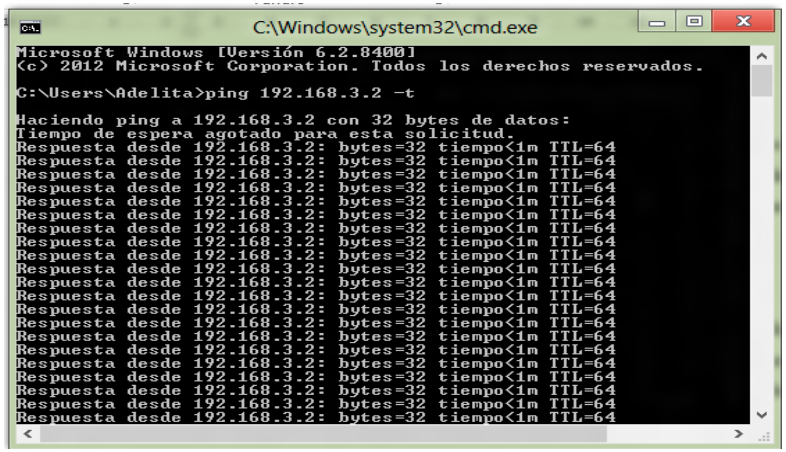


FIGURA 25: *Verificación del acceso a la red con comando Ping*
Fuente: *Recuperación de imagen de la consola de cmd de Windows*

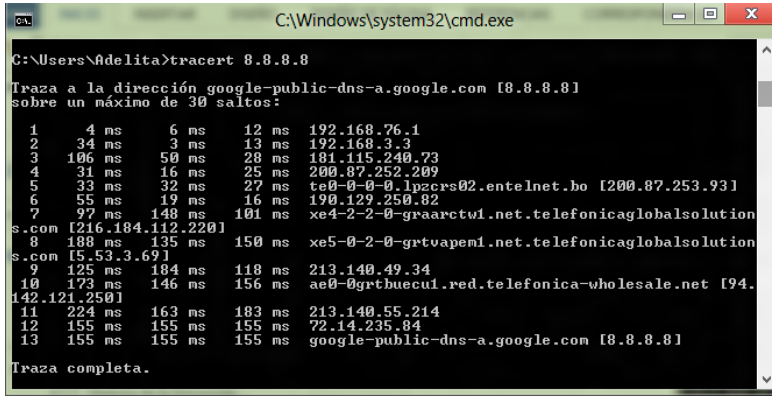


FIGURA 26: *Verificación del acceso a Internet con comando Tracert*
Fuente: *Recuperación de imagen de la consola de cmd de Windows*

- **Prueba de medición**

  Es la que va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información la misma se realiza también utilizando los comandos ya mencionado anteriormente.

Cabe mencionar que todas y cada una de las pruebas realizadas anteriormente ayudaron a determinar el origen de las fallas, en alguno de los casos se utilizaba una o todas las pruebas ya mencionadas anteriormente con el objetivo de hallar las fallas.

Se puede observar en la siguiente tabla los datos de las fallas detectadas en el transcurso del desarrollo del Trabajo Dirigido.

Meses	Falla	Motivo de la falla	Cantidad
Junio, julio, agosto, septiembre, octubre.	Fallas de conectividad lógica(Conflicto de IP, Configurar IP, firewall)	Alguien de la red se puso arbitrariamente una IP que pertenecía a otro usuario o cuando un usuario nuevo quiere que se le asigne un IP o cuando el firewall sufre sobrecarga y deja la conexión hacia el servidor lenta.	34
	Conectividad física(Falla de conmutador, cable, conectores, falta de	Cuando un conmutador sufre sobrecarga, o cuando un cable sufre una ruptura, un conector está en mal estado, o cuando el hardware de un dispositivo está en mal	61

	corriente entre otros)	estado, cuando se ocasiona un corte de energía eléctrica entre otros.	
Total de fallas detectadas			95

TABLA 15: *Fallas detectas en el trascurso del desarrollo del Trabajo Dirigido*
Fuente: *Elaboración Propia*

GRAFICO 1: *Casos de fallas detectadas por tipo de conexión*
Fuente: *Elaboración propia*

En el gráfico anterior muestra el porcentaje de fallas por tipo de conectividad detectadas en el trascurso del desarrollo del Trabajo Dirigido, como se aprecia del total de las fallas, las más comunes con un 64% fueron las fallas de conectividad física, las mismas fueron causadas por: sobrecarga de conmutador, ruptura de cable, conector en mal estado entre otros. Un 36% fue por causa de conectividad lógica las mismas fueron por: la falta de configuración de IP en la red, por un conflicto de IP o por un problema del firewall.

5.2.2. Proceso AF 2: Corrección de Fallas.

Esta etapa es donde se recupera las fallas de conectividad física como lógica y se plantean las soluciones para corregir el error tecnológico de la red, para dar solución es necesario la asistencia técnica, la misma ayuda a dar solución a las fallas.

Una vez realizada la corrección de la falla o requerimiento requerido se elaboraba el formulario de conformidad de requerimientos la siguiente imagen muestra un formulario de conformidad recibido y satisfecho por el servicio prestado, puede ver los detalles de los formularios en el ANEXO C.

FORMULARIO CONFORMIDAD DE REQUERIMIENTO DE SISTEMA SIRINGUERO

Código:	DIA-USA-FOR-003
Versión:	v.01
Vigencia:	2015-12-11
Página **1** de **1**	

DATOS GENERALES DE LA CONFORMIDAD DE REQUERIMIENTO					
De	**Marco Antonio Montevilla Ruiz**	**Vía**	**Ing. Freddy Morales Blanco**	**Para**	**Lic. Juan Carlos Huanca Guanca**
Cargo	**Administrador de Redes de Datos**	**Cargo**	**Responsable Unidad de Sistemas Académico**	**Cargo**	**Director de Información Académico**
				#cite	

DESCRIPCION DE REQUERIMIENTO
• Implementación de nuevos puntos de red

DETALLE DE CONFORMIDAD DE REQUERIMIENTO	
NRO	**ACTIVIDADES DESARROLLADAS**
	De acuerdo a formulario de solicitud de requerimientos se realizó la implementación de 4 puntos de red en la unidad de unidad de trámites.

M.Sc. Juan Carlos Huanca Guanca DIRECTOR DE INFORMACIÓN ACADÉMICA a.i. Universidad Amazónica de Pando	Yesenia Velasco Amasifuen Administrador de Sistemas Académicos Unidad de Sistemas Académicos	M.Sc. Ing. Freddy Morales Blanco

Para la solución de las fallas se hizo uso de los mecanismos más conocidos planteados por la metodología modelo funcional para la administración de red tales como: Reemplazo de recursos dañados, Aislamiento del problema, Redundancia y Recarga del sistema, cambio de configuración.

- **Servicio técnico informático por fallas de los servicios de la Red de Datos.**

  Existen diversos problemas causados por la falla de conexión de la computadora con la red de datos, como se muestra en la tabla y gráfica anterior, se mencionará los más sobresaliente durante la ejecución del Trabajo Dirigido en la Dirección de Información Académica.

  - **Asistencia técnica por conectividad lógica.**

    La asistencia técnica de conectividad lógica se realizó cada vez que se recibía los formularios de solicitud de requerimiento, para ello se realizaba la verificación de redundancia y verificación de la duplicidad de IP, configurando las IP en las equipos de los usuarios que así lo requerían, del mismo modo se realizaba la verificación los problemas en la configuración de la seguridad del firewall.

    En el caso de la configuración IP, se la realizó en coordinación con el Administrador de la Red de Datos de la Universidad Amazónica de Pando dependiente de la USIC, esta configuración se realizó en el protocolo de red TCP/IP

    La siguiente figura muestra la configuración realizada a un usuario mediante el protocolo TCP/IP.

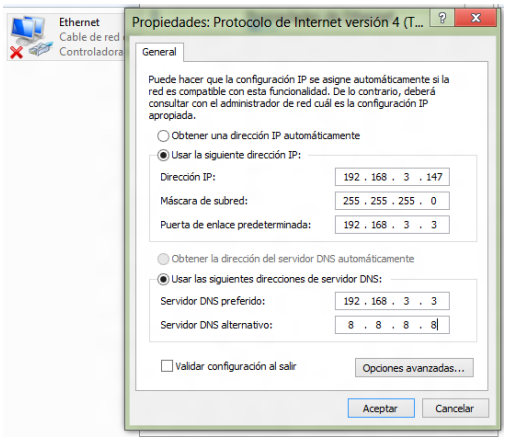


FIGURA 27: *Ventana de configuración de protocolo TCP/IP*
Fuente: *Elaboración propia*

- **Asistencia técnica por conectividad física.**

  La asistencia técnica por falla de conectividad física se realizó cuando se requería el reemplazo de un recurso dañado: la misma se la realizó cuando se requería de un nuevo punto de red, reemplazo del cableado en puntos existentes, verificación y cambio de los conectores RJ 45, conmutador, hardware (tarjeta de red etc.) estaba en mal funcionamiento o en mal estado.

  Con respecto a la recarga de sistema se la ejecutaba cuando ocurría una falla en el conmutador, firewall o un equipo de red sufría de sobre carga de datos, se daba solución realizando un reinicio del equipo.

  Con respecto al aislamiento del problema se realizaba el Aislamiento del recurso que se encuentra dañado o que este afectaba a otros recursos de la red tal como sucedió que un equipo (computador) estaba ocasionando que los conmutadores dejen de trasmitir información.

- **Asistencia técnica de Software**

  La asistencia técnica de Software se realizó cuando los usuarios de la Unidad de Sistemas Académico requería la instalación de un software, tales como: la reinstalación de sistema operativo o la instalación de algún Software de oficina, antivirus entre otros.

➢ **Fallas con relación a otros aspectos.**

Este punto trata de las fallas ocurridas con relación a otros aspectos como ser: la seguridad física (equipo de vigilancia), impresión en red, compartir información en Red, copias de seguridad entre otros, las mismas fueron subsanadas con algún mecanismo ya mencionado anteriormente.

➢ **Servicio técnico informático atendidas durante el periodo del Trabajo Dirigido.**

Durante la ejecución del periodo del Trabajo Dirigido se realizó la asistencia técnica bajo los siguientes aspectos. A continuación se muestra la tabla 16 detallando los servicios técnicos realizados en los diferentes meses y por tipo de fallas.

MES	ASISTENCIA TÉCNICA POR CONECTIVIDAD LÓGICA	ASISTENCIA TÉCNICA POR CONECTIVIDAD FÍSICA	ASISTENCIA TÉCNICA SOFTWARE	FALLAS CON RELACIÓN A OTROS ASPECTOS	CASOS ATENDIDOS POR MESES
Junio	8	23	2	3	**36**
Julio	4	15	1	5	**25**
Agosto	5	11	0	7	**23**
Septiembre	3	12	1	8	**24**

Octubre	2	8	0	3	**13**
CASOS ATENDIDOS POR TIPO DE FALLA	**22**	**69**	**4**	**26**	**121**
TOTAL DE CASOS ATENDIDOS					**121**

TABLA 16: *Fallas atendidas en el trascurso del Trabajo Dirigido*
Fuente: *Elaboración propia*

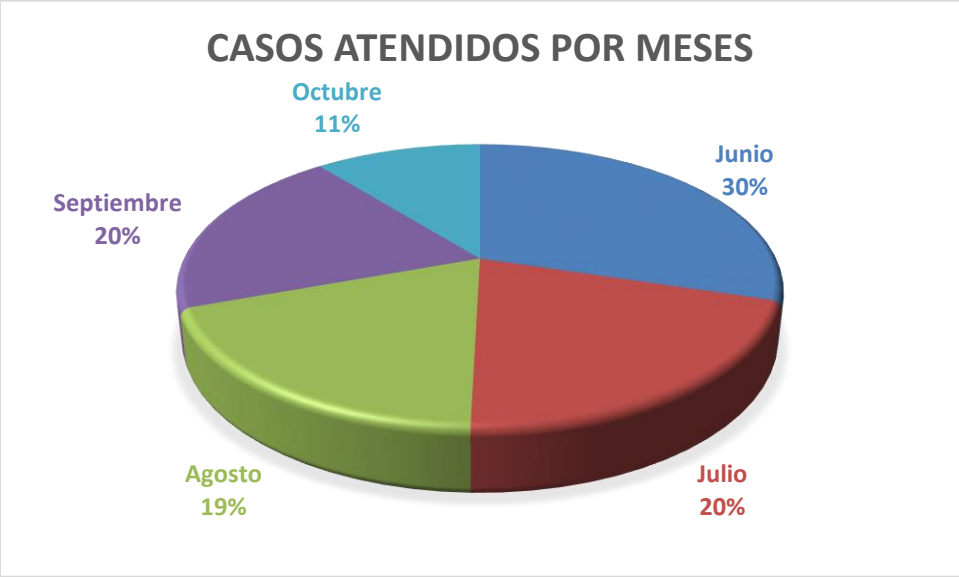


GRAFICO 2: *Casos de fallas atendidos por mes.*
Fuente: *Elaboración Propia*

El total de casos atendidos por distintas causas en el trascurso del desarrollo del Trabajo Dirigido (Gestión de la Red de Datos en la Dirección de Información Académica de la UAP), se observa en el gráfico anterior y se deduce que en los meses:

- **Junio**

  El mes de junio fue donde se presentó más casos de asistencia técnica por parte de los usuarios, donde se dio solución a los problemas producidos a un 30% de asistencia técnica realizada

- **Julio**

  El mes de julio se dio solución a menos casos con un 20% de asistencia técnica a los usuarios.

- **Agosto**

  En el mes de Agosto se redujo mu más al del mes anterior los casos de solicitudes que fue un 19% de asistencia técnica.

- **Septiembre**

  En el mes de Septiembre se elevó no consideradamente los casos atendidos, las mismas fueron por una u otras razones las mismas alcanzaron un 20% de casos atendidos.

- **Octubre**

  El mes de octubre fue el que menos casos se atendió lo cual se optimizaron sin ningún percance los casos llegaron a un 11% de asistencia técnicas atendidas.

GRAFICO 3: *Casos de fallas atendidos por tipo de fallas*
Fuente: *Elaboración propia*

Como se observa en el gráfico anterior donde se muestra el porcentaje de las fallas atendidas por su tipo, de las mismas se deduce que: las fallas más originadas con un 57 % fueron las de conectividad física, siguiendo con un 22% las de conectividad con relación a otros aspectos, con un 18% las de conectividad lógica, por último se tiene las fallas de Software las mismas tienen el porcentaje más bajo de todas las anteriores con un 3%, las mismas fueron subsanadas satisfactoriamente. +

En la fase de gestión de fallas se realizó la corrección de las fallas presentadas durante el periodo del Trabajo Dirigido, los casos de asistencia técnica atendidas fueron por diversos factores: fallas de conexión en la red de datos, falta de configuración de IP en la red , falla de algún conmutador, falla en las cámaras o equipo de seguridad, falla en el cable UTP o en los conectores, donde se realizaron las

actividades constantes para dar solución a cada uno de los casos, todos y cada uno de los caso se realizaron satisfactoriamente brindando una buena atención eficiente al usuario.

5.3. ADMINISTRACIÓN DE LA SEGURIDAD(AS)

En cuanto a la Administración de la seguridad la Dirección de Información Académica cuenta con políticas y mecanismos de seguridad tales como el Firewall Cisco SA 540, la misma tiene incorporado un sistema de prevención de intrusos, por otra parte se cuenta con cámaras de seguridad en cuanto a la seguridad física, las mismas son de mucha ayuda en cuanto a la prevención y detección del acceso de los recursos de la red.

5.3.1. Actividad AS 1: Mecanismos de Seguridad

- **Mecanismos Seguridad lógica**

  En cuanto a la prevención de ataques y la seguridad lógica se la realizó utilizando el mecanismo de seguridad Firewall Cisco SA 540 el mismo tiene incorporado el sistema de prevención de intrusos (IPS).

  a) Prevención de Intruso

  La prevención de intrusos se logra mediante el Firewall Cisco SA 540 que tiene integrado el sistema de prevención de intruso la cual permite el filtrado e inspección del estado de paquetes y el sistema de prevención de intrusiones que proporcionan protección de tráfico no deseado y ataques maliciosos en la red de datos.

  El mismo incorpora políticas IPS y protocolos de inspección para mejorar la seguridad de la red tales como bloqueo de puertos, códigos maliciosos e intrusos. Cabe mencionar que el firewall con el que se cuenta permite mejorar la distribución de la red de

datos implementando zonas (WAN, LAN y DMZ). Este recurso incluye un firewall dinámico para resguardar la seguridad de la red de datos, detección de intrusos, entre otros.

La verificación del sistema de prevención de intrusos se la realizaba el monitoreo diariamente, la siguiente figura muestra la pantalla principal del sistema de prevención de intrusos.

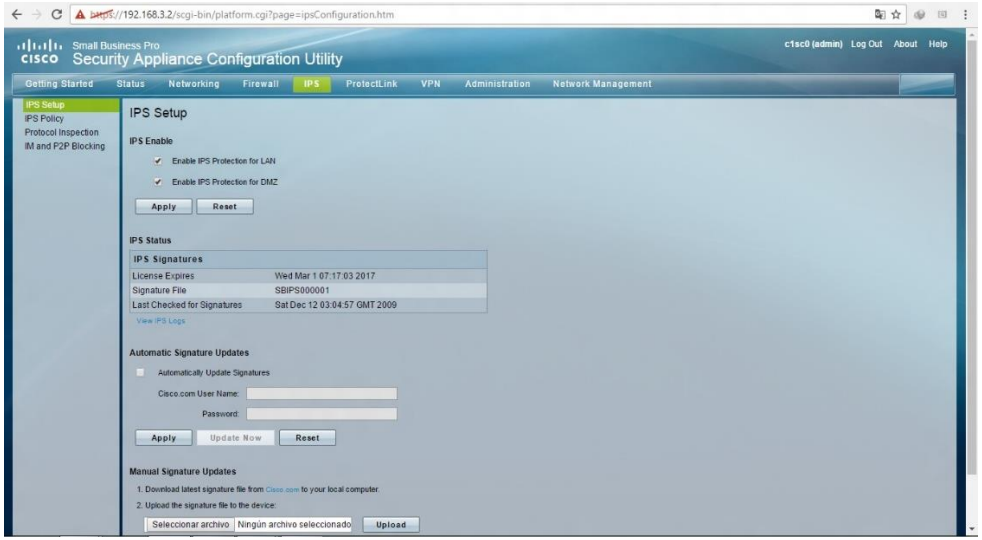


FIGURA 28: *Pantalla principal de configuración del Sistema de prevención de intrusiones (IPS)*
Fuente: *Recuperación de imagen del menú del Firewall Cisco SA 540*

La siguiente figura muestra las políticas de inspección que utiliza el sistema de prevención de intrusos las mismas son: políticas de inspección DOS, EXPLOIT, FTP, LOCAL, SQL/DB, SHELLCODE., TROJAN/VIRUS, LDAP, WEB-MISC_ATTACKS, WEB-SERVER, BACKDOOR.

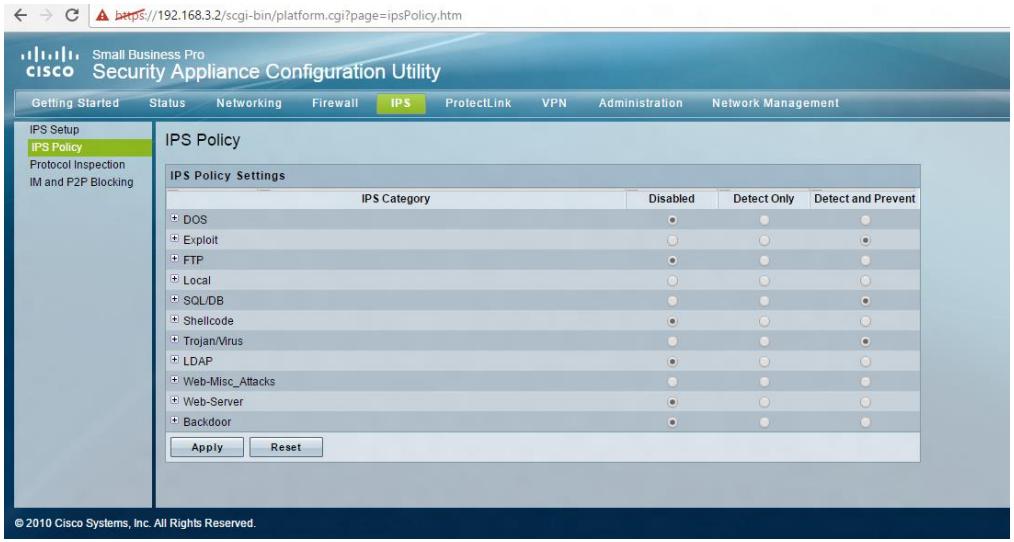


FIGURA 29: *Políticas de inspección del Sistema de Prevención de Intrusos*
Fuente: *Recuperación de imagen del menú del Firewall Cisco SA 540*

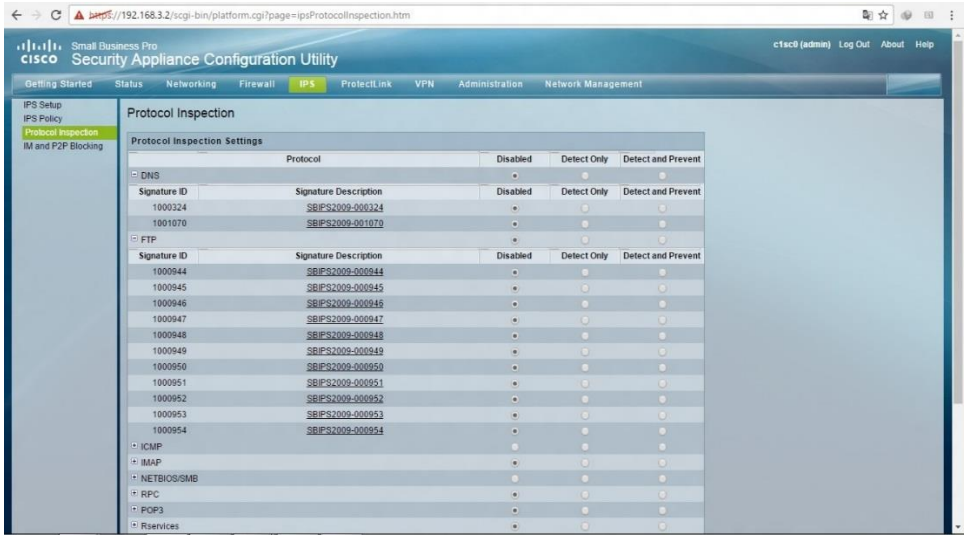


FIGURA 30: *Protocolo de inspección del Sistema de Prevención de Intrusos*
Fuente: *Recuperación de imagen del menú del Firewall Cisco SA 540*

La figura anterior detalla los protocolos de inspección del sistema de prevención de intrusos el mismo utiliza diferentes tipos de protocolos los mismos son: DNS, FTP, ICMP, IMAP, NETBIOS/SMB, RPC, SMTP, Telnet, VOIP, HTTP y SQL.

- **Revisión de los registro en el Firewall.**

Una vez dentro del servidor firewall se verifica o revisa si hubo algún incidente en el IPS en los servicios hacia el sistema siringuero, la siguiente imagen muestra todos los registros en el Firewall incluyendo el IPS.

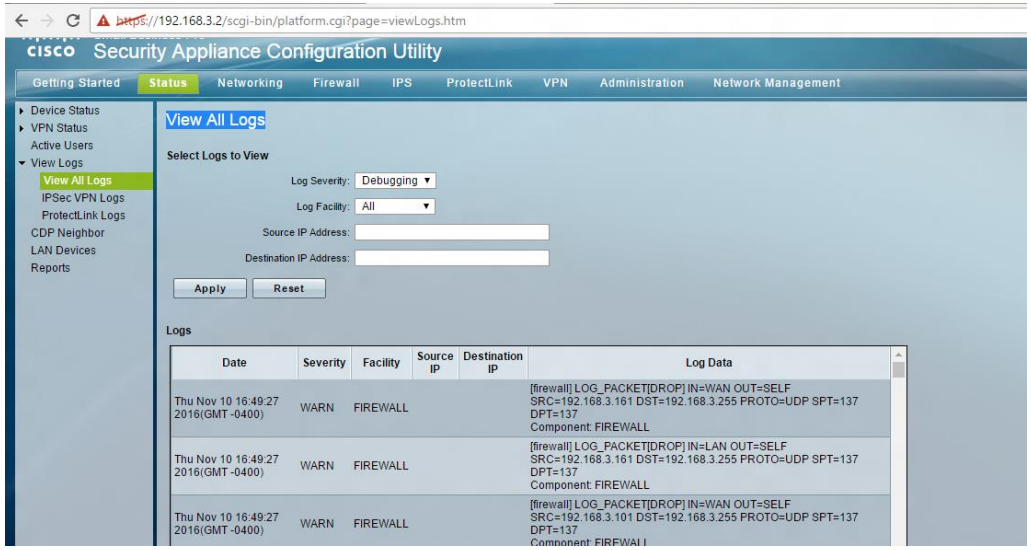
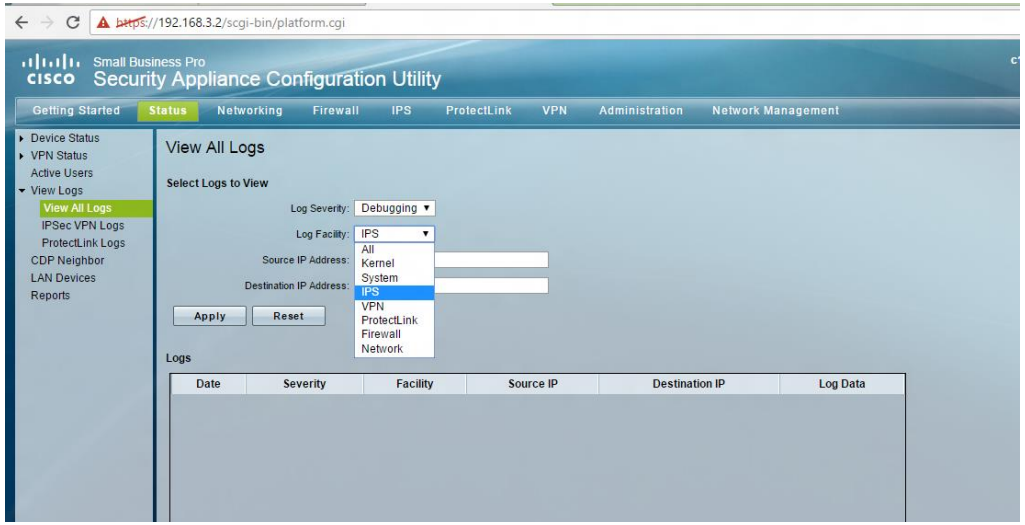


FIGURA 31: *Verificación de todos los registros del Sistema de Prevención de Intrusos*
Fuente: *Recuperación de imagen del menú del Firewall Cisco SA 540*



La anterior imagen muestra los registros del sistema de prevención de intruso, en caso de encontrar algún incidente se prepara un informe técnico al responsable de U.S.A, la misma se preparar un informe técnico Ver Anexo D: Formulario Informe de Incidentes en el Firewall, al responsable de U.S.A.

- **Mecanismos Seguridad Física**

  En cuanto a la seguridad física se cuenta con cámaras de seguridad la misma permite realizar el monitoreo de los ambientes de la Dirección de Información Académica, La administracion del sistema de monitoreo de cámaras de seguridad sirve para garantizar el resguardo de la documentación, Servidores, equipos de computación y activos de alto costo para la U.A.P. La misma se realizó diariamente como se muestra en las figuras N° 30 y 31.

  Para llevar a cabo esta actividad se hizo uso del Software SmartPSS el mismo tiene incorporado múltiples funciones, la siguiente figura muestra las imágenes capturadas en el desarrollo del monitoreo.

FIGURA 32: *Monitoreo diario con las Videocámaras*
Fuente: *Recuperación de imagen del Software SmartPss*

La siguiente figura muestra las copia de seguridad de los videos capturados en el transcurso del día las misma permitía realizar la copia de seguridad de 30 días, el medio de almacenamiento con el que se cuenta es un HDD de 2 Terabyte.

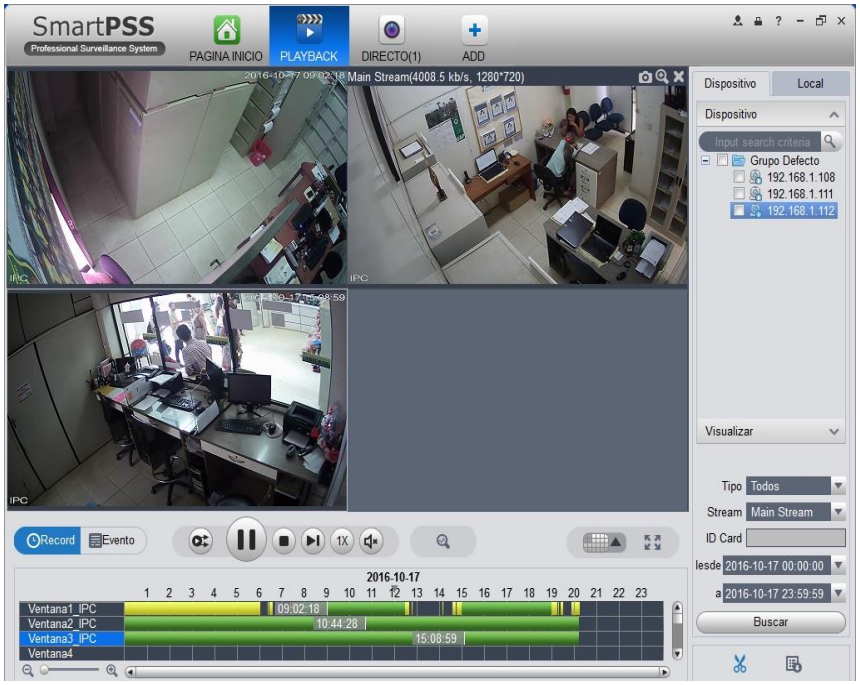


FIGURA 33: *Revisión de videos recolectados con las Videocámaras*
Fuente: *Recuperación de imagen del Software SmartPss*

5.3.2. Actividad AS 3: Políticas de Seguridad

En cuanto a las políticas de seguridad se recurrió al uso de las políticas ya existentes con las que cuenta la Dirección de Información Académica, las mismas establecen las acciones a realizar, las cuales fueron utilizadas las políticas 8, 10, 13 y 15, para ver a más detalle de las políticas observe el Anexo F.

A continuación se describirá las acciones y tareas realizadas en cuanto a estas políticas las mismas facilitaron el desarrollo del Trabajo Dirigido “Gestión de la Red de Datos en la Dirección de Información Académica”.

- **POLÍTICA 8: SOFTWARE UTILIZADO Y SOFTWARE LIBRE**

  En cuanto a la política de utilización de Software libre se hizo uso del Software SmartPSS para el monitoreo de las cámaras de seguridad, las mismas fueron de mucha ayuda a la hora del resguardo de la documentación, Servidor, equipos de computación y activos de alto costo para la Universidad Amazónica de Pando.

- **POLÍTICA 10: ALMACENAMIENTO Y RESPALDO**

  En cuanto a este punto se realizó las copias de respaldos o también llamados "backup", la misma se la realizo todos y cada uno de los equipos de la Dirección de Información Académica ver ANEXO C.

- **POLÍTICA 13: SEGURIDAD FISICA**

  En cuanto a este punto se hizo uso del mecanismo de seguridad, las cuales son las cámaras de seguridad, la misma permite resguardar la información, documentación, Servidor, equipos de computación y activos de alto costo para la Universidad Amazónica de Pando.

- **POLÍTICA 15: ADMINISTRACIÓN DE LA SEGURIDAD**

  Esta política facilitó las acciones a tomar cuando se detecte a alguna persona que no sea de la Unidad de Sistema tomando control de las sesiones sobre las terminales, este capturando información sensible y si son detectados vulnerando la red interna o externa, y haciendo uso de alguna herramienta Hacking en la Red para dañar el servidor.

CUADRO COMPARATIVO

Nro.	Características a Comparar	Antes de la Ejecución del Trabajo Dirigido	Después de la Ejecución del Trabajo Dirigido

1.	Diseño físico	No cuenta	Propuesta de diseño acorde norma y estándar de cableado estructurado
2.	Diseño Lógico	No cuenta	Propuesta de diseño acorde norma y estándar de cableado estructurado
3.	Direcciones de IP	Desordenado ni dividido en subred	Propuesta de mejoramiento en direcciones IP y dividir en subredes diferentes
4.	Redes de Áreas Locales Virtual(Vlan)	No cuenta	Cuenta una nueva Vlan para la Unidad de Sistemas Académicos
5.	Soporte Técnico	Insuficiente	Se mejoró y agilizo la el servicio técnico vía asistencia técnica los mismos fueron atendidos 121 casos atendidos
5.	firewall	Ningún registro de monitoreo	se realizó el monitoreo diario, se realizó la copia de seguridad de firewall
6.	Cámaras IP	No cuenta	Se realizó la implementación de cámaras IP en cuanto en la seguridad física

7.	Políticas de Seguridad	la utilización no era la adecuada	Se mejoró en el uso de las políticas de seguridad respecto a redes.

TABLA 17: *Cuadro comparativo de la Gestión de la red de Datos.*

Fuente: Elaboración Propia

5.4. ACTIVIDADES EXTRAS REALIZADAS EN EL TRASCURSO DEL DESARROLLO DEL TRABAJO DIRIGIDO

En este punto se detallará las actividades extras realizadas, una de ellas fue el desarrollo de un sitio Web para la Dirección de Información Académica, ver detalles en Anexo G.

El apoyo de administración de usuarios para el acceso al Sistema Siringuero, se la realizó tanto para estudiantes como docente de la Universidad Amazónica de Pando, del mismo modo se apoyó en la modificación de retroceso de fases de las evaluaciones de las asignaturas, ver detalle en el Anexo H.

Otra de las actividades realizadas fue brindar apoyo técnico en la primera jornada académica desarrollada los días 19 al 21 de octubre.

A continuación se muestra la pantalla principal del sitio Web realizado.


PRINCIPAL
192.168.8.175/dia511/index.php
DIRECCIÓN DE INFORMACIÓN ACADÉMICA
PRINCIPAL PRESENTACION HISTORIA OBJETIVO Y MISION ESTRUCTURA EXAMPLE PAGES
CERTIFICACION
ISO
9001 - 2015
A LA CALIDAD
A partir de 2015 los procedimientos fueron implementados bajo la Norma ISO 9001-2015
Unidad de Sistemas de Información y la DIA, rumbo a la Certificación en Sistema de Gestión de Calidad ISO 9001-2015
Procedimientos Bajo ISO 9001 - 2015
ESCALAFÓN DOCENTE
POSTGRESQL
PROCEDIMIENTOS
Enlaces
U.A.P.
PRESENTACIÓN
La Dirección de Información Académica dependiente del Vicerrectorado es la instancia que presta servicios de apoyo logístico y administrativo de toda actividad académica y de información que se lleva a cabo en la Universidad Amazónica de Pando.
En este sentido optimizamos nuestros servicios, brindando un servicio cordial, eficaz y eficiente a nuestros usuarios: Comunidad Universitaria y Comunidad en general, que son la razón de ser de nuestra dirección. Asimismo somos el ente oficial en la entrega y certificación de información académica de esta casa superior de estudios
Cuatro unidades son las que coadyuvan en la mejora del servicio, las cuales son: Unidad de Trámites y Registros (UTR), Unidad de Archivo Académico Universitario (UAAU), Unidad de Informaciones (UI) e Unidad de Sistemas Académicos (USA), cada uno de ellos son pilares fundamentales de las transformaciones y mejoras en los servicios académicos que brinda nuestra dirección.
Login Form
Usuario
Contraseña
Identificarse
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua
Misión
Somos una dirección técnica de gestión de la información, que brinda un servicio eficiente a la comunidad universitaria y población en general, utilizando nuevas tecnologías de información y comunicación, para contribuir al desarrollo académico administrativo en la Universidad Amazónica de Pando.
Read more: Beginners
Visión
Ser una dirección técnica transparente en la gestión de la información, que brinda un servicio óptimo con calidad, a la comunidad universitaria y población en general, utilizando modernas tecnologías de información y comunicación; siendo un referente institucional en la Universidad Amazónica de Pando y contribuyendo al desarrollo académico del sistema universitario nacional.
Objetivo
Mejorar continuamente y sistemáticamente los servicios académicos y de información con el uso de las modernas Tecnologías de la Información y Comunicación TIC, con el fin de fortalecer la gestión académica de la Universidad Amazónica de Pando.
Read more: Professionals
Search
Buscar...
SEARCH
Tab1
Breadcrumbs
Inicio
The Pixels sample site is designed as a simple site that can be routinely updated from the front end of Joomla!.
As a site, it is largely focused on a blog which can be updated using the front end article submission
New weblinks can also be added through the front end.
A simple image gallery uses com_content with thumbnails displayed in a blog layout and full size images shown in article layout.

FIGURA 34: *Pantalla principal del sitio Web de la Dirección de Información Académica*
Fuente: *Recuperación de imagen de la pantalla principal del sitio Web*

CAPITULO VI

6.CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

En base a las consideraciones y resultados obtenidos de las actividades realizadas y expuestas en el capítulo anterior, se llega a las siguientes conclusiones:

- Como resultado del Trabajo Dirigido, se llegó a la conclusión que los servicios de la Red de Datos mejoraron significativamente, permitiendo un flujo más constante y seguro sin muchos cortes, la gestión de la red de datos mejoró porque en el trascurso del Trabajo Dirigido se realizaron las diferentes actividades que mejoraron su funcionamiento.
- Con relación a la Administración de la configuración permitió realizar el análisis inicial de requerimientos de los usuarios de la red, de acuerdo al análisis y los requerimientos encontrados se realizaron los diseños físico y lógico de la red cumpliendo normas y estándares internacionales, se realizó la selección de infraestructura de la red, como parte de la configuración de software se realizó la configuración e implementación de una nueva red a área local virtual la misma es para mejorar la seguridad de la Unidad de Sistemas Académicos.

- Como parte de la gestión de fallas se realizaron las pruebas diagnóstico para encontrar las distintas fallas, con relación a la corrección de las falla se mejoró y agilizó la atención de las fallas encontradas por algún tipo, ya sea conectividad física o lógica en la red de datos, mediante la asistencia técnica constante realizadas se logró mejor la atención del servicio técnico vía asistencia técnica.
- En cuanto a la Administración de la seguridad se realizó la prevención de intrusos en la red con el dispositivo firewall Cisco el mismo aplica políticas y protocolos de inspección de paquetes, en cuanto a la prevención y detección del acceso a los datos físicos se realizó el monitoreo constante con cámaras de seguridad, del mismo modo se hiso uso de las políticas de seguridad existente, en cuanto a este punto se vio que los mecanismos de seguridad no son suficiente puesto que la seguridad no es a un nivel deseado del 100%.

6.2. RECOMENDACIONES

Al concluir el presente Trabajo Dirigido se pone en consideración las siguientes recomendaciones con el propósito de mejorar aún más el funcionamiento de la red de datos en la Dirección de Información Académica, para lo cual se hace las siguientes sugerencias y recomendaciones:

- En consideración con la seguridad de la red de datos y tomando en cuenta la administración del Sistema Siringuero en la red, se recomienda realizar la adquisición de mas equipos de seguridad, tanto como para la seguridad física y lógica para evitar las vulnerabilidades de las mismas.
- Realizar la implementación del cableado estructurado de acuerdo a los diseños plasmados en el capítulo anterior, los mismos cumplen normas y estándares de cableado estructurado, lo cual permitirá compartir mejor los recursos y así tener un mejor flujo de información segura, confiable y constante.
- Realizar una mejor configuración y segmentación de la red de la Dirección de Información Académica puesto que es una Dirección que más flujo de información tiene.

7.BIBLIOGRAFÍA

Aida Noemy Domingo Sales, E. B. (2012). *SEGURIDAD INFORMATICA.* Obtenido de SEGURIDAD INFORMATICA: https://docs.google.com/document/d/1Y4_DJ11TIs-qNWsT0zkDGlcCh2mHamd208G4o6r4_GE/edit

Barba Martí, A. (1999). *Gestion de red.* españa: UPC.

Borghello, C. (4 de agosto de 2000 - 2009). *segu-info*. Obtenido de segu-info: http://www.segu-info.com.ar/logica/seguridadlogica.htm

C. S. (2010). *Cisco SA 500 Series Security Appliances.* Obtenido de Cisco SA 500 Series Security Appliances: http://www.cisco.com/c/dam/en/us/products/collateral/security/small-business-sa500-series-security-appliances/c45-562587-01_sa_500_security_appliance_aag_v2a_4087.pdf

Cabero, A. J. (1998). *Cibersociedad y juventud: la cara oculta (buena) de la Luna.* Obtenido de Cibersociedad y juventud: la cara oculta (buena) de la Luna.: http://tecnologiaedu.us.es/cuestionario/bibliovir/ciberjuve.pdf

Calizaya, L. (2012). *En el trabajo de grado "Administración de la Red de Datos c Internet en el Predio Central de la U.A.P."* . Cobija-Pando-Bolivia.

Castro, H. (septiembre de 2014). *sistemasacademico.uniandes.edu.co.* Obtenido de sistemasacademico.uniandes.edu.co: https://sistemasacademico.uniandes.edu.co/~isis3204/dokuwiki/lib/exe/fetch.php?media=tutoriales:tutorial_wireshark_rev_1.pdf

Cisco. (2016). *Cisco.* Obtenido de Cisco: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Cisco, c. (2016). *CISCO*. Obtenido de CISCO: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

CiscoASA. (1 de Enero de 2015). *OVH.es*. Obtenido de OVH.es: https://www.ovh.es/servidores_dedicados/firewall_vpn_baie_virtuelle.xml

Ecured. (24 de agosto de 2016). *Red de área local (LAN)*. Obtenido de Ecured: http://www.ecured.cu/Red_de_%C3%A1rea_local_(LAN)

e-ducativa.catedu.es. (20 de agosto de 2016). *Seguridad informatica*. Obtenido de Seguridad informatica: http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio/1000/1063/html/1_la_seguridad_informtica.html

ESTEVE, J. M. (2008). la educacion en la sociedad del conocimiento. *La Tercera revolucion educativa*.

Fong, V. H. (2015). *Implementación de una red de datos del laboratorio del programa de ingeniería de sistemas en el área de ciencia y tecnología de la universidad amazónica de pando.* Cobija-Pando-Bolivia.

Gardey, J. P. (2011. Actualizado: 2014). *definicion.de*. Obtenido de definicion.de: http://definicion.de/cableado-estructurado/

gmtyasoc. (2000-2001). *gmtyasoc.com.* Obtenido de gmtyasoc.com: http://www.gmtyasoc.com.ar/contenido/cableado.htm

Huaygua, A. C. (2005). *Administración de la red de datos e internet (DIA).* cobija-pando-bolivia.

Ing, J. J. (2013). *CABLEADO ESTRUCTURADO*. URUGUAY.

Joskowicz, D. I. (2013). *CABLEADO ESTRUCTURADO*. Montevideo, URUGUAY: Instituto de Ingeniería Eléctrica, Facultad de Ingeniería.

Ledezma. (2012). *En proyecto de internet como una red de redes.* Cobija-Pando-Bolivia.

Magedanz, S. T. (diciembre de 1996). redes, gestión de redes y servicio de administración. *Diario de Redes y Sistemas de Gestión, Vol. 4*, pág. No 4.

Mamani, H. E. (2015). *En el trabajo de grado Implementación de la red de datos para la ampliación y optimización del ancho de banda de coteco LTDA.* Cobija-Pando-Bolivia.

Mendez, A. (2011). *Implementacion de un servidor proxy para la administracion de la red de datos e internet en el Consulado dle Basil en Cobija.* Cobija-Pando-Bolivia.

Merino, J. P. (2011-2014). *definicion.de.* Obtenido de definicion.de: http://definicion.de/red-de-computadoras/

MÓDULO I: Las TIC y Educación. (2005). *SEMINARIO PARA DECIDORES DE POLÍTICAS SOBRE TIC EN EDUCACIÓN PARA CENTROAMÉRICA.*

Monasterios, V. H. (2015). *IMPLEMENTACIÓN DE UNA RED DE DATOS DEL LABORATORIO DEL PROGRAMA DE INGENIERÍA DE SISTEMAS EN EL ÁREA DE CIENCIA Y TECNOLOGÍA DE LA UNIVERSIDAD AMAZÓNICA DE PANDO.* Cobija Pando Bolivia.

Nunez, D. M. (26 de febrero de 2012). *scribd.* Obtenido de scribd: https://es.scribd.com/doc/313601038/Manual-Wireshark

ORTI, C. B. (2016). *LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACION (TIC).* Unidad de Tecnología Educativa. Universidad de Valencia.

Pascual, M. F. (2004-2005). *Redes de Datos.* tudela.

Porto, A. G. (2011. Actualizado: 2014). *definicion.de.* Obtenido de definicion.de: http://definicion.de/cableado-estructurado/

Porto, J. P. (2012). *Definicion.de.* Obtenido de Definicion.de: http://definicion.de/soporte-tecnico/

raymundo, g. f. (2016). *camelo.* Obtenido de camelo: http://es.calameo.com/read/00444388428e4c4b640c7

sales, R. B. (2016). *Micogo.* Obtenido de Micogo: http://www.mikogo.es/guia/soporte-informatico/

Sanchez, V. G. (2009). *ENTORNOS VIRTUALES PARA LA FORMACION PRACTICA DE ESTUDIANTES DE EDUCACION: IMPLEMENTACION, EXPERIMENTACION Y EVALUACION DE LA PLATAFORMA AULAWEB.* Universidad Granada.

Seguridad, M. d. (2016). *Seguridad en Redes.* Obtenido de Seguridad en Redes: http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

Sistem, v. (2004-2012). *vigo Sistem.* Obtenido de vigo Sistem: http://www.vigosystem.com/servicios_redes.asp

trendcorp. (2014). *trendcorp.* Obtenido de trendcorp: http://www.trendcorp.com.pe/intrusos.html

Tripod. (2016). *Tripod.* Obtenido de Tripod: http://salmo-01.tripod.com/Topologias1.HTML

UAP. (2016). *Universidad Amazonica de Pando.* Obtenido de http://uap.edu.bo/index.php/launiversidad/resena-historica

UAP. (15 de 03 de 2016). *Universidad Amazonica de Pando*. Obtenido de http://uap.edu.bo/index.php/launiversidad/resena-historica

uv.es. (17 de julio de 2016). *uv.es*. Obtenido de uv.es: http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html

Vicente, C. A. (cinco de mayo de 2005). *Un modelo funcional para la administración de redes.* Obtenido de ABCdatos: http://www.abcdatos.com/tutorial/administracion-redes.html

wiikipedia. (2016). *wikipedia.* Obtenido de wikipedia: https://es.wikipedia.org/wiki/Monitoreo_de_red

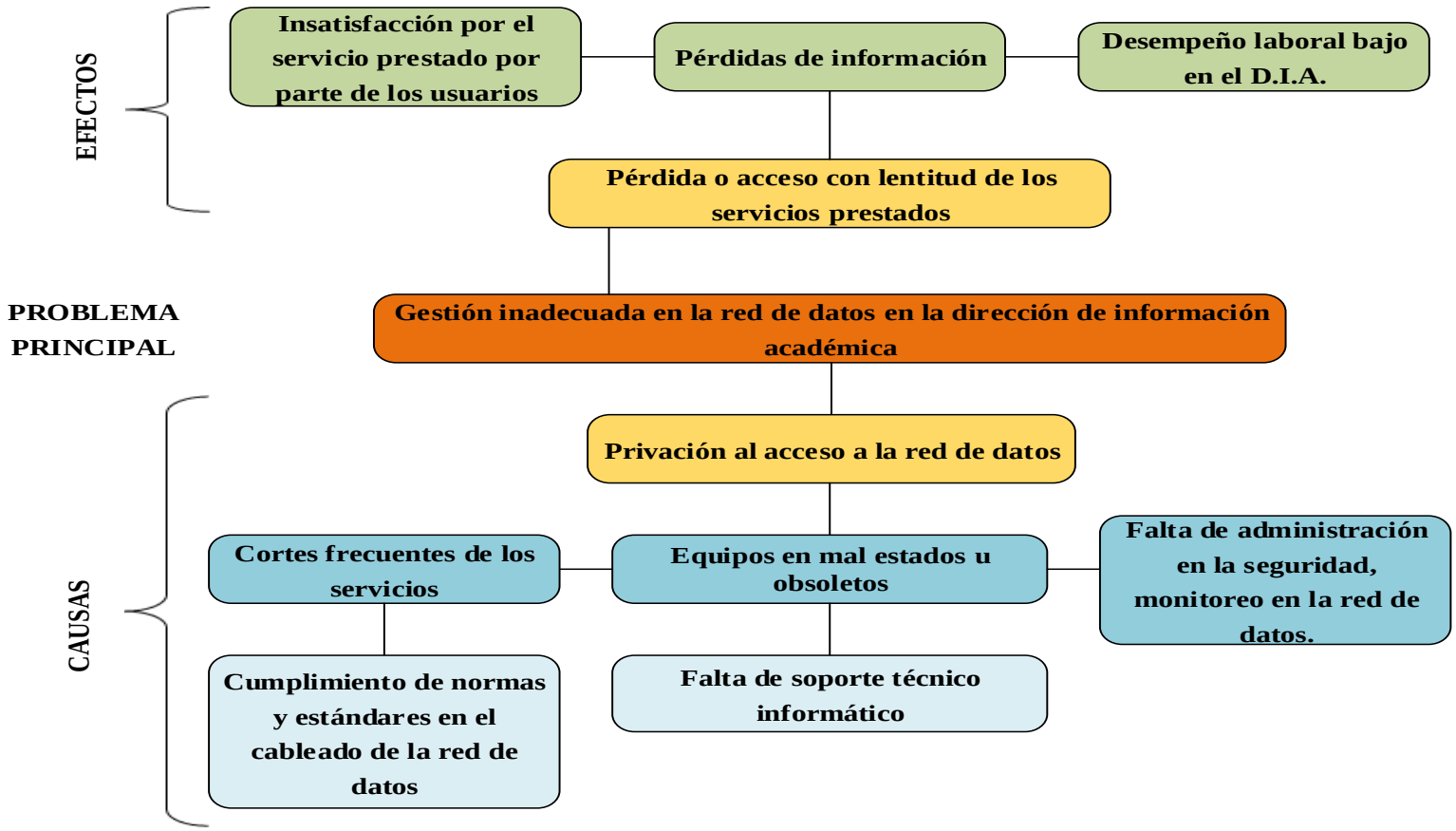
wikitel. (2016). *wikitel.* Obtenido de wikitel: www.wikitel.info/wiki/Redes_de_datos

Zenteno, D. (2009). *Servidor de administracion de ancho dr banda en la Universidad Amazonica Pando.* Cobija-Pando-Bolivia.

8.ANEXOS

ANEXO A

ARBOL DE PROBLEMA


EFECTOS
Insatisfacción por el servicio prestado por parte de los usuarios
Pérdidas de información
Desempeño laboral bajo en el D.I.A.
Pérdida o acceso con lentitud de los servicios prestados
PROBLEMA PRINCIPAL
Gestión inadecuada en la red de datos en la dirección de información académica
Privación al acceso a la red de datos
CAUSAS
Cortes frecuentes de los servicios
Equipos en mal estados u obsoletos
Falta de administración en la seguridad, monitoreo en la red de datos.
Cumplimiento de normas y estándares en el cableado de la red de datos
Falta de soporte técnico informático

ANEXO B

CUESTIONARIO SOBRE LA RED DE DATOS

Análisis de Requerimientos por parte de los Usuarios de la Red de Datos.

Como parte de la planeación y diseño de la red de datos se vio en la necesidad de reunir las necesidades de los usuarios y de la red, para ello se realizó un análisis de los requerimientos de los usuarios, para la obtención de la información se realizó entrevistas y una encuesta a los usuarios de la red de la Dirección de Información Académica. El análisis sirvió para apreciar las necesidades con las que contaban los usuarios, toda la información que fue adquirida por parte de los usuarios fue referente a los requerimientos de la red de datos.

Se realizó la recolección de los registro de los datos físico de los usuarios y se aplicó una encuesta para reunir las necesidades de los usuarios, fueron registrados y encuestados los usuarios que tienen acceso a la red de dato. El diagnóstico total, ayudó a detectar un conjunto de problemas los cuales surgen como una necesidad por parte de los usuarios.

A través de la información obtenida en el análisis se muestra la representación gráfica de cada pregunta de selección múltiple, que resume el estado de la red de datos en la Dirección de Información Académica.

Las preguntas realizadas en la encuesta fue referente a las necesidades por parte de los usuarios, la misma se la realizó a cada uno de los funcionarios de la Dirección de Información Académica, posteriormente se realizó la respectiva verificación y ponderación en porcentaje de las respuestas de todos los encuestados, cabe mencionar que los usuarios encuestados fueron 18.

CUESTIONARIO SOBRE LA RED DE DATOS DE LA DIRECCIÓN DE INFORMACIÓN ACADÉMICA

1. -Usted tiene acceso a los Sistema de la UAP
   a) Siringuero
   b) Monitoreo
   c) Otro…

2. ¿Cómo comparte sus archivos con otros funcionarios de la Unidad?
   a) A través de Flash
   b) A través de un Disco Portable
   c) A través de una Red Interna
   d) Otro
   e) Ninguno

3. ¿Cómo realiza usted sus impresiones?
   a) A través de Una Red
   b) Utilizo una impresora de la Oficina

4. ¿Qué sugerencia tiene Ud. Para tener una comunicación fluida en cuanto a datos e Información?

   ……
   ……
   ……

5. ¿Cómo calificaría al servicio de la red de datos en la Dirección de Información Académica?
   a) Excelente
   b) Bueno
   c) Regular
   d) Malo
   e) Pésimo

6. ¿Usted cree que la implementación de una red de datos, en la Dirección de Información Académica mejoraría los servicios en la red de datos?
   a) Si
   b) No

7. ¿Cuenta con soporte técnico informático o asistencia técnica de alguna duda que tenga con el servicio de la red?
   a) Si
   b) No

A continuación se observa el diagnóstico realizado en la Dirección de Información Académica.

1) Usted tiene acceso a los Sistema de la UAP

GRAFICO 4: *Resultado del diagnóstico de la primera interrogante de la encuesta*
Fuente: *Elaboración propia*

Esta interrogante tenía como objeto saber si se contaba con acceso a algún sistema de la Universidad, del total de las personas entrevistadas las mismas fueron 18 un 94% señaló tener acceso al sistema Siringuero, un 6% señala que tiene acceso al sistema de Monitoreo y un 0% señala no tener acceso a otro sistema. Del análisis de los resultados obtenidos podemos señalar que todos los usuarios cuentan con acceso de uno u otro sistema.

2) **¿Cómo comparte sus archivos con otros funcionarios de la Unidad?**

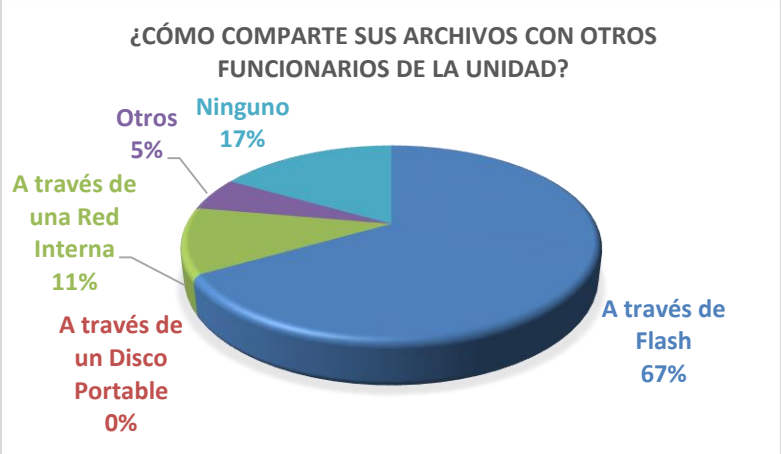


GRAFICO 5: *Resultado del diagnóstico de la segunda interrogante sobre la encuesta.*
Fuente*: Elaboración propia*

Esta interrogante tenía como propósito saber el medio o forma de compartir sus archivos con los demás funcionarios de su Unidad. Del total de las personas entrevistadas las mismas fueron 18 un 67% respondió al respecto de esta interrogante que compartía su información a través de Flash, el otro 11% comparte a través de la Red interna, el 5% utiliza otro medio de trasmisión de su información, también se puede evidenciar que un 17% no comparte o no tiene algún medio o forma de como compartir su información. Como se puede afirmar que solo un 11% utiliza la red, se llega a la necesidad de tener la red optima, segura, para mantener su información protegida y así mismo los demás usuarios puedan compartir sus archivos.

3) **¿Cómo realiza usted sus impresiones?**

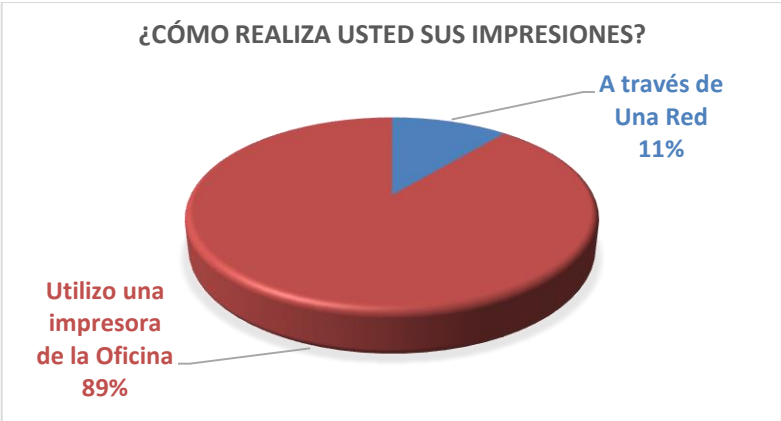


GRAFICO 6: *Resultado del diagnóstico de la tercera interrogante de la encuesta*

***Fuente**: Elaboración propia*

Con relación a la interrogante de cómo realiza sus impresiones, un 89% de los 18 usuarios entrevistados menciona que realiza sus impresiones utilizando la impresora de oficina, y solo un 11% utiliza el servicio de impresión en red, de acuerdo a estos datos se ha visto necesario la configuración del servicio de impresión en red, ya que muchas veces en cada Unidad se cuenta solo con una impresora.

4) **¿Cómo calificaría al servicio de la red de datos en la Dirección de Información Académica?**

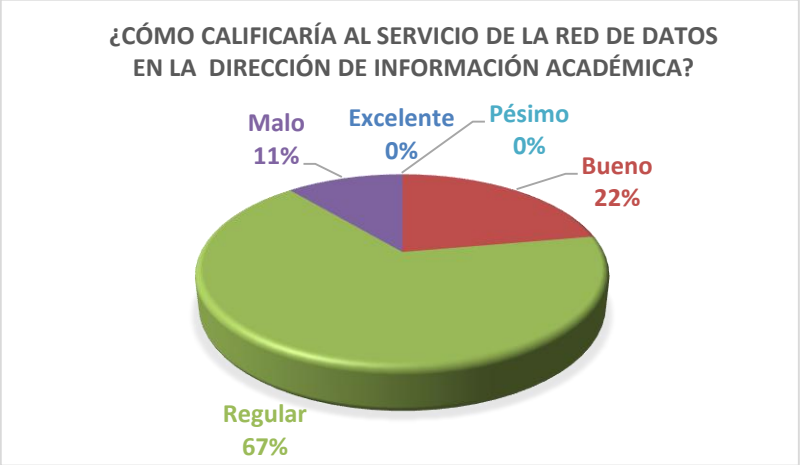


***GRAFICO 7:** Resultado del diagnóstico de la cuarta interrogante de la encuesta*
Fuente: Elaboración propia

Al respecto a esta interrogante que es una de las más significativa, ya que trata la calidad del servicio de la red de datos, la misma un 22% la consideró como buena y un 67% señaló como regular y un 11% señala que la red es mala, la misma ayuda a darnos cuenta que se debe mejorar el servicio de la red de datos, los mismos resultados obtenidos fue de un total de 18 encuestados.

5) **¿Usted cree que la implementación de una nueva red de datos, en la Dirección de Información Académica le permitirá mejorar su desempeño laboral?**

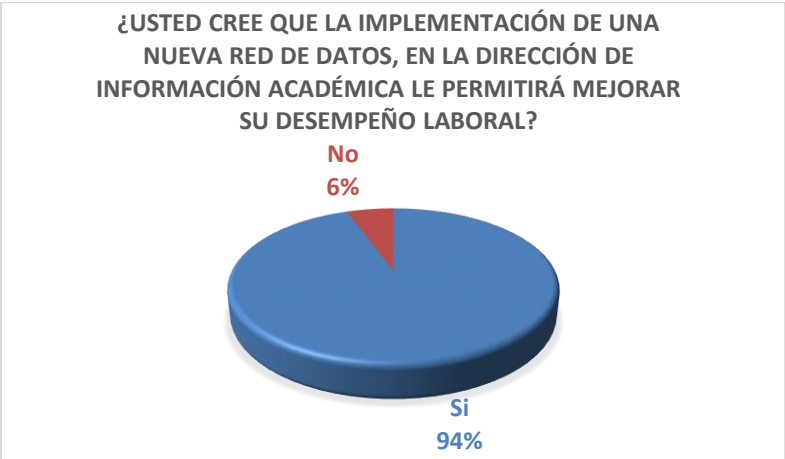


GRAFICO 8: *Resultado del diagnóstico de la quinta interrogante de la encuesta*
Fuente*: Elaboración propia*

Con relación a esta interrogante del total de las personas encuestadas las cuales fueron 18, un 94% señaló que si es necesaria la nueva implementación de la red de datos, ya que no satisface las necesidades de los usuarios, y un 6% especifican que no se requiere un cambio. La misma la mayoría si ve por conveniente el cambio.

6) **¿Cuenta con soporte técnico informático vía asistencia técnica de alguna duda que tenga con el servicio de la red?**

GRAFICO 9: *Resultado del diagnóstico de la secta interrogante de la encuesta*
Fuente*: Elaboración propia*

Esta última interrogante es a respecto al soporte técnico informático vía asistencia técnica, la cual del total de encuestados los mismos fueron 18, un 39% a especificado que si se lo

realiza y un 61 % señala que no se la realiza, la misma nos ayuda a afirmar que se tiene que mejorar al respecto a este punto.

De acuerdo a los resultados obtenidos de la encuesta y entrevista realizada a los usuarios de la Dirección de Información Académica, se ha determinado los siguientes requerimientos para un mejor funcionamiento de la red de datos:

- Realizar el diseño lógico y físico de la Red de datos de Datos en la Dirección de Información Académica, para así en lo posterior realizar su implementación.
- Configurar el servicio de impresión en red.
- Configurar la red para tener acceso a los sistemas que tiene la Universidad Amazónica de Pando.
- Tener una red optima segura para compartir archivos en la Dirección de Información Académica.
- Brindar soporte técnico informático constante para así mejor el servicio de los usuarios.

ANEXO C

FORMULARIO DE SOLICITUD DE REQUERIMIENTOS

	FORMULARIO SOLICITUD DE REQUERIMIENTO DE SISTEMA SIRINGUERO	Código: DIA-USA-FOR-001
		Versión: v.01
		Vigencia: 2015-12-11
		Página 1 de 1

DATOS GENERALES DEL SOLICITANTE			
De		Para	Ing. Freddy Morales Blanco
Cargo		Cargo	Responsable Unidad de Sistemas Académicos
Dirección o Unidad		Dirección o Unidad	Unidad de Sistemas Académicos
Fecha			

Universidad	Acite (solo para ...)	

DESCRIPCIÓN DE REQUERIMIENTOS GENÉRICOS		
N°	Requerimientos	Opción
1	Asignación de usuario y contraseña	
2	Desarrollo y mantenimiento de módulos del Sistema Siringuero	
3	Modificación y/o rectificación de datos en el Sistema Siringuero	
4	Revisión de alarmas de seguridad en las pruebas del Vase-Reforzado	
5	Capacitación a los usuarios administrativos, docentes y estudiantes del Sistema Siringuero	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIONES Y/O COORDINACIONES		
Nro.	Requerimiento	Opción
6	Parametros de programacion, impresion de actas, registro de notas.	
7	Apoyo técnico para manejo del Sistema Siringuero	
8	Otros	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIÓN INFORMACIÓN ACADÉMICA		
Nro.	Requerimiento	Opción
9	Mantenimiento y conectividad de redes de datos	
10	Apoyo técnico para manejo del Sistema Siringuero	
11	Creación de nuevos planes de estudios	
12	Creacion de cursos extracurriculares y tramites que no se encuentran en el Sistema Siringuero.	
13	Servicio de sistemas de colas, asignación de nuevas ventanillas y cajas	
14	Habilitacion de cupos en Sistema Siringuero para habilitacion de postulantes	
15	Otros	
Otros requerimientos que no estén contemplados en el formulario Especificar:		

DESCRIPCION DE REQUERIMIENTO
En esta sección puedes describir el requerimiento o adjuntar documentos

Usuario Solicitante	Jefe Inmediato Superior

FORMULARIO DE SOLICITUD DE REQUERIMIENTOS

	FORMULARIO CONFORMIDAD DE REQUERIMIENTO DE SISTEMA SIRINGUERO	Código: DIA-USA-FOR-003
		Versión: v.01
		Vigencia: 2015-12-11
		Página 1 de 1

DATOS GENERALES DE LA CONFORMIDAD DE REQUERIMIENTO					
De		Via		Para	
Cargo		Cargo		Cargo	
				Acite	

DESCRIPCION DE REQUERIMIENTO

DETALLE DE CONFORMIDAD DE REQUERIMIENTO	
NRO	ACTIVIDADES DESARROLLADAS

Aceptación de Conformidad	Administrador de Sistemas	Responsable U.S.A.

MCR-USA-004

	FORMULARIO	**Código:** DIA-USA-FOR-001
	SOLICITUD DE REQUERIMIENTO DE SISTEMA SIRINGUERO	**Versión:** v.01
		Vigencia: 2015-12-11
		Página **1** de **1**

DATOS GENERALES DEL SOLICITANTE			
De	Lic. Mayerlin Moreno Lima	Para	Ing. Freddy Morales Blanco
Cargo	Resp. Informaciones	Cargo	Resp. Unidad de Sistemas Académicos
Dirección o Unidad	Dirección de Información Académica	Dirección o Unidad	Dirección de Información Académica
Fecha	18/04/2016		
		#cite (solo para u.s.a)	

DESCRIPCIÓN DE REQUERIMIENTOS GENÉRICOS		
Nº	**Requerimientos**	**Opción**
1	Asignación de usuario y contraseña	
2	Desarrollo y mantenimiento de módulos del Sistema Siringuero	
3	Modificación y/o rectificación de datos en el Sistema Siringuero	
4	Revisión de cámaras de seguridad en los predios del Vice-Rectorado	
5	Capacitación a los usuarios administrativos, docentes y estudiantes del Sistema Siringuero	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIONES Y/O COORDINACIONES		
Nro.	**Requerimiento**	**Opción**
6	Parámetros de programación, impresión de actas, registro de notas.	
7	Apoyo técnico para manejo del Sistema Siringuero	
8	Otros… ……..	

DESCRIPCION DE REQUERIMIENTOS PARA DIRECCIÓN INFORMACIÓN ACADÉMICA		
Nro.	**Requerimiento**	**Opción**
9	Mantenimiento y conectividad de redes de datos	✓
10	Apoyo técnico para manejo del Sistema Siringuero	
11	Creación de nuevos planes de estudios	
12	Creación de cursos extracurriculares y trámites que no se encuentran en el Sistema Siringuero.	
13	Servicio de sistemas de colas, asignación de nuevas ventanillas y cajas	
15	Habilitación de cupos en Sistema Siringuero para habilitación de postulantes	
14	Otros	
Otros requerimientos que no estén contemplados en el formulario Especificar: Backup de Computadoras		✓

UNIDAD DE SISTEMAS ACADÉMICOS
COBIJA 18 ABR 2016
Horas: 12:05 Firma:
Universidad Amazónica de Pando

DESCRIPCION DE REQUERIMIENTO
En esta sección pueden describir el requerimiento o adjuntar documentos

Lic. Mayerlin Moreno Lima
RESP. INFORMACIONES
Universidad Amazónica de Pando
Usuario Solicitante

UNIVERSIDAD AMAZÓNICA DE PANDO
UNIDAD DE INFORMACIONES
COBIJA - BOLIVIA

Lic. Richard Rojas Lopez
JEFE UNIDAD DE TRÁMITES, REGISTROS E INFORMACIONES
Universidad Amazónica de Pando
Jefe Inmediato Superior

FORMULARIO CONFORMIDAD DE REQUERIMIENTO DE SISTEMA SIRINGUERO

Código:	DIA-USA-FOR-003
Versión:	v.01
Vigencia:	2015-12-11
	Página **1** de **1**

DATOS GENERALES DE LA CONFORMIDAD DE REQUERIMIENTO					
De	**Marco Antonio Montevilla Ruiz**	**Vía**	**Ing. Freddy Morales Blanco**	**Para**	**Lic. Juan Carlos Huanca Guanca**
Cargo	**Administrador de Redes de Datos**	**Cargo**	**Responsable Unidad de Sistemas Académico**	**Cargo**	**Director de Información Académico**
				#cite	

DESCRIPCION DE REQUERIMIENTO

- Implementación de nuevos puntos de red

DETALLE DE CONFORMIDAD DE REQUERIMIENTO

NRO	ACTIVIDADES DESARROLLADAS
	De acuerdo a formulario de solicitud de requerimientos se realizó la implementación de 4 puntos de red en la unidad de unidad de trámites.

M.Sc. Juan Carlos Huanca Guanca DIRECTOR DE INFORMACIÓN ACADÉMICA a.i. Universidad Amazónica de Pando **Aceptación de Conformidad**	Yesenia Velasco Amasifuen Administrador de Sistemas Académicos Unidad de Sistemas Académicos Universidad Amazónica de Pando **Administrador de Sistemas**	M.Sc. Ing. Freddy Morales Blanco Jefe Unidad de Sistemas Académicos Dirección de Información Académica Universidad Amazónica de Pando **Responsable U.S.A.**

ANEXO D

Formulario **DIA-USA-FOR-014** Informe de Incidentes en el Firewall

IDENTIFICACIÓN DE INCIDENTES

Información General

Información Detector de Incidentes:

Nombre:_____ Fecha y hora Detectado: _____

Unidad: _____

Telf:_____ Alt. Telf _____ Ubicación incidentes detectados Desde_____

_____ E-mail: _____

Datos del Incidente: _____

_____

Firma del Detector:_____

Resumen

Tipo de Propiedad Intelectual (IP) Detectado: Número total de artículos de IP detectados_____

- Image(s)
- Video
- Documento (s)
- Audio
- Aplicación (s) información adicional:_____

Otro:_____ _____

Raíz Localización de Elementos de IP (URL, etc.) sobre el Sistema Detectado:-_____

_____

Cómo se detecto:-_____

_____

_____

_____

_____

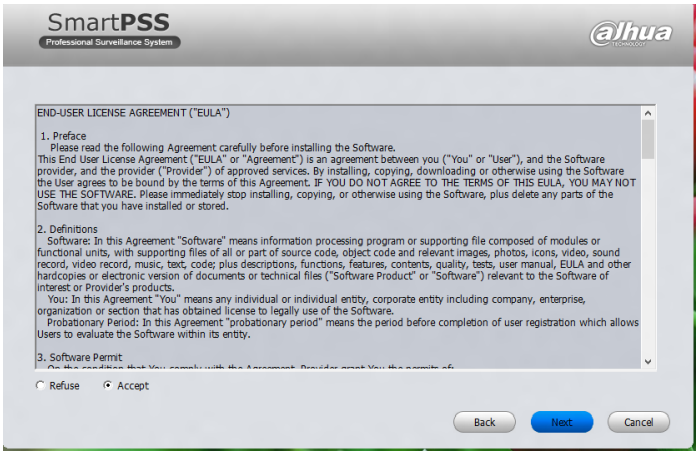
_____

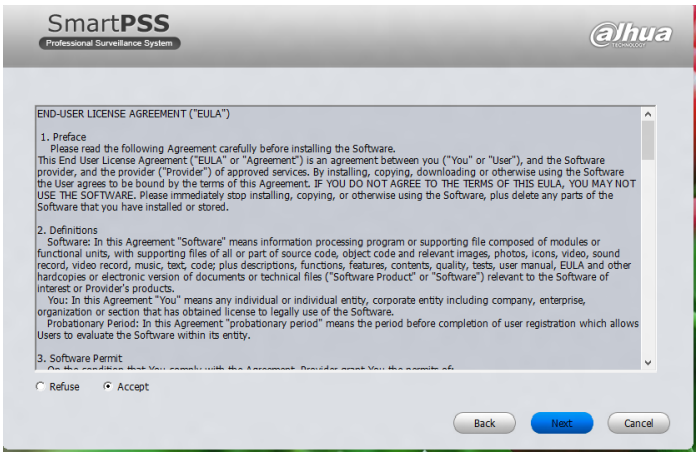
_____

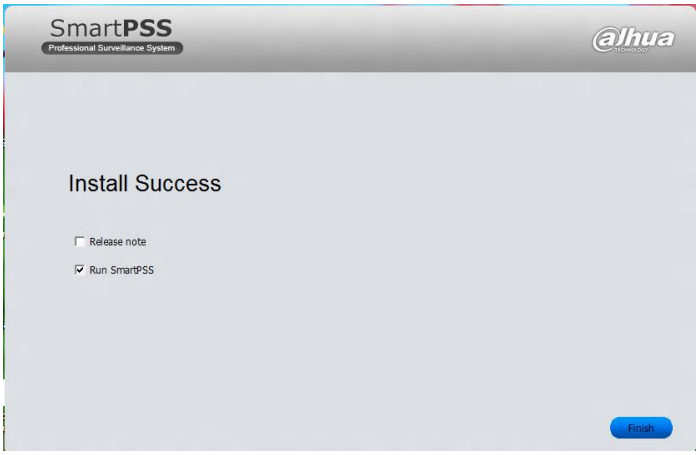
ANEXO E

INSTALACIÓN Y CONFIGURACION DEL SOFTWARE SMARTPSS

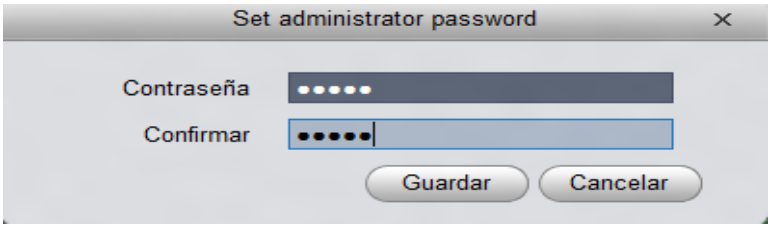
Al inicio de la instalación se lo instala por defecto presionando siguiente hasta finalizar la instalación.



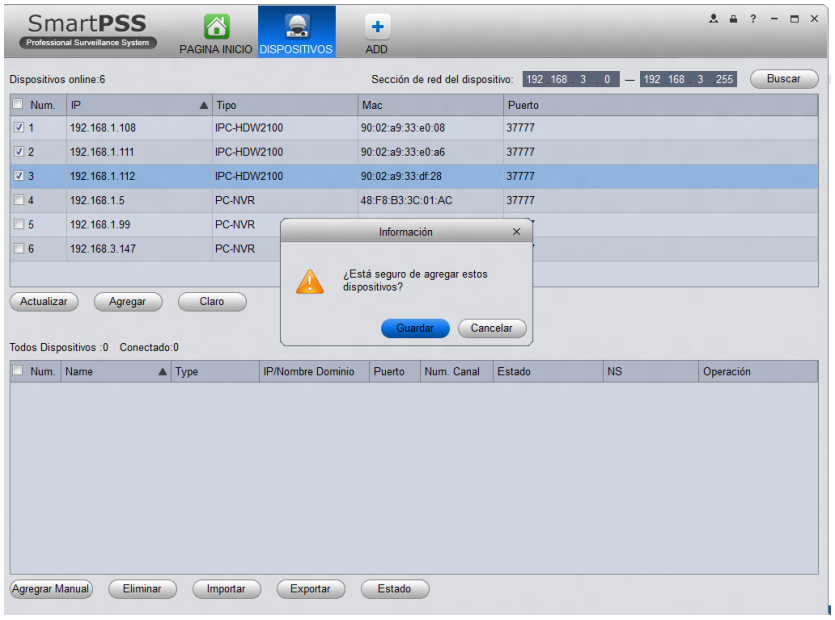




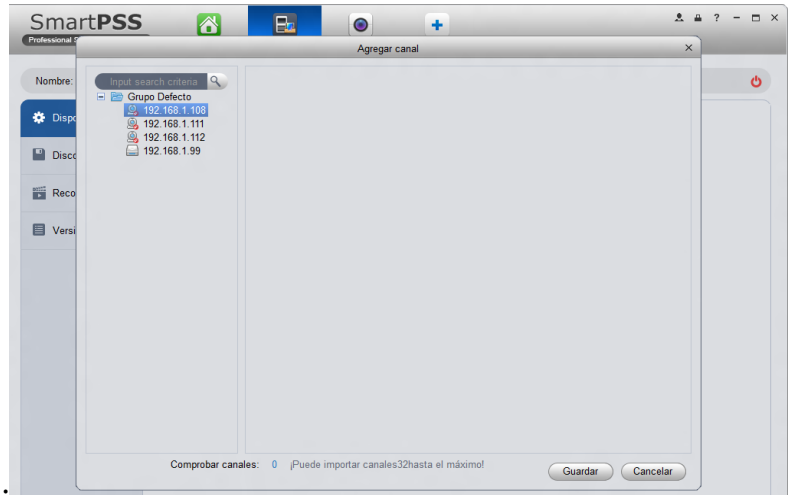
En la hora de ingresar por primera vez al programa le pedira ingresar una contraseña para el administrador, posteriormente esa contraseña le servira para ingresar al programa.

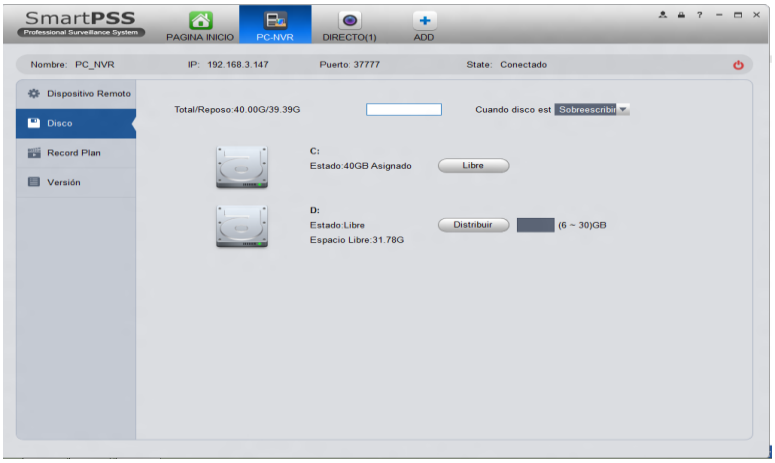


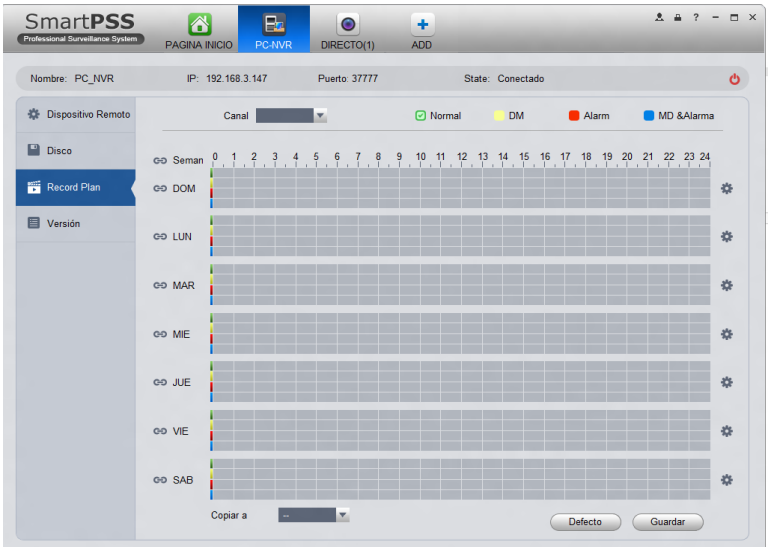
En esta figura se muestra la forma de agregar las cámaras para luego poder ser visualizada mediante el programa.



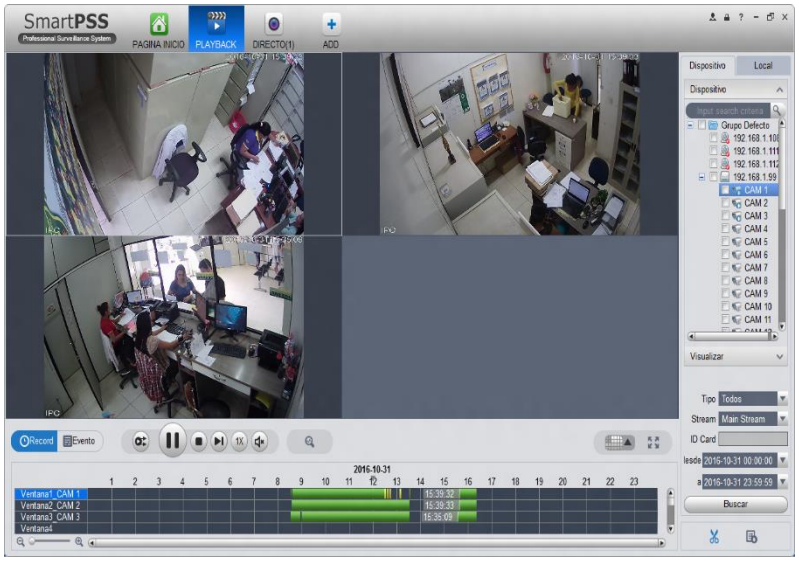
Las siguiente figuras muestran la configuración de PCNVR que permite almacenar las imágenes capturas por un periodo de tiempo







Para concluir con la configuración se puede verificar las imágenes almacenadas de un periodo anterior.



ANEXO F

POLITICAS DE SEGURIDAD

INTRODUCCION

El propósito de establecer las Políticas de Seguridad de Sistemas de Información en la Universidad Amazónica de Pando, es proteger la información y los activos de la Unidad de Sistemas Académicos/D.I.A, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos.

Estas políticas emergen como el instrumento para concienciar a cada uno de los miembros acerca de la importancia y sensibilidad de la información y servicios críticos. Para facilitar la gestión de la información en la U.A.P.

El proponer esta política de seguridad requiere un alto compromiso del personal de la U.S.A/D.I.A, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico.

JUSTIFICACION

Se propone estas políticas de seguridad, porque los servidores con los que cuenta la Unidad de Sistemas Académicos. Son de vital importancia y contienen información confidencial para toma de decisiones académicas y administrativas, es así que la confidencialidad emerge desde el momento en que se registran transacciones monetarias en cuanto a tramites en general y otras recaudaciones realizadas en dicha unidad, de la misma manera son de vital importancia proteger contra accesos internos, externos no autorizados, ya que se suministran notas de calificaciones académicas realizadas por las unidades académicas tanto docentes como estudiantes, estos dos componentes *(Transacciones monetarias y suministro de notas)* son considerados de alto grado de confidencialidad y críticas con respecto a seguridad.

La integridad y fiabilidad del funcionamiento de sistema Siringuero, y otros depende directamente y/o indirectamente de esos dos componentes citados anteriormente, es por tanto que es de mucha importancia y de prioridad la implementación de estas políticas de Seguridad. Ya que en los años

anteriores se ha visto vulnerados por agentes externos (Crackers) y han estado dañando la integridad del sistema y más específicamente del Sistema Siringuero.

OBJETIVO GENERAL

El objetivo general consiste en garantizar la seguridad, integridad y disponibilidad de la información de la Unidad de Sistemas Académicos para la Universidad Amazónica de Pando, donde se definen los lineamientos con el fin de establecer una cultura de la seguridad sistémico en la Universidad Amazónica de Pando. Asimismo establece los requisitos a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por este documento.

ALCANCE DE LAS POLÍTICAS

Las políticas definidas del presente documento aplica a todos los funcionarios, administrativos, docentes, estudiantes de la Universidad Amazónica de Pando, y otras personas relacionadas con terceras partes que utilicen recursos informáticos del Sistema Académico (siringuero).

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

Ataque cibernético: Un ataque cibernético es un intento por una o más personas organizada e intencionado de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones de dañar y perjudicar a un sistema informático o red.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Certificado Digital: un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor

Cifrar: quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama “descodificar" o “descifrar". Los sistemas de cifra miento se llaman 'sistemas criptográficos".

Criptografía de llave publica: es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

DIA: Dirección de Información Académica.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

Política: son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Siringuero: Sistema Académico Administrativo de la U.A.P.

USA: Unidad de Sistemas Académicos.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios del de la U.A.P., pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos

DESCRIPCIÓN DE LAS POLITICAS

POLITICA 1

ACCESO A LA INLORMACIÓN

Todos los funcionarios administrativos, docentes, estudiantes que trabajan con el Sistema Académico (siringuero). Deben tener acceso sólo a la información necesaria para el desarrollo de

sus actividades. En el caso de personas ajenas a la U.A.P., La Unidad Sistemas Académicos debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información en cuanto a bases de datos, algoritmos, software, está a cargo del responsable de U.S.A. Solicitando con una carta al Vicerrectorado para cualquier fin.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la U.A.P., la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Universidad.

Calendario Académico

Todos los privilegios para el uso del Sistema Académico (SIRINGUERO) de la Universidad Amazónica de Pando, deberá terminar de acuerdo a cumplimiento del Calendario Académico establecido a inicio de gestión en concordancia con la finalización de prestación de servicios del (los) contratados, caso contrario deberán confirmar la cesación de sus funciones haciendo llegar la información mediante los medios correspondientes considerados para tal fin (ejemplo: DIA-USA-FOR-OOl " SOLICITUD DE REQUERIMIENTO DE SISTEMA")

Docentes

Docentes solamente deben tener privilegios según calendario académico para llevar a cabo las funciones aprobadas tales como subir las notas al Sistema académico (siringuero) y los estudiantes todo el año completo para ver sus notas respectivas.

Registro de eventos

Mediante el registro de eventos en los diversos recursos informáticos de la Unidad de Sistemas Académicos, Se deberá efectuar un seguimiento a los accesos realizados por los usuarios al Sistema Académico (siringuero) de la U.A.P., con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información documentando y aplicando las acciones tendientes a su solución, así mismo se registrará los ip de los usuarios con los cuales acceden al sistema.

POLITICA 2

ADMINISTRACION DE CAMBIOS

Todo cambio (creación y/o modificación de programas, pantallas y reportes) que afecte el Sistema Académico (siringuero), debe ser requerido por los usuarios y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración del sistema tendrá la facultad de aceptar o rechazar la solicitud.

Diferencia de Cambio entre Base de datos y Módulos

EL sistema SIRINGUERO trabajo en el modelo cliente servidor lo cual hace que los módulos como la base de datos, lo cual permite cambios diferentes a uno o a otro o a ambos a la vez no necesariamente tiene que los dos al mismo tiempo.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona solicitante.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por la Unidad de Sistemas, de acuerdo con el tipo de cambio, desarrollo y/o modificación o mejoras solicitado.

Cualquier tipo de cambio en el Sistema Académico (siringuero) debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio de un recurso informático de la Unidad de Sistemas Académicos relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

POLITICA 3:

SEGURIDAD DE LA INFORMACION

Los funcionarios administrativos, docentes, estudiantes y personal de apoyo de la U.A.P. son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Universidad (Estatutos, Normas y Políticas de la U.A.P), para proteger y

evitar pérdidas de información, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios administrativos, docentes, estudiantes, y personal de apoyo están completamente prohibidos suministrar cualquier información relacionada con la información de la Universidad administrada por el Sistema Académico (siringuero) a entes externos sin las autorizaciones respectivas del responsable de la Unidad de Sistemas Académicos.

Todo funcionario que utilice el Sistema Académico (siringuero), tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los funcionarios administrativos, docentes, estudiantes y personal de apoyo son responsables de la confidencialidad, el buen manejo de la información. Después de que deja de prestar sus servicios a la UAP, deben hacer entrega de toda la información respectiva de todo su trabajo realizado. Una vez cumplida su contrato y/o cesado su cargo, está totalmente prohibido utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la U.A.P. está estipulado en la ley N° 1322 sobre el derecho del autor, directamente o través de terceros, así mismo, los funcionarios administrativos, docentes y estudiantes que detecten el mal uso de la información está en la obligación de reportar el hecho a las autoridades correspondientes (Dirección de Información Académica).

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

POLITICA 4

SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

Los funcionarios administrativos, docentes, estudiantes y personal de apoyo no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de texto, correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Universidad Amazónica de Pando. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fúentes, documentación y otros materiales.

Los funcionarios administrativo, docentes, estudiantes y personal de apoyo que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la Universidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet, tales políticas emanadas por la USIC.

En cualquier momento que un personal dependiente de la Unidad de Sistemas Académicos, publique un mensaje en un grupo de discusión de Internet, SMS de texto, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la U.S.A.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la unidad correspondiente, no utilizar el computador y desconectarlo de la red.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

POLITICA 5

SEGURIDAD EN RECURSOS INFORMATICOS

Todos los recursos informáticos, sistemas de información, sistemas y bases de datos deben cumplir como mínimo con lo siguiente:

Administración de cuentas de usuarios: Establece como deben ser utilizadas las claves de ingreso al Sistema Académico (siringuero) y otros recursos informáticos. Establece parámetros sobre la

longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: El Sistema Académico (siringuero), bases de datos y otras aplicaciones deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles de acuerdo su competencia. También deben permitir que un rol de usuario se encargue de la administración del sistema.

Plan de auditoría: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

Los agujeros de seguridad: Los agujeros de seguridad son entradas no convencionales al Sistema Académico (siringuero), bases de datos y otras aplicaciones. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas de información, bases de datos y otras aplicaciones, en tal sentido es necesario efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso al Sistema Académico (siringuero) y otros sistemas informatizados de la unidad de Sistemas Académicos debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso al Sistema Académico (siringuero) y otras aplicaciones que suministran los funcionarios administrativos, docentes, estudiantes y personal de apoyo son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna otra persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo.

Las Identificaciones de usuario deben únicamente identificar individuos esto quiere decir todo sistema debe tener definidos los perfiles de usuario de acuerdo con la fúnción y cargo de los usuarios que acceden a él.

El nivel de súper usuario del sistemas Académico (siringuero) u otros sistemas de información se consideren críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del Sistema Académico (siringuero).

Toda la información del servidor del Sistema Académico (siringuero) y otras bases de datos son consideradas crítica o valiosa en tal sentido debe tener controles de acceso y sometida a procesos de cifra miento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los directores, jefes de unidades, en conjunto con el personal de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en ejecución.

Los ambientes de desarrollo de sistemas, pruebas y puesta en marcha deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

POLITICA 6

SEGURIDAD EN COMUNICACIONES

Las direcciones de URL (Localizador Uniforme de Recursos) internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Unidad Sistemas Académicos, deberán ser considerados y tratados como información confidencial.

La red de amplia cobertura geográfica a nivel nacional e internacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la U.A.P, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifra miento y

verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Los computadores de la Dirección de Información Académica los cuales se tienden a conectarse de manera directa con computadores de entidades externas, estas deben suministrar y ser supervisados que cuenten con conexiones seguras, y además previa autorización del personal de seguridad informática y/o la Unidad de Sistemas Académicos.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la U.A.P. e Internet deberá estar cifrada.

POLITICA 7

SEGURIDAD PARA USUARIOS TERCEROS

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de instituciones o personas externas para el funcionamiento del Sistema Académico (siringuero) que no sean propios de la U.A.P. y que deban ubicarse en sus instalaciones, los recursos serán.

Administrados y registrados por los personeros de la Unidad de Sistemas Académicos de la U.A.P. llenando el siguiente formulario (DIA-USA-FOR-OOl).

Los usuarios terceros tendrán acceso al Sistema Académico (siringuero) y a otros Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador. En todo caso deberá llenar el siguiente formulario (DIA-USA-FOR-OOl).

La conexión entre los sistemas internos de la Unidad de Sistemas Académicos, y otros de terceros debe ser aprobada y certificada por el personal de Seguridad Informática y/o Unidad de Sistemas Académico (siringuero) con el fin de no comprometer la seguridad de la información de la U.A.P.

Los equipos de usuarios terceros que deban estar conectados a la Red después de haber llenado el siguiente formulario (DIA-USA-FOR-OOl) se les informaran que deben cumplir con todas las normas de seguridad informática vigentes en la U.S.A. aprobado por las instancias superiores.

Para interconectar las redes de la U.A.P. con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la Unidad de Sistemas Académicos llenando el siguiente formulario (DIA-USA-FOR-OOl). La U.S.A. se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La U.S.A. se reserva el derecho de cancelar y terminar la conexión al Sistema Académico (siringuero) de terceros que no cumplan con los requerimientos internos establecidos por la U.S.A, sin antes realizando un correspondiente informe a instancias superiores.

POLITICA 8

SOFTWARE UTILIZADO Y SOFTWARE LIBRE

Todo software que utilice la U.A.P. será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Unidad de Sistemas Académicos o reglamentos internos.

Todo el software y/o sistemas de manejo de datos que utilice la U.S.A. dentro de la D.I.A. Ya sea de Comunicación o Académicas, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Unidad de Sistemas Académicos que garantice el conocimiento por parte de los funcionarios de las implicaciones que tiene el instalar software pirata en las computadoras de la unidad.

Existirá un inventario de las licencias de software oficial de la Unidad de Sistemas Académicos. Que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado. Deberá existir una reglamentación de uso para los productos de software instalado en demostración en los computadores de la U.S.A.

En el marco gubernamental, Bolivia es el único país que cuenta con normativa que respalda la migración hacia el software libre, expresado en el artículo 77 de la Ley de Telecomunicaciones y TIC (No. 164) y apoyado con la Resolución No 034/2014 del XII CONGRESO NACIONAL DE UNIVERSIDADES.

Es por tanto que el software libre está permitido y debe usarse para la actualización constante del software adecuando las aplicaciones al ámbito académico, investigativo, interacción social y extensión universitaria.

POLITICA 9

ACTUALIZACION DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos Servidores del Sistema Académico (siringuero) y otros equipos de cómputo ubicado dentro de la Unidad de Sistemas académicos de la U.A.P. (cambios de procesador, adición de memoria o tarjetas, etc.) debe tener previamente una evaluación técnica y autorización de la Dirección de Información Académica y la misma unidad.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (PC, servidores etc.) no deben moverse o reubicarse sin la aprobación previa de la Dirección de Información Académica y del Responsable de la Unidad de Sistemas Académicos a través del llenado del formulario (DIA-USA-FOR-OOl).

POLITICA 10

ALMACENAMIENTO Y RESPALDO

La información que es soportada por el Sistema académico (siringuero). Deberá ser almacenada y respaldada de acuerdo a instructivos de copia de seguridad de base de datos del sistema siringuero implementado en la gestión de calidad.

Debe existir una definición formal de las estrategias de generación, retención y rotación de las copias de respaldo.

La unidad de sistemas académicos definirá la custodia de los respaldos del Sistema Académico (siringuero) que se realizará externamente con una compañía especializada en este tema, para evitar pérdidas, daños, alteraciones y/o robos, etc.

El almacenamiento de la información deberá realizarse interna y/o externamente a la Unidad de sistemas académicos, esto de acuerdo con la importancia de la información para el funcionamiento correcto y la operación del sistema.

La Unidad de Sistemas Académicos en conjunto con el responsable de seguridad informática de los sistemas definirán las estrategias a seguir para el respaldo de la información.

POLITICA 11

CONTINGENCIA

El administrador o responsable de la Unidad de Sistema Académico (siringuero). Debe crear, preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que

Permita al sistema académico Siringuero que las. Aplicaciones y comunicación consideradas como críticas o valiosas estar disponibles en el evento de un desastre de grandes proporciones como incendio, terremoto, explosión, terrorismo, inundación etc.

Se realizara el respaldo de acuerdo a instructivos de copia de seguridad de base de datos del sistema siringuero implementado en la gestión de calidad.

POLITICA 12

AUDITORIA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la U.S.A, como son D.I.A, otros sistemas de información, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.

Todos los archivos a ser auditados deben proporcionar suficiente información para apoyar el monitoreo, control y auditorías.

Todos los archivos de auditorías de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos a la Unidad de Sistemas académicos previa autorización de la autoridad competente de la suministración y/o administración y custodia.

Todas las computadoras de la unidad de Sistemas Académicos (siringuero) deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoría interna o externa sea correcto.

POLITICA 13

SEGURIDAD FISICA

La unidad de sistemas académicos (siringuero), deberá contar con los mecanismos de control de acceso hacia los servidores del Sistema académico (siringuero), sistemas de base de datos, y otras aplicaciones tales como puertas de seguridad, sistemas de seguridad a través de sistema de alarmas y circuitos cerrados con cámaras de seguridad en las dependencias que la Unidad de Sistemas Académicos considere críticas.

Las instalaciones donde se alojen los equipos servidores, equipos de cómputo, telecomunicaciones deben estar completamente cerrados y aislados de las circulaciones de funcionarios. Las puertas y las ventanas deben contener llaves no vulnerables a personas maliciosos, de la misma manera deben estar completamente acondicionadas los cuales puedan generar temperaturas apropiadas para el funcionamiento adecuado de los equipos de cómputo o servidores.

Los visitantes hacia la Unidad de Sistemas Académicos de la U.A.P. deben ser escoltados durante todo el tiempo por un personal de Seguridad Informática autorizado, asesor o funcionario. Esto significa que se requiere de un escolta tan pronto como un visitante entra a la

Unidad de Sistemas Académicos y hasta que este mismo visitante sale de la misma controlada. Todos los visitantes requieren una escolta incluyendo administrativos, antiguos empleados, docentes, miembros de la familia del trabajador, personal de apoyo, consultores, estudiantes etc.

Siempre que un personal de la Unidad de Sistemas Académicos. Se dé cuenta que un visitante no está debidamente escoltado y se encuentra dentro de la Unidad de Sistemas Académicos de la

U.A.P, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en esta área restringida e informar a las responsables de la Seguridad Informática y/o responsable de la Unidad de Sistemas Académicos, y esta situación debe ser documentada para posteriores percances.

La Unidad de Sistemas, unidades de archivos, tramites académicos o áreas que la Unidad de Sistemas Académicos considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por un personal de la Unidad o Areas que trabajan cotidianamente en estos lugares.

Toda persona que se encuentre trabajando dentro de la Unidad de Sistemas Académicos deberá portar su identificación en un lugar visible.

En la Unidad de Sistemas Académicos. El responsable de la unidad si considera críticas deberá equipar con elementos de control de incendio, inundación, cámaras de videos y alarmas.

Las áreas de la Unidad de sistemas Académicos que el Responsable. Considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todas las personas externas y/o funcionarios de la U.A.P., etc. Visitantes a las Oficinas de la Unidad de Sistemas Académicos e instalaciones de los servidores de bases de datos y otras aplicaciones deben mostrar identificación con fotografía y firmar antes de obtener el acceso a estas áreas restringidas controladas por el responsable de la unidad y/o el responsable de Seguridad Informática.

Los equipos de microcomputadores de la Unidad de Sistemas Académicos (PC, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa, de los personeros de la Unidad de Sistemas Académicos.

Los particulares en general, entre ellos, los familiares de los funcionarios de la unidad de sistemas académicos., no están autorizados para utilizar los recursos informáticos de la U.S.A.

POLITICA 14

ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento de información, almacenados y manipulados en estaciones de trabajo (escritorio, oficina, etc.) como CD, USB memoria etc. con fin de reducir los riesgos, alteración y daño de la información durante el horario normal de trabajo y fuera del mismo.

POLITICA 15

ADMINISTRACION DE LA SEGURIDAD

Las pruebas de intrusión desde la red interna o externa, están totalmente prohibidas solo se autorizara el permiso a través del responsable de la Unidad de Sistemas Académicos, en el caso se encuentre personas tomando control de las sesiones sobre las terminales, este capturando información sensible y si son detectados vulnerando la red interna o externa, y usando las siguientes herramientas serán notificados y enviados a las autoridades pertinentes el caso:

Modem ADSL 1024 Kbps ISA ISP Server

Escáner de puertos y servicios

Escáner de Vulnerabilidades de Red

Injection SQL, Sniffer.

Escáner de Vulnerabilidades Web

Escáner de Vulnerabilidades BB.DD

Otras Herramientas de Hacking.

La evaluación de riesgos de seguridad para los sistemas de información y los Recursos Informáticos se debe ejecutar al menos una vez cada mes. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al responsable de la Unidad de Sistemas Académicos. O responsable de Seguridad Informática.

Los funcionarios administrativos, docentes, estudiantes y el personal de apoyo de la U.A.P. que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por Unidad de Sistemas Académicos y responsable de Seguridad Informática.

El responsable de Seguridad Informática divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportara a la dirección correspondiente, los casos de incumplimiento con copia a las Unidades de Sistema Académicos.

POLITICA 16

SEGURIDAD EN EL ACCESO AL SISTEMA SIRINGUERO

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para el control de acceso y para el seguimiento de las actividades de los usuarios.

A continuación se detalla las diferentes partes implicadas en garantizar la seguridad de la información del Sistema Académico (siringuero).

Identificación de usuarios.

Es la clave que permite a un usuario acceder de forma individual al Sistema Académico (siringuero). Cada identificador de usuario está asignado a una persona, que es responsable de las actividades realizadas por él. El identificador de usuario se asigna a una persona para facilitarle el acceso al Sistema Académico (siringuero).

Utiliza un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación una sola vez, en la primera conexión al Sistema Académico (siringuero).

Dedicar un sistema a las funciones de control de seguridad, de modo que antes de permitir el acceso del usuario al Sistema Académico (siringuero), se verifique una sola vez su identidad y autorizaciones de acceso. Este Sistema es gestionado por el Responsable de la U.S.A.

Autorización de Usuarios.

El acceso de cada usuario al Sistema Académico (siringuero) para los trabajadores administrativos tales como directores, coordinadores, auxiliares de técnicos. Tiene que hacer una solicitud a la D.I.A. y luego derivado a la U.S.A. para asignarle un usuario en el sistema. Hay definido un formulario (DIA-USA-FOR-009), para autorizar la inclusión de nuevos identificadores de usuarios y contraseñas en el sistema Académico (siringuero).

El acceso de cada usuario al Sistema Académico (siringuero) para los docentes y estudiantes. Tienen que apersonarse a la Unidad de Informaciones. Hay definido un procedimiento, para autorizar la inclusión de nuevos identificadores de usuarios y contraseñas en el Sistema Académico (siringuero).

Eliminación de Usuarios.

En caso de terminación de la necesidad de uso del Sistema Académico (siringuero) por razones de abandono a la Universidad Amazónica de Pando o caducación de acceso al sistema, hay definido un formulario (DIA-USA-FOR-009), para la eliminación o baja de usuarios. El director o inmediato superior del usuario es responsable de comunicar al responsable de la unidad de sistemas académicos las condiciones de que son motivo dicha eliminación. Esto es para prevenir el acceso de un usuario al Sistema Académico (siringuero), inmediatamente después de la comunicación de su director o responsable. Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro.

Control de contraseñas.

El acceso a la información sensible del Sistema Académico (siringuero), aplicaciones y sistemas informáticos está regulada contra accesos no autorizados, requiriéndose, dentro del ámbito informático el uso de una clave de usuario y una contraseña para poder acceder a ella.

La contraseña no podrá ser vista en ningún momento y en ningún sistema.

La contraseña deberá ser una combinación de letras mayúsculas, minúsculas, números y símbolos no relacionada con ningún dato de carácter personal.

La contraseña debe tener una longitud mínima de 8 caracteres y 12 máxima.

No empezar ni terminar con un número, no tener más de tres caracteres consecutivos idénticos, en cualquier posición, a los de una contraseña usada anteriormente.

No contener el usuario, como parte de la contraseña.

Ser cambiada, al menos, cada 120 días para usuarios generales como ser estudiantes y cada 30 días para usuarios que tengan algún tipo de privilegio o autoridad. Tiene que haber instalado un control que informe a los usuarios cuando su contraseña tenga que ser cambiada.

No ser reutilizada hasta después de, al menos, 12 cambios. El sistema Académico (siringuero) rechazará las contraseñas que no cumplan la normativa del control de contraseñas.

Restauración o cambio de contraseñas.

Hay definido un formulario (DIA-USA-FOR-OOl) para asegurar la restauración o cambio de contraseña, por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona. El formulario incluye la identificación positiva del solicitante, en caso contrario, el envío de la nueva contraseña al director, responsable o inmediato superior del usuario. Este proceso es automatizado para favorecer la gestión de la contraseña por el propio usuario o su director inmediato. Tanto la solicitud como la respuesta se realizan a través del formulario (DIA-USA-FOR-009).

En el caso de Directores de Áreas, administrativos, coordinadores etc. El/la administradora del sistema Académico (siringuero) es la encargada de restaurar o cambiar de contraseñas para los casos en los que a los usuarios se les haya olvidado.

Para los docentes y estudiantes pueden realizar también el cambio de contraseñas solicitando a la unidad de información académica.

Autorizaciones de acceso:

La autorización de acceso tiene que ser verificada mediante un identificador de usuario y contraseña válidos. Lina vez verificada la identidad del usuario que está accediendo, no debe haber restricciones para establecer la conexión, salvo las propias de la sesión o servicio.

ANEXO G

SITIO WEB DESARROLLADO PARA LA DIRECCIÓN DE INFORMACIÓN ACADÉMICA

Cabe mencionar que la misma no está en funcionamiento por de algunos percances que se presentaron.

ANEXO H

FORMULARIO MODIFICACIÓN DE RETROCESO DE FASES DE LAS EVALUACIONES DE LAS ASIGNATURAS.

UNIVERSIDAD AMAZÓNICA DE PANDO – COBIJA - BOLIVIA – MCMXCIII	**FORMULARIO** **RETROCESO DE FASE DE LAS ASIGNATURAS**	Código: DIA-UI-FOR-006 Versión: v.00 Vigencia: 2015-09-23 Página 1 de 1

ESTE FORMULARIO ESTA DESTINADO A MODIFICAR LAS FASES DE LAS EVALUACIONES DE LAS ASIGNATURAS

DATOS DEL /LA DOCENTE

Nombres y Apellidos: CARLOS MARADEY VIERA
Programa : DERECHO
Asignatura : ASESORAMIENTO Y REGISTRO DE DERECHOS REALES
Fecha : 30 de Septiembre 2016

DETALLE DE LOS SERVICIOS REALIZADOS POR EL / LA DOCENTE

EVALUACIÓN	☐ REGULAR	**FASE ACTUAL**	☐ REGULAR
	☐ MESA DE EXAMEN		☐ 2ª INSTANCIA
	☐ CURSO DE TEMPORADA		☒ PRE-CERRADA

DETALLE DE LOS SERVICIOS SOLICITADOS POR EL / LA DOCENTE

MODIFICACIÓN DE LA FASE	☐ REGULAR
	☐ 2ª INSTANCIA
	☒ PRE-CERRADA

Observaciones:.....
.....

Firma del Docente Solicitante	Firma del Coordinador del Programa	Firma Responsable Unidad de Informaciones

Dr. Mauricio Cairo Sánchez
COORDINADOR DEL PROGRAMA DE DERECHO
AREA DE CIENCIAS JURIDICAS Y POLITICAS
Universidad Amazónica de Pando

ANEXO I

DESARROLLO DE ACTIVIDADES REALIZADAS EN EL RED ACTUAL DE LA DIRECCIÓN DE INFORMACIÓN ACADÉMICA

Direcciones IP asignadas a las computadoras de la Dirección de Información Académica se muestra en la siguiente tabla:

Unidad de Sistemas Académicos		
1.	192.168.3.153	YESSENIA VELASCO AMASIFUEN
2.	192.168.3.148	ING. FREDDY MORALES BLANCO
3.	192.168.3.154	YOSEL JUTINIANO SALVATIERRA
4.	192.168.3.152	ALVARO MENDOZA SALAS
5.	192.168.3.250	ROGELIA AJNO BLANCO
6.	192.168.3.147	MARCO MONTEVILLA RUIZ
7.	x.x.x.x	SISTEMA SIRINGUERO BD
8.	x.x.x.x	SISTEMA SIRINGUERO APLICACION
9.	192.168.x.x (LAN) x.x.x.x (WAN)	FIREWALL
Unidad de Tramites y Registros e Informaciones Académicos		
10.	192.168.3.160	LIC.DANIELA NAKASHIMA
11.	192.168.3.137	LIC.ANAHI STEFANY VALLEJOS ACOSTA
12.	192.168.3.145	ALEXANDRA MENDOZA CRESPO
13.	192.168.3.162	VENTANILLA1
14.	192.168.3.161	VENTANILLA2
Unidad de Archivos Académicos		

15.	192.168.3.172	LIC. GUILLERMINA SUAREZ NOZA
16.	192.168.3.167	KEVIN RASHID NAJAYA MOLINA
17.	192.168.3.171	HAILIN VON BOEDT G.
18.	192.168.3.169	DYRCY CONDORI MELINA
19.	192.168.3.170	VIVIANA BEYUMA GARCIA
20.	192.168.3.77	MARCO ANTONIO CANEDO ROJAS
21.	192.168.3.168	DYRCCE MICAELA HEREDIA PACHECO
Dirección de Información Académica		
22.	192.168.3.152	MSC.LIC. JUAN CARLOS HUANCA GUANCA
23.	192.168.3.146	LIC. LORENA CALIZAYA LEDEZMA
24.	192.168.3.158	NARDA RISELY GUARI MEJIA
25.	192.168.3.150	SISTEMA DE COLA

Del mismo modo cabe mencionar que la dirección de información académica no cuenta con cableado estructurado, de toda forma se realizó el etiquetado de los cables para así tener un mejor control.

Unidad de Sistemas Académicos		
1.	Busa-u6	YESSENIA VELASCO AMASIFUEN
2.	Busa-u7	ING. FREDDY MORALES BLANCO
3.	Busa-u13	YOSEL JUTINIANO SALVATIERRA
4.	Busa-u14	ALVARO MENDOZA SALAS
5.	Busa-u15	UNIDAD DE TRAMITES Y REGISTROS
6.	Busa-u16	UNIDAD DE ARCHIVOS ACADÉMICOS
7.	Busa-u17	FIREWALL CISCO

8.	Busa-u18	ROGELIA AJNO BLANCO
9.	Busa-u19	MARCO MONTEVILLA RUIZ
10.	Busa-u20	SISTEMA SIRINGUERO BD
11.	Busa-u19	SISTEMA SIRINGUERO APLICACION
Unidad de Tramites y Registros e Informaciones Académicos		
12.	Butr-u1	LIC. DANIELA NAKASHIMA
13.	Butr-u2	LIC.ANAHI STEFANY VALLEJOS ACOSTA
14.	Butr-u3	ALEXANDRA MENDOZA CRESPO
15.	Butr-u4	VENTANILLA1
16.	Butr-u5	VENTANILLA2
17.	Butr-u8	CONMUTADOR CAJA
18.	Butr-u9	CERTIFICADOS
Unidad de Archivos Académicos		
19.	Buaa-u1	LIC. GUILLERMINA SUAREZ NOZA
20.	Buaa-u2	KEVIN RASHID NAJAYA MOLINA
21.	Buaa-u3	HAILIN VON BOEDT G.
22.	Buaa-u4	DYRCY CONDORI MELINA
23.	Buaa-u5	VIVIANA BEYUMA GARCIA
24.	Buaa-u6	MARCO ANTONIO CANEDO ROJAS
25.	Buaa-u7	DYRCCE MICAELA HEREDIA PACHECO
Dirección de Información Académica		
26.	Bdia-u1	NARDA RISELY GUARI MEJIA
27.	Bdia-u2	LIC. LORENA CALIZAYA LEDEZMA
28.	Bdia-u3	MSC.LIC. JUAN CARLOS HUANCA GUANCA
29.	Bdia-u4	CONMUTADOR CAJA
30.	Bdia-u5	SISTEMA DE COLA