UNIVERSIDAD AMAZÓNICA DE PANDO
ÁREA DE CIENCIAS Y TECNOLOGÍA
PROGRAMA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADO

TITULO: "IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO DEL SISTEMA SIRINGUERO DE LA UNIDAD DE SISTEMAS DEL VICE-RECTORADO DE LA U.A.P."

INFORME FINAL DEL PROYECTO DE GRADO PARA OPTAR AL TITULO DE INGENIERO EN SISTEMAS INFORMATICOS

Elaborado por: Univ. David Calliconde Montero.

Tutor **:** M.sc. Ing. Freddy Morales Blanco.
Asesor **:** Ing. Jhonny Willy Mamani Yanaca.

Cobija - Pando - Bolivia

2014

AGRADECIMIENTO

Al finalizar un trabajo tan arduo y lleno de dificultades como el desarrollo del proyecto de grado, es inevitable ocultar lo agradecido que estoy por las personas, que me rodean y me apoyaron en los momentos del desarrollo del proyecto de grado y a la Dirección de Información Académica como la Unidad de sistemas Académicos que han facilitado las cosas para que este trabajo llegue a un feliz término. Por ello, es para mí un verdadero placer utilizar este espacio para ser justo y consecuente con ellos, expresándoles mis agradecimientos.

A Dios por estar siempre conmigo en esta vida. Gracias a mis padres Ozita Montero Brito y Sixto Calliconde Mendoza, por haberme dado animó de estudiar y ayudarme a poder llegar a este objetivo a todos mis hermanos. Me gustaría hablar de mi gratitud por la valiosa orientación a mi Asesor el Ing. Jhonny Willy Mamani Yanca dando las gracias también a mi Tutor el Msc. Ing. Freddy Morales B., y a todos los docentes del área de ciencias y tecnología que contribuyeron en mi educación.

Como dejar de agradecer a todos los compañeros que conforma parte de la carrera de ingeniería informática, que en conversas de pacillo siempre, fortalecían mis ganas de seguir estudiando y también esos consejos de amigos.

Dedicatoria:

Se lo dedico a mi madre, mi padre, hermanos, y amigos por los incentivos, confianza y fortaleza en tiempos difíciles para que llegara a más una victoria.

Atte. David Calliconde Montero su Hijo y amigo.

RESUMEN

Uno de los métodos para la administración del acceso a los sistemas a través de las redes, es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada, la característica fundamental de un sistema de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red, esto quiere decir: soporte para los protocolos de red más importantes, una vez seleccionando la herramienta adecuada para la implementación, se utilizó la metodología basada en modelos funcionales estándar de la ITU, teniendo las ventajas y desventajas, se obtiene una análisis de uso del siringuero y la seguridad.

INDICE

1.- INTRODUCCIÓN

En la actualidad, con el crecimiento de los sistema de información que trabajan bajos las redes de computadoras en la utilización del internet o red LAN los sistemas computacionales que usan este medio para su funcionamiento son propensos a ataques, en gran medida maliciosos, estos ataques buscan intervenir en el buen funcionamiento de los sistemas operativos, sistemas de información, deteriorando o haciendo mal uso de la información.

Generalmente cuando se piensa en seguridad para los sistemas computacionales basados en redes se piensa en Routers, redes trampa o Honeynets, en Sistemas de Detección de Intrusos (IDS), uso de cifrado entre otros. En este contexto es como se nos presentan los Firewall (cortafuegos) como alternativa bastante útil y como una medida eficaz que nos permita a finar nuestros criterios de seguridad, además de darnos a conocer algunas debilidades o vulnerabilidades que pueda tener el sistema Siringuero.

La Universidad Amazónica de Pando ha evolucionado estructuralmente, así como los usuarios que acceden al sistema siringuero, El servidor del sistema siringuero está conectado solo por la red interna para brindar el servicio para la comunidad universitaria, La cual no cuenta con ningún nivel de seguridad para el acceso por la cual viaja todo tipo de información como las notas de los alumnos, transacciones de dinero etc.

En la actualidad el acceso al sistema siringuero del campus universitario presenta deficiencias entre las que podemos citar o detallar: No cuenta con registros que ingresan al sistema siringuero, sistema de identificador de intrusos (IDS), antivirus etc.

El propósito de la administración del acceso de seguridad al sistema siringuero es que permita garantizar la Confidencialidad, Integridad y Disponibilidad de la información que administra el sistema siringuero.

1.1. ANTECEDENTES

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

La Universidad Amazónica de Pando tiene servicio como servidores, Sistema SIRINGUERO, Servidor de ASISTENCIA. La red interna es administrada por la Unidad de Sistema de Información y Comunicación (U.S.I.C.) y el otro el de la Cooperativa de Telecomunicaciones Cobija LTDA (Coteco).

En la Universidad Amazónica de Pando se comenzó con servidor proxy para la administración de red LAN, Para las conexiones de los sistemas Coimata lo cual se limitaba en administrar solo la red de datos e internet, cuando no se contaba a un con mucho personal de la (Unidad de Sistemas de información y comunicación) U.S.IC. de la U.A.P.

Posteriormente se implementó un servidor proxy para la administración de la red datos e internet, basado en Linux debían, este ya realizaba el control del internet de todo los usuarios de la Universidad Amazónica de Pando.

Actualmente se obvio algunos de los servidores para la administración de red ya comentados anteriormente ya que se optó por implementar servidor MikrotikRouteros para la administración de la red de la U.A.P. La Unidad de Sistemas Académicos donde se encuentra el sistema Siringuero se encuentra conectada.

La administración de red actual que tiene no brinda todo aspecto de seguridad de la red del sistema siringuero porque solo se dedica a la administración de la red LAN y el internet y no específicamente hacia el sistema siringuero la cual no cuenta con la suficiente seguridad para el acceso de la información que brinda el sistema siringuero de la Universidad Amazónica de Pando.

1.2. DESCRIPCIÓN DEL PROBLEMA

El sistema siringuero de la Universidad Amazónica de Pando, por su gran crecimiento de sus infraestructura y la red de datos la misma no brindan ninguna seguridad al acceso de la información, proporcionados por el sistema siringuero de la U.A.P.

Por lo tanto, el sistema siringuero es vulnerable a intrusos y como consecuencia puede alterarse o perderse la información de notas y otros de los estudiantes o transacciones financieras, resultando para la institución daños irreparables a la administración académica de la Universidad Amazónica de Pando.

Por lo que se concluye que el problema principal es el siguiente:

"El sistema de seguridad del acceso al sistema siringuero no funciona de manera adecuada, lo que no permite el control de manera eficiente, en la Unidad de Sistemas de Vice-Rectorado de la U.A.P."

1.3. SOLUCIÓN PROPUESTA

Es de implementar un sistema de seguridad para el acceso al sistema siringuero, para que funcione de manera eficiente y segura el tráfico de la red para el sistema siringuero, en la que todos los usuarios estarán gestionados por un administrador, así evitando disconformidad en la conectividad y seguridad de la información, también se contara con un monitoreo continuo de los usuarios que accedan al sistema siringuero.

1.4. OBJETIVOS Y ALCANCES DEL PROYECTO

1.4.1. Objetivo general

Implementar un sistema de seguridad de acceso al sistema siringuero con características integrales, utilizando la metodología Modelo Funcional para la Administración de Redes, la cual permita administrar de manera eficiente en la Unidad de Sistemas del Vice-Rectorado de la U.A.P.

1.4.2. Objetivos específicos

- Análisis y diagnóstico del acceso al Sistema Siringuero de la Universidad Amazónica de Pando.
- Especificar el proceso de instalación de un servidor GNU/Linux de forma económica en un entorno administrativo, Configuración y Administración de Firewall.
- Asegurar los recursos del sistema siringuero, denegando el acceso a intrusos internos de la institución.

1.4.3. Alcances

El presente proyecto se limitara en:

El sistema a implementarse será accesible a los usuarios que puedan acceder al sistema siringuero desde los predios de la Universidad Amazónica de Pando así como Rectorado, Vicerrectorado etc. De manera segura al Sistema Siringuero respetando el acuerdo de servicio de conexiones internas por el administrador de redes de la Unidad de Sistema de Información y Comunicación (USIC), sin afectar el rendimiento de la red y con recursos disponibles que tiene la U.A.P.

Se delimita al filtrado de la información que contempla la red datos que ingresa al sistema de información (siringuero), Y no así al control de elementos tangibles de la red de datos de la U.A.P.

Otra limitación es que el Firewall "NO es contra Ingeniería Social", es decir que si un intruso logra entrar a la Unidad de Sistemas Académicos (U.S.A) y descubrir información, passwords y difunde esta información.

“Un largo camino comienza con su primer paso**”**

El anterior proverbio expresa lo que este proyecto quiere lograr, el mejorar la seguridad informática de la Universidad Amazónica de Pando, y servir como referencia para mejorar la seguridad de una red de datos en otras Organizaciones, tratando de cubrir todas las vulnerabilidades que pueda tener una empresa o institución.

1.5. METODOLOGÍA Y HERRAMIENTA UTILIZADA

1.5.1. Metodología

La metodología empleada para el proyecto de grado es el "Modelo Funcional para la Administración de Redes", el motivo principal para tomar esta metodología que el proyecto de grado es un cargo en base a funciones y esta metodología se basa en funciones, además, divide la administración de red en áreas funcionales (configuración, fallas, desempeño, contabilidad y **seguridad**), definiendo de esta forma una estructura organizacional con funciones bien definidas.

Esta metodología contiene cinco procesos (configuración, fallas, desempeño, contabilidad y **seguridad**) cada proceso tiene sus propias actividades. En base a la metodología adoptada, se consideró uno de los cinco procesos que es **Administración de la seguridad**, para dar solución a las necesidades inmediatas de mayor importancia abordadas en el presente trabajo.

1.5.2. Herramientas utilizada

La herramienta a utilizarse es Endian es una distribución OpenSource de Linux, desarrollada para actuar como corta fuego (firewall), enlutar y gestionar amenazas. Endian Firewall está basado originalmente en IPCop es una distribución del sistema operativo Linux y que su finalidad es la protección de la red en el que está instalado, proporciona una interfaz web para su administración, Se distribuye bajo la GNU una (Licencia Pública General), de muchos ventajas que tiene, es que su código es de código abierto que permite a los expertos la seguridad World Wide Web (Red mundial), examinar y reparar problemas de seguridad. ENDIAN tiene como objetivo ser un potente enrutador cortafuegos con altas funcionalidades extra, sin dejar de lado la simplicidad tanto en administración como en requerimientos de hardware, que a su vez, es un fork (desarrollo de software) de Smoothwall; pero ahora se está basando en LFS (Linux From Scratch – Linux desde cero).
La implementación de esta herramienta es totalmente gratuita, ya que es una distribución GNU/Linux, por lo tanto su licencia es OpenSource; por lo que se puede descargar una ISO desde el sitio Web oficial del proyecto Endian http://www.endian.com, no se requiere mucha capacidad física en la maquina en donde se va a implementar.

MARCO TEORICO

Este capítulo tiene por finalidad brindar el fundamento teórico en el cual se basa el presente trabajo dirigido. Para garantizar la comprensión de este fundamento teórico se vio por conveniente estructurar y clasificar en tres aspectos: el primer aspecto va relacionado a la metodología de administración de las redes de datos, el segundo aspecto va relacionado a la seguridad informática y tercer aspecto va relacionado a la red de datos.

2.1. METODOLOGÍA DEL MODELO FUNCIONAL PARA LA ADMINISTRACIÓN DE REDES

Según (Untiveros, 2004) 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.

2.1.1. Administración de redes.

El término *administración de redes* es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

Tres dimensiones de la administración de redes.

a) **Dimensión Funcional.** Se refiere a la asignación de tareas de administración por medio de áreas funcionales.
b) **Dimensión Temporal.** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.
c) **Dimensión del escenario.** Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

a) Dimensión Funcional

Existen diversas modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN de la ITU como el modelo OSI-NM (Network Management) son modelos funcionales que dividen la administración de una red en áreas funcionales (configuración, fallas,

desempeño, contabilidad y seguridad), definiendo de ésta forma una estructura organizacional con funciones bien definidas. De esto se deriva el nombre de modelos funcionales. El presente trabajo se basa únicamente a lo que proponen los modelos funcionales mencionados.

2.1.2. Desarrollo De La Metodología

Se sugiere la creación de las siguientes áreas funcionales para ser aplicadas en la administración de redes.

2.1.2.1.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.

a) 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:

- 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.

- Diseñar la topología de la red
- Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
- Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.
- 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.

b) 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.

c) 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.

- **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.

➢ **Administración del software, e**s 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 requiere 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 ftp.

d) 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.

e) 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.

2.1.2.2.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.

a) 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 utilizado por cada uno de los enlaces de área local (Ethernet, Fast ethernet, Gigabit Ethernet, etc), ya sea por elemento o de la red en su conjunto.
b) *Caracterización de tráfico, e*s 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 está 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.

b) 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:

- *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.
- *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.
- *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.

- *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.
- *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.

2.1.3. 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 restablecer la situación o minimizar el impacto de la falla.

2.1.3.1. 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.

a) 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.

b) 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.

2.1.3.2.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.

a) 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, s*on 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, e*sta 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.

2.1.3.3.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.

2.1.3.4.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.

a) 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 debe 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

b) 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 esta debe poder ser consultada en cualquier momento por el administrador.

c) 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.

d) 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.

2.1.4. 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.

2.1.4.1.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.

2.1.4.2.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.

2.1.4.3.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.

2.1.4.4.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.

2.1.4.5.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.

2.1.4.6.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.

2.1.4.7.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 la política de seguridad mediante los mecanismos adecuados.

2.1.5. Conclusiones

La administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras. Esto nos lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño más énfasis se debe poner en esta tarea.

En los puntos anteriores se describió una propuesta de administración para redes de datos. La propuesta se basó en la recomendación de la ITU-T, el modelo TMN y en el modelo OSI-NM de ISO. Se presentó una propuesta global que enfatiza en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc.

La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

2.2 SEGURIDAD FÍSICA Y LÓGICA

2.2.1 Seguridad física:

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

2.2.2 Seguridad lógica:

Es la seguridad que se logra a través de recursos incorpóreos, que no son físicamente tangibles, pero que están en capacidad de impedir que un individuo tenga acceso a un recurso que no le está autorizado.

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."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

a) Restringir el acceso a los programas y archivos.
b) Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

c) Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
d) Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
e) Que la información recibida sea la misma que ha sido transmitida.
f) Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
g) Que se disponga de pasos alternativos de emergencia para la transmisión de información.
h) Controles de Acceso

2.3 SEGURIDAD INFORMÁTICA

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, reglas, 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.

2.3.1 Objetivos de la seguridad informática

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

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.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

a) **Confidencialidad.-** La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.
b) **Integridad.-** La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).
c) **Disponibilidad.-** El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.
d) **No repudio.-** Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.
e) **Autenticación.-** La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

2.4 VULNERABILIDAD

Es la exposición latente a un riesgo en el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

2.5 VIRUS

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus

pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

2.6 SPYWARE

Los Spyware o archivos espías son unas diminutas aplicaciones cuyo objetivo es el envío de datos del sistema donde están instalados, mediante la utilización subrepticia de la conexión a la red, a un lugar exterior, el cual por lo general resulta ser una empresa de publicidad de Internet. Estas acciones son llevadas a cabo sin el conocimiento del usuario. El verdadero nombre de estos archivos espías, y procede de "Advertissing Supported Software".

Hay que aclarar que, aunque evidentemente tienen cierta similitud con los programas Troyanos, los Spyware no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos, así como una navegación más lenta.

2.7 SQL inyection

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté embebido dentro de otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

2.8 RFI (**Remote File Inclusión**)

Traducido al español como Inclusión Remota de Archivos - vulnerabilidad existente solamente en páginas dinámicas en PHP que permite el enlace de archivos remotos situados en otros servidores a causa de una mala programación de la página que contiene la función include().

Este tipo de vulnerabilidad no se da en páginas programadas en ASP o en cualquier otro tipo de lenguaje similar que no contenga la posibilidad de la inclusión remota de archivos ajenos al servidor.

2.9 BUFFER OVERFLOW

Básicamente un desbordamiento de buffer no tiene mucho secreto. Lo podemos comparar a cuando llenamos un cubo de agua, nos despistamos, el agua sale del cubo, no nos damos cuenta y al final se filtra y le cae al vecino de abajo. Normalmente este fallo se da cuando el programador no tiene en cuenta el tamaño de algún buffer dentro de su programa y si este se llena de datos que no tienen salida, afecta a otras partes de la memoria en las cuales hay otros datos o partes de otro programa viendo se afectados y pudiendo causar un bloqueo tanto del programa afectado y del propio software que lo produce.

2.9.1 ¿Cómo afecta a la seguridad de un equipo?

El problema de seguridad de los buffer overflow consiste en que si el programa hace llamadas a subrutinas con comandos que modifiquen esas subrutinas y estas caen en un desbordamiento de buffer, es decir, las subrutinas llamadas con esos modificadores se salen del buffer mediante un exploit, el proceso padre queda perdido y es cuando un atacante mediante dicho exploit puede incorporar rutinas a medida para que hagan lo que él, y no el programa afectado, quiera, y dentro de este ámbito de posibilidades está el peligro ya que podrían ejecutar aplicaciones con los permisos que tenga ese programa, normalmente de SYSTEM.

2.10 FIREWALL

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

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego una tercera red, llamada *Zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección (Ver Figura 2.1).

Figura 2.1: Esquema de un Firewall

Fuente: (www.uazuay.edu.ec***)***

2.11 SISTEMA DE PREVENCIÓN DE INTRUSIONES (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 Haile y Vern 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.

También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.

Funcionamiento

- Detección basada en firmas
- Detección basada en políticas
- Detección basada en anomalías
- Detección *honey pot* (jarra de miel)

Funcionamiento.- Un sistema de prevención de intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección basada en firmas: como lo hace un antivirus.
- Detección basada en políticas: el IPS requiere que se declaren muy específicamente las políticas de seguridad.
- Detección basada en anomalías: en función con el patrón de comportamiento normal de tráfico.
- Detección *honey pot* (jarra de miel): funciona usando un equipo que se configura para que llame la atención de los *hackers*.

Detección basada en firmas

Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta. Por ejemplo, los ataques contra los servidores Web generalmente toman la forma de URLs. Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor web. Sin embargo, como este

tipo de detección funciona parecido a un antivirus, el administrador debe verificar que las firmas estén constantemente actualizadas.

Detección basada en políticas

En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que hosts pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección basada en anomalías

Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. En este tipo de detección tenemos dos opciones:

1. Detección estadística de anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
2. Detección no estadística de anormalidades: En este tipo de detección, es el administrador quien define el patrón «normal» de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Detección *honey pot* (jarra de miel)

Aquí se utiliza un *distractor*. Se asigna como *honey pot* un dispositivo que pueda lucir como atractivo para los atacantes. Los atacantes utilizan sus recursos para tratar de ganar acceso en el sistema y dejan intactos los verdaderos sistemas. Mediante esto, se puede monitorizar los métodos utilizados por el atacante e incluso identificarlo, y de esa forma implementar políticas de seguridad acordes en nuestros sistemas de uso real.

Un IPS es un sistema de prevención/protección para defenderse de las intrusiones y no sólo para reconocerlas e informar sobre ellas, como hacen la mayoría de los IDS. Hay dos características principales que distinguen a un IDS (de red) de un IPS (de red):

El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como un 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.).

2.12 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

2.13 ANTIVIRUS

Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

Un antivirus tiene tres principales funciones y componentes:

- **Vacuna** es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real.

- **Detector**, que es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.
- **Eliminador** es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva.

2.14 REDES VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.
Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

2.15 REDES DE COMPUTADORAS

Según (Chapman, 2002), las redes de computadoras son un conjunto de equipos informáticos (computadoras) interconectados con la finalidad de compartir sus recursos de información así como los recursos de hardware (Ver Figura 2.2).

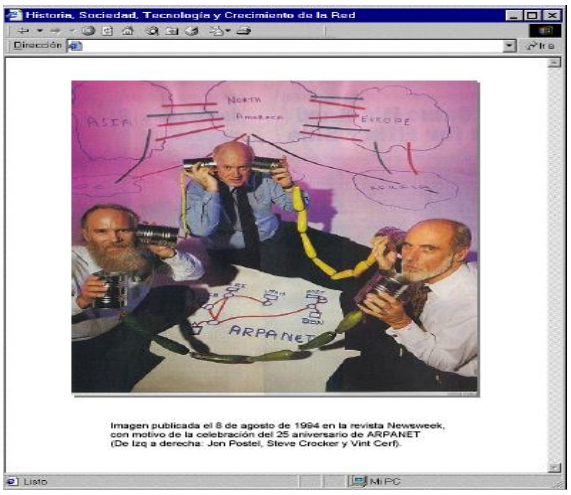


Figura 2.2: Prehistoria de la red (1964-1995)

Fuente: (Vea Baro, 2002)

2.15.1 Redes LAN

Según (Chapman, 2002), las redes LAN son propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo. Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red, además que suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.

2.15.2 Redes MAN

Este tipo de redes es una versión más grande que la LAN y que normalmente se basa en una tecnología similar a esta, La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione, que equivale a la norma IEEE.

Las redes Man también se aplican en las organizaciones, en grupos de oficinas corporativas cercanas a una ciudad, estas no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Estas redes pueden ser públicas o privadas.

Las redes de área metropolitana, comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 Km. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos.

2.16.3 Redes WAN

Son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un Router. Suelen ser por tanto redes punto a punto.

La subred tiene varios elementos:

- Líneas de comunicación: Mueven bits de una máquina a otra.
- Elementos de conmutación: Máquinas especializadas que conectan dos o más líneas de transmisión. Se suelen llamar en caminadores o Routers.

Cada host está después conectado a una LAN en la cual está el en caminador que se encarga de enviar la información por la subred.

Una WAN contiene numerosos cables conectados a un par de en caminadores. Si dos en caminadores que no comparten cable desean comunicarse, han de hacerlo a través de en caminadores intermedios. El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre.

Se pueden establecer WAN en sistemas de satélite o de radio en tierra en los que cada en caminador tiene una antena con la cual poder enviar y recibir la información. Por su naturaleza, las redes de satélite serán de difusión.

2.16 Topología de red

Según (Chapman, 2002) se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que podíamos llamar "puros" los cuales son: anillo, bus y estrella.

2.16.1 Estrella extendida

Según (Chapman, 2002), una topología en estrella extendida tiene una topología en estrella central, con cada uno de los nodos extremos de la topología en 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.

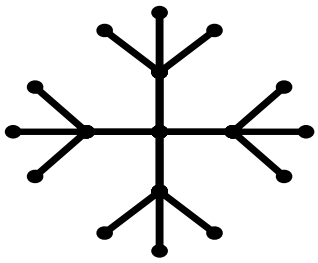


Figura 2.2: Topología de red estrella extendida

Fuente: (Chapman, 2002)

DESARROLLO DEL PROYECTO

Para llevar a cabo la implementación de un sistema de seguridad para la red de datos del sistema siringuero de la Unidad de Sistemas del vice-rectorado de la U.A.P., y la realización del esquema estructural de la red de datos del sistema siringuero de la Universidad Amazónica de Pando, se está haciendo seguimiento a la metodología funcional para la administración de redes, el cual se describió de manera detallada en el capítulo anterior, En la fase de análisis y diagnóstico se utilizó las herramientas como encuestas, Observación y análisis, Luego se utilizó la fase de administración de seguridad, para la implementación de seguridad de la red de datos del sistema siringuero de la U.A.P .

3.1. FASE DE ANÁLISIS Y DIAGNOSTICO

En esta fase se realizara el análisis anterior y diagnóstico, ya que por el aumento de usuarios y peticiones de conexiones al sistema de información, también creció la inseguridad de la red del sistema siringuero, en la que se optó, realizar el diseño del esquema de la red del sistema siringuero, utilizando la metodología funcional para la administración de redes, también las encuestas, para así hacer el estudio del uso del sistema siringuero, con los datos adquiridos se puede describir el funcionamiento debido de la red de datos del sistema siringuero y la descripción de cada usuario que este en la red del sistema siringuero.

3.1.1. Diagnóstico del uso del sistema siringuero

Se realizó el levantamiento de datos vía encuesta para diagnosticar el uso actual del sistema siringuero, fueron encuestados los funcionarios que tienen accesos a la sistema siringuero, para así poder tener un diagnostico actual de las problemáticas e inquietudes de cada usuario que gozan de este servicio.

Es así que obteniendo los resultados de dicha encuesta, se realizó el dicho estudio del análisis elaborado, dividiéndolos así en dos partes, en el análisis resultante actual y análisis provisional, en la que a continuación se explicara de forma narrativa.

a) **Análisis resultante actual:** Es logrado en la encuesta obtenida a los usuarios, que usan el sistema siringuero de la Universidad Amazónica de Pando, ya que fueron datos cuantitativos se deduce de esta manera:

   En el parámetro de tiempo se observó que los usuarios usan el sistema siringuero, en un promedio mayor a ocho hora diarias y en el horario de 08:00 a 12:00, aun teniendo en cuenta que la red del sistema siringuero no es muy seguro, en la que la mayoría de los usuarios usan sistema siringuero de acorde a su labor de trabajo, pero se obtuvo un porcentaje considerado de las personas que usan y acceden al siringuero en la que la mayor parte describe su problema de acceso al sistema siringuero es la red del campus de la Universidad Amazónica de Pando.

   Obteniendo la información de dicha encuesta, se puede predecir que es necesaria la implementación del servidor para la administración de la seguridad para la red de datos del sistema siringuero, de acuerdo esta conclusión obtenida:

   Tomando en cuenta que el uso del sistema siringuero es necesario en el ámbito laboral de la Universidad Amazónica de Pando y que el acceso al siringuero es constante y la red de datos no es muy segura, es necesario dicha implementación del servidor de seguridad lógica, ya que los usuarios acceden al sistema siringuero donde hacen visitas o ingresan al sistema siringuero, para el ingreso de notas de estudiantes, es por eso que el sistema siringuero debe de tener un sistema de seguridad para que así puedan acceder con seguridad al siringuero.

El estudio realizado también se puede observar de acuerdo a cada pregunta así se tendrá un vistazo aproximado de los resultados generales ya que se hizo bajo el modelo estadístico de

tipo encuesto donde eran mixtas las preguntas del tipo muestreo de toda la comunidad universitaria, docentes y estudiantes, es así que se tiene los resultados según a las preguntas propuestas, en la encuesta que se realizó **(VER ANEXO A).**

Así como se tiene los resultados obtenidos de cada pregunta, podemos mostrar un gráfico representativo de la preguntas de las encuestas realizadas:

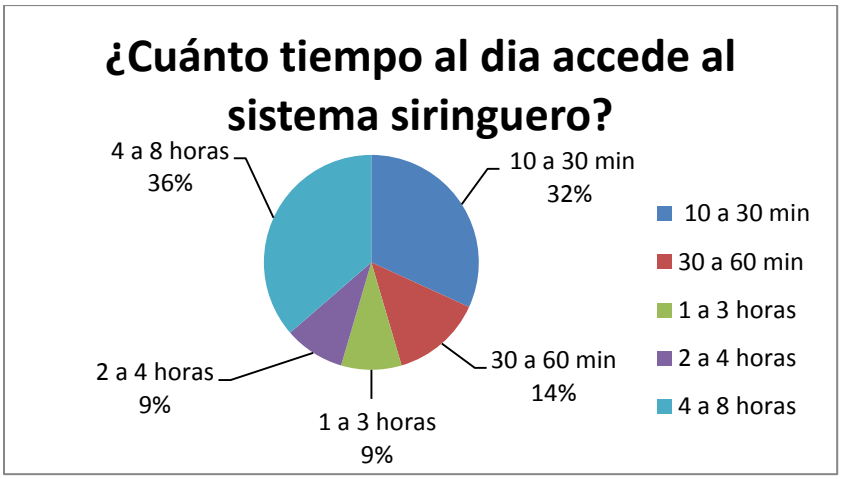


Figura 3.1: *Torta del tiempo de acceso al sistema siringuero*
Fuente: *Elaboración Propia.*

3.1.2. Diagnóstico de la red estructural vía observaciones y Análisis.

Se realizó el diagnóstico de la red del sistema siringuero mediante la observación, en la que se pudo observar el estado físico de la red, como también de los dispositivos que se interconectan entre sí de igual forma el cableado estructurado que su mayor parte no estaba bajo las normas adecuadas, y no se encuentra en buenas condiciones, ya que para la implementación del servidor no se debe tener roturas de conexión ni fugas de paquetes, por eso es necesario contar con un cableado regular para una buena comunicación entre el sistema siringuero y el usurario.

Figura 3.2: *Fotografía de una de las estaciones de trabajo*
Fuente: *Elaboración Propia*

Inicialmente, En esta primera parte voy a reconocer la estructura de la red de datos con el dude la organización de la red LAN. Para la Determinación de equipos activos

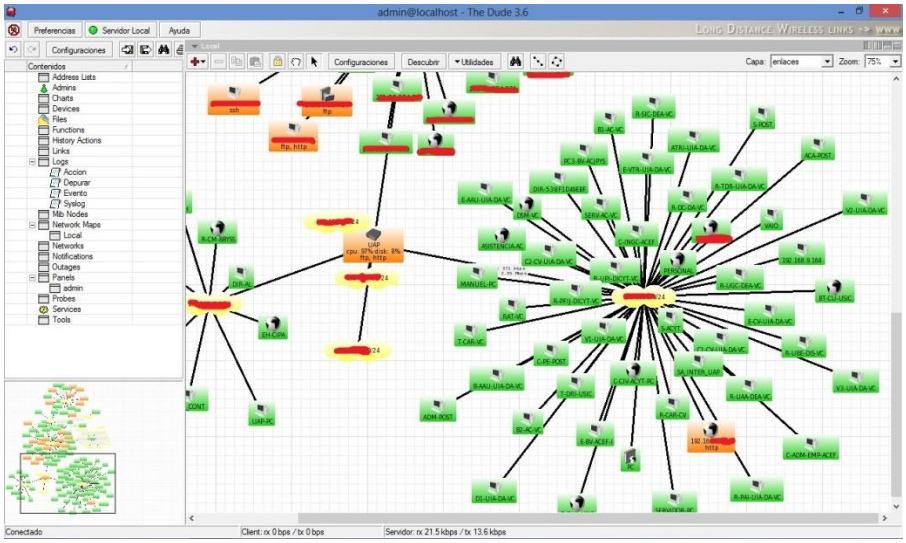


Figura 3.3: *Imagen de escaneo con Dude.*
Fuente: *Mapeo de Dude.*

Seguidamente, la seguridad de la infraestructura se evalúa con una herramienta para la detección de escaneos de la red de datos para saber todos los usuarios que están en la red, enfocada a encontrar las direcciones IP y los nombres de la red de datos de la U.A.P.

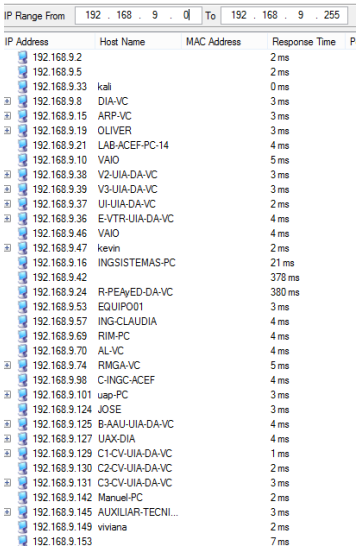


Figura 3.4: *Escaneo de la red.*
Fuente: *Escaneo con Ipscan.*

Ahora se hace el escaneo para la Determinación de puertos ya que conocemos en que red esta y cuál es el IP, Se ejecutó una prueba de seguridad con la herramienta Nmap a un sistema siringuero alias sin el firewall implementado con el IP 192.168.9.35:8080/siringuero, con el fin de revisar la información acerca de los puertos abiertos, lo cual se utilizó el sistema operativo Kali Linux ya que es un sistema operativo exclusivo para sacar vulnerabilidades y muchas otras cosas más contiene varias herramientas de escaneos.

Figura 3.5: *Sistema siringuero Alias.*
Fuente: *Elaboración propia.*

Escaneo en modo oculto activamos el comando –sS o -Pn para hacer un escaneo sin dejar huellas de la ip. Así pues, consiste en terminar la conexión antes de que el "diálogo" con el host destino esté completo.

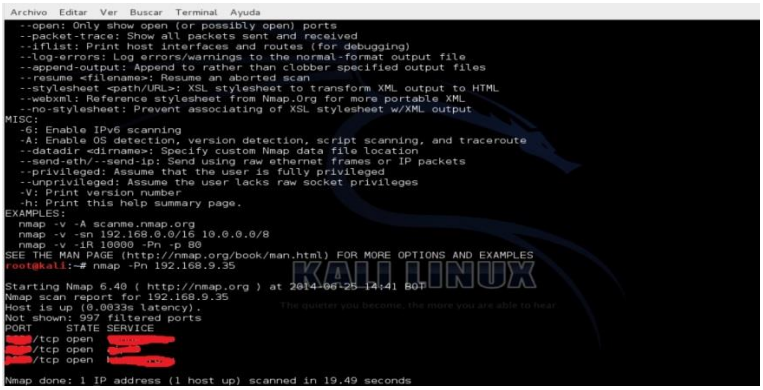


Figura 3.6: *imagen del* Rastreo de puertos abiertos con Nmap.
Fuente: *Recuperación de imagen del sistema Kali Linux.*

Escaneo de servicios de los puertos que están habilitados , este es uno de los pasos fundamentales para dar el salto al siguiente método , porque ya teniendo la información de cada uno de los servicios uno podría buscar en la base de bug o vulnerabilidad es de por ejemplo http://www.securityfocus.com/ y ya sabiendo esta información podría buscarse un exploit para "explotar" esta vulnerabilidad ofrecida por nuestro cliente el atributo para activar este tipo de escaneo es -sV

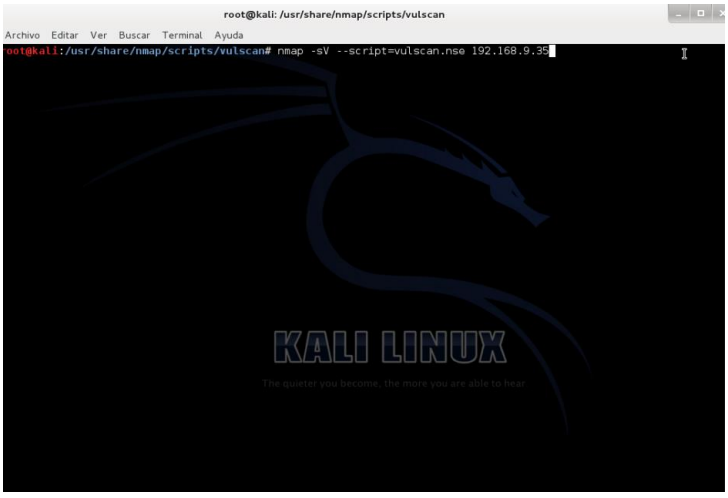


Figura 3.7: *imagen del comando para el escaneo con Nmap.*
Fuente: *Recuperación de imagen del sistema Kali Linux.*

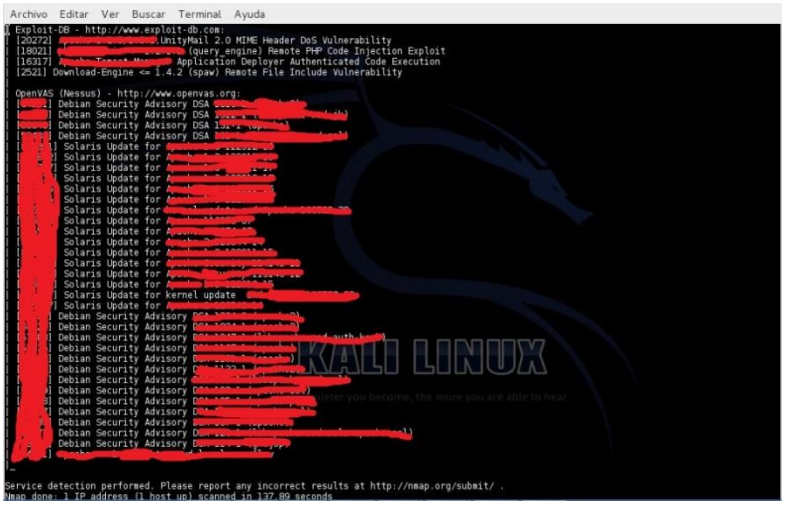


Figura 3.8: *imagen del* Rastreo de aplicaciones.
Fuente: *Recuperación de imagen del sistema Kali Linux.*

3.2. FASE DE ADMINSTRACION DE 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, El servidor de seguridad de la red de datos tiene módulos específicos en seguridad de red, en la que está dedicado a protección bajo Linux Endian firewall, la otra parte es el IDS que es de gran utilidad en la parte de filtrados por el cortafuegos también está integrado un antivirus agregado al Firewall, que nos sirve para realizar un filtrado más óptimo de virus.

3.2.1. 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 un motor de antivirus que filtra los contenidos y el control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

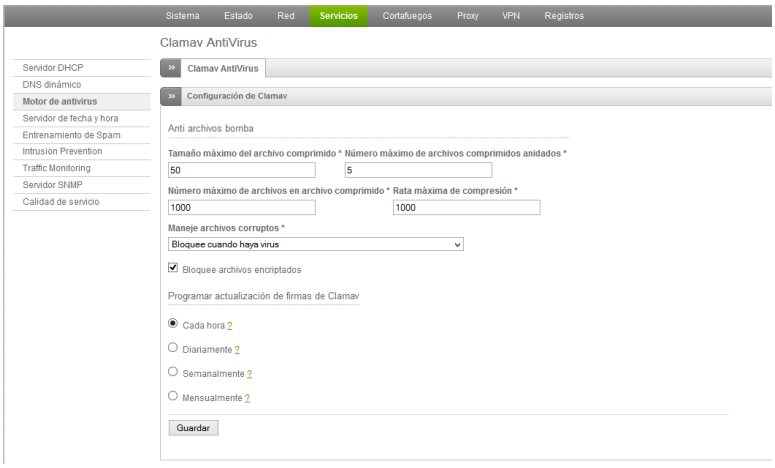


Figura 3.9: *Motor de antivirus.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

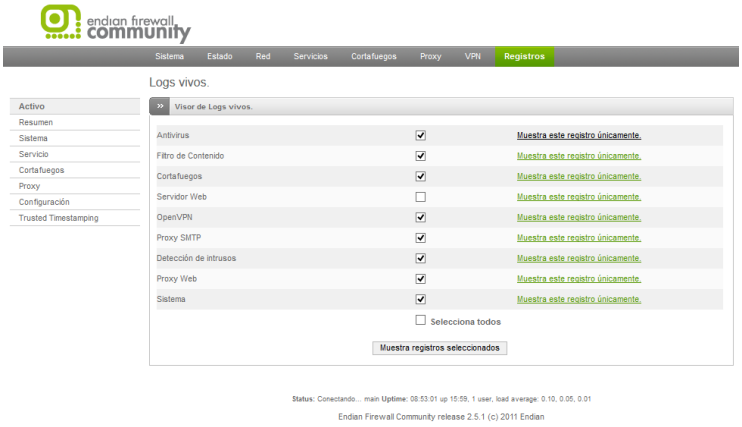


Figura 3.10: *Opción para ver Registros de Motor de antivirus.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

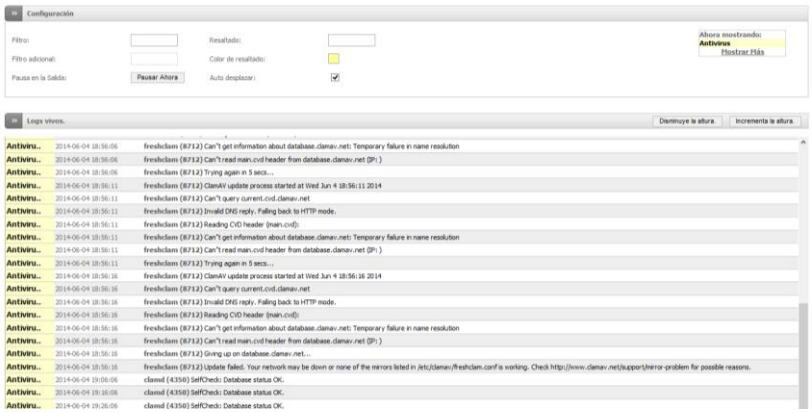


Figura 3.11: *registros de Motor de antivirus.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

3.2.2. Detección de intrusos

La detección de intrusos se puede lograr mediante un sistema de protocolos IDS-Firewall que vigila el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmas que indiquen el momento en que se detecte una situación anormal en la red como también bloquea los puertos débiles y limita herramientas peligrosas.

Figura 3.12: *Sistema de prevención de intrusos.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

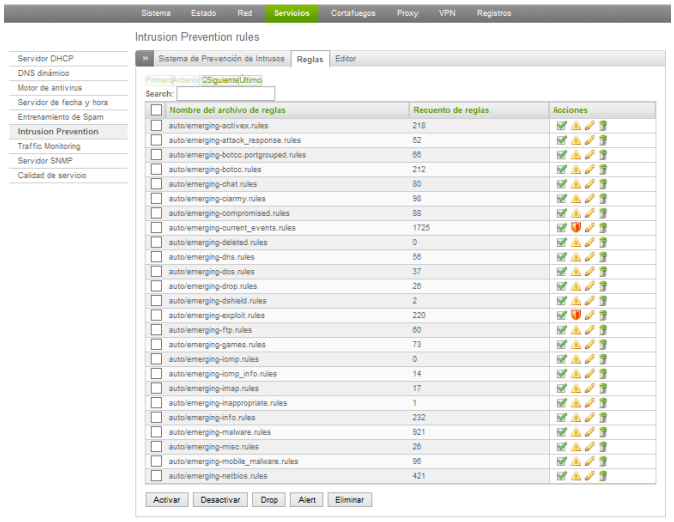


Figura 3.13: *Interfaz gráfica de reglas del IDS.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

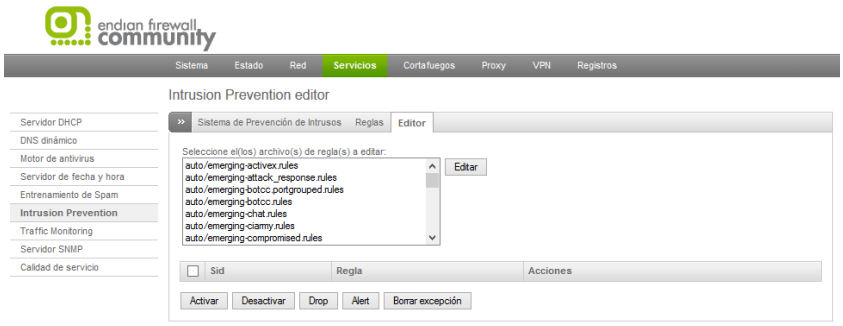


Figura 3.14: *Interfaz gráfica de editor de registros del IDS.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

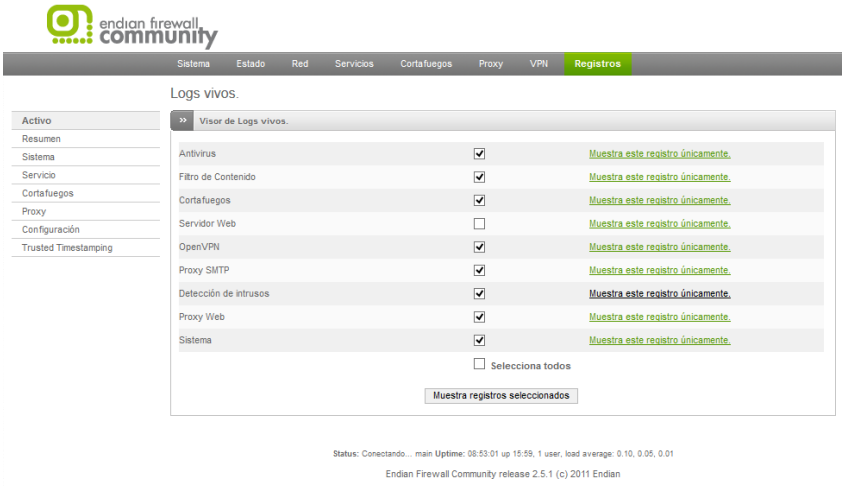


Figura 3.15: *Interfaz gráfica del IDS-Firewall.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

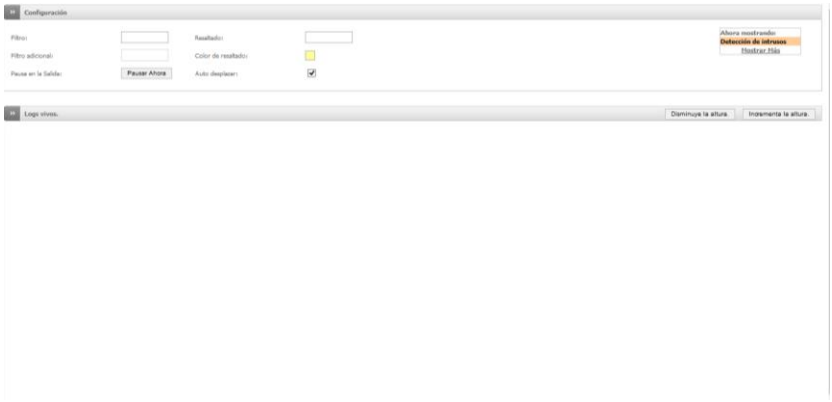


Figura 3.16: *Interfaz gráfica de Registro de IDS-Firewall.*
Fuente: *recuperación de imagen del menú de Firewall ENDIAN.*

3.2.3. 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, para este caso se creó un formulario para la forma de manejo de incidentes. **(VER ANEXO B).**

3.2.4. 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. Es por eso que se creó las políticas después de haber hecho un análisis profundo de las necesidades en la Unidad de Sistemas Académicos para la seguridad de la red de datos del sistema siringuero de la U.A.P.

Las políticas de seguridad de sistemas de información son:

- **POLITICA 1: ACCESO A LA INFORMACIÓN**
- **POLITICA 2: ADMINISTRACION DE CAMBIOS**
- **POLITICA 3: SEGURIDAD DE LA INFORMACION**
- **POLITICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS**
- **POLITICA 5: SEGURIDAD EN RECURSOS INFORMATICOS**
- POLITICA 6: SEGURIDAD EN COMUNICACIONES
- **POLITICA 7: SEGURIDAD PARA USUARIOS TERCEROS**

Las políticas de seguridad de sistemas de información completa ver **(VER ANEXO C).**

3.2.5. 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.

Figura 3.17: *Capas del modelo OSI.*
Fuente: *Elaboración propia.*

La seguridad informática se resume, por lo general, en cinco objetivos principales:

f) **Confidencialidad.-** La confidencialidad consiste en hacer que la información sea incomprensible para aquellos individuos que no estén involucrados en la operación.
g) **Integridad.-** La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).
h) **Control de acceso.-** Impide el acceso a la información a aquellas personas o procesos no autorizados.
i) **No repudio.-** Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

j) **Autenticación.-** La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

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

SERVICIO DE SEGURIDAD.	CAPA						
	1.Fisica	2.Enlace	3.Red	4.Transporte	5.Sesion	6.Presentación	7.Aplicación
Autenticación							
Control de acceso							
Confidencialidad							
Integridad							
No repudio							

Figura 3.18: *Tabla de servicios de seguridad con la capa OSI.*
Fuente: *Elaboración propia.*

3.2.6. Mecanismos de seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. La herramienta que se está usando es: herramientas de control de acceso, cortafuegos ENDIAN (firewall).

Esta herramienta Open-Source la cual nos permite mejorar la distribución de nuestra red implementando zonas (WAN, LAN y DMZ). Este paquete incluye un firewall dinámico para asegurar nuestra red, detección de intrusos, escaneo de puertos, etc. Algunas de las características de Endian es la distribución de la carga de datos, el manejo de proxy, el servicio de antivirus, filtrado de contenido, enrutamiento y alta disponibilidad.

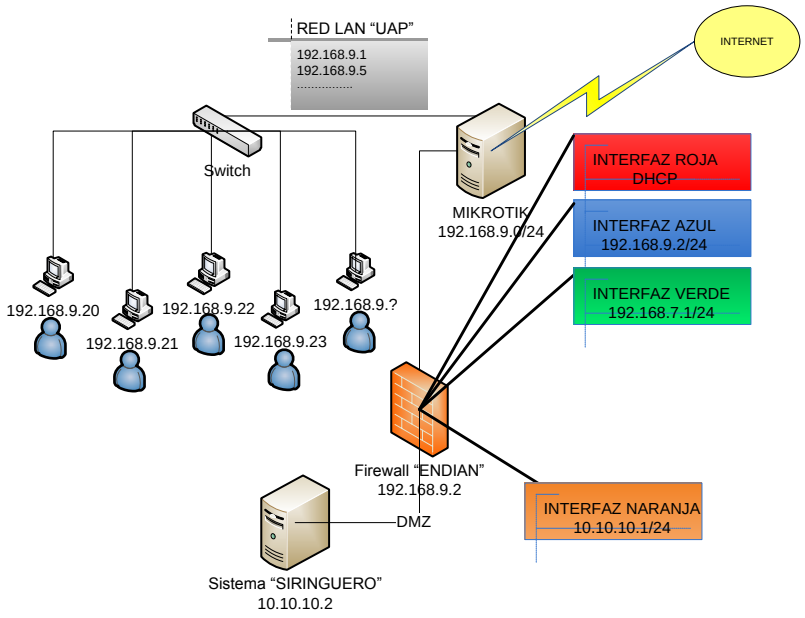


Figura 3.19: *Esquema de red.*
Fuente: *Elaboración propia.*

Todos estos elementos en su conjunto conforman el modelo de seguridad de la red datos del sistema siringuero de la U.A.P.

3.2.7. 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.
- 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 de datos del sistema siringuero de la U.A.P.

En este caso utilizaremos el Endian firewall Community, veremos como instalarlo y configurarlo Endian Firewall Community 2.5.1 Esta es una herramienta OpenSource, desarrollada para el funcionamiento de un cortafuegos (firewall), gestionar amenazas, servicios de VPN y PROXY,etc.

Endian está basado originalmente en Ipcop.

La instalación de Endian Firewall a través de CD de arranque es simple con particionamiento automático, lo que resulta en un sistema con una interfaz Web con la opción de varios idiomas. **(VER ANEXO D).**

Figura 3.20: *Imagen de Endian Firewall Community 2.5.1.*
Fuente: *De la página oficial de Endian.*

El Endian Firewall es una distribución Linux firewall que se especializa en firewall tiene una interfaz de gestión web, añadiendo distintos programas informáticos libre en un paquete integrado de implementación y configuración rápida. **(VER ANEXO E).**

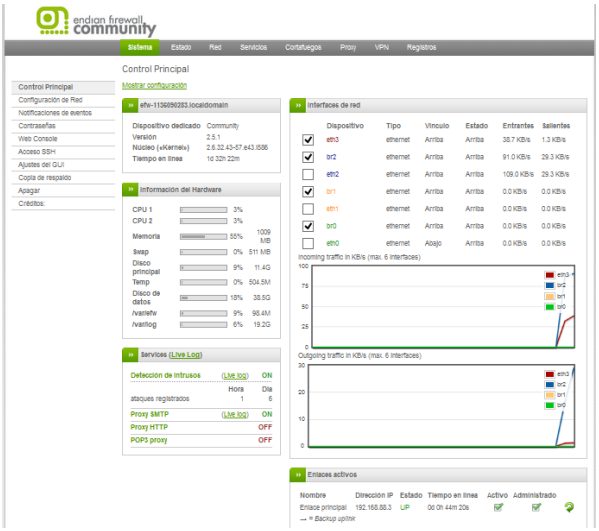


Figura 3.21: *Imagen de la pantalla principal del Firewall configurado.*
Fuente: *Recuperación de imagen de Endian Firewall 2.5.1.*

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

Como conclusión del presente proyecto, Es La implementación de un Firewall como Endian, permitió que el control de todo el tráfico de la red de datos sea administrado, lo que le quita carga de trabajo a la plataforma mejorando su desempeño al sistema siringuero.

La importancia de investigar adecuadamente sobre una herramienta de software libre como el firewall, conocer su funcionamiento, ventajas, desventajas…. es una manera fácil de saber que herramienta utilizar a la hora de solucionar problemas de filtrado de paquetes para la seguridad de red de datos.

El implementar herramientas bajo licenciamiento libre, es una de las mejores opciones que tienen los administradores a la hora de escoger un producto e implementarlo en su red local o externa.

Reconocimos la ventaja de trabajar con herramientas de entorno grafico para tareas complejas como son la de crear reglas de filtrado.

Se aprendió a diferenciar diferentes clases de herramientas de Firewall, con el fin de tener más opciones de implementación a la hora de resolver un problema.

Obtenidos los conocimientos, es hora de ponerlos en práctica.

Este servidor se implementó de acuerdo al cronograma presentado en el perfil, y se basó bajo las etapas de la metodología funcional, tomando en cuenta que se inició la fase de funcionamiento hace 3 meses atrás, en la que fue de gran utilidad y se corrigió algunos percances en el proceso de uso.

4.2 RECOMENDACIONES

Recomendamos el presente proyecto, como para tomar en cuenta los siguientes puntos, para poder estructurarlos a corto plazo y a largo plazo, planteando como temas de otras investigaciones:

- Implementar un mayor ancho de banda, para una mejor actualización diaria de los servicios como el antivirus y reglas del IDS del servidor de seguridad de la red de datos, realizar una restructuración de la red de datos del Vicerrectorado para que así no tener molestias de conexiones con los usuarios como también para conexiones a otros predios de la U.A.P.
- Comprar un servidor específico de característica mejorada y de más capacidad, para habilitar la mayoría de los servicios de seguridad de la red datos, ya que el que tenemos es de características regulares.
- Implementar más servicios de seguridad para la red de datos más específicos, Para así tener un completo control de toda la red de datos del sistema siringuero.
- La solución aquí documentada fue implementada exitosamente, por lo que es recomendable es posible la implementación en cualquier institución pública y privada que tenga una red de datos conectados a un sistema de información, tanto como, herramienta de uso de los funcionarios.

BIBLIOGRAFÍA

- González Dumrauf (2002, 13 de Mayo) Administración De Redes.
  Extraído 13 de Agosto 2010 desde:
  www.chaco.gov.ar/UTN/AdmRedes/Traduccion/cap1.doc
- Gabriel Verdejo Álvarez (2003, septiembre) Seguridad en Redes IP.
  Extraído 25 de Abril 2010 desde:
  http://archivos.abcdatos.com/tutoriales/O/O149/O149.zip
- White Paper (2002) Las redes IP: Conceptos básicos
  Extraído 14 de agosto 2010 desde:
  http://www.casadomo.com/redirLink.aspx?url=images%5Carchivos%5Caxis_las_redes_ip.pdf&src=/profesionalesDetalle.aspx
- Sergio Untiveros, (2004, Julio) Metodología Funcional para la administración de redes.
  Extraído el 11 de Agosto 2010 desde:
  www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf
- Free Software Foundation, la definición de software libre. Boston. 2007. Disponible en: http://www.gnu.org/philosophy/free-sw.html. Consultado el: 01 de mayo 2010.
- REAL ACADEMIA ESPAÑOLA (2003) Diccionario de la Real Academia Española. 22.ª EDICIÓN,
- RUBINI, ALESSANDRO; 2001; Linux Device Drivers, 2nd Edition; O'Relly. ISBN: 0-59600-008-1.
- XIOMAR DEGADO, ROJAS, EUNED, (1998), Auditoria Informatica.
- ACISSI, (2011), Seguridad informática: ethical hacking: conocer el ataque para una mejor defesa, ISBN, 2746068117, 9782746068117.
- FRASCONE, DAVID; *Mayo 2002 LinuxJournal;* Debugging Kernel Modules with User Mode.
- INSOLVIBLE, GIANLUCA; *Febrero 2002 LinuxJournal*; Inside the Linux Packet Filter.

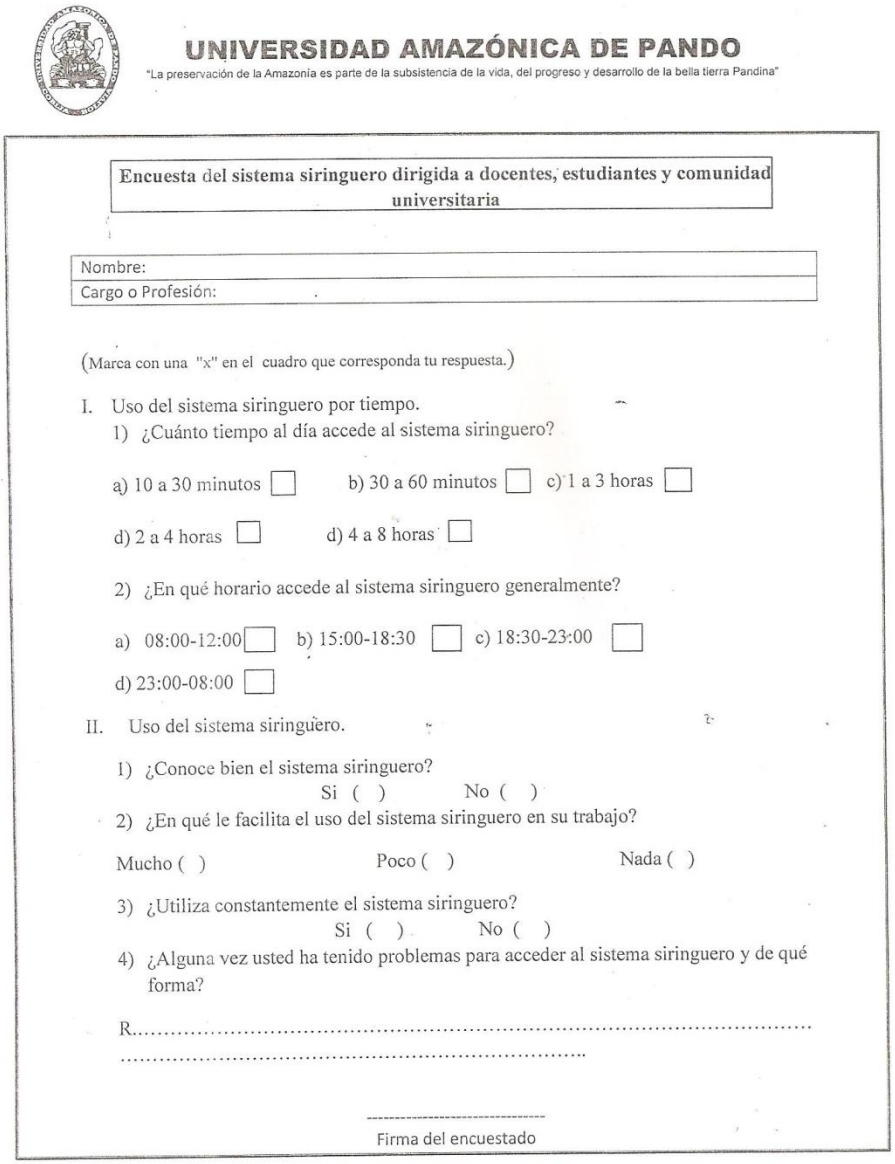
- INSOLVIBLE, GIANLUCA; *Junio 2001 LinuxJournal*; The Linux Socket Filter: Sniffing Bytes over the Network.
- RUSSELL, PAUL; Unreliable Guide to Hacking The Linux Kernel; *http://www.netfilter.org/unreliable-guides/.*
- RUSSELL, PAUL; Linux 2.4 Packet Filtering HOWTO; *http://www.netfilter.org/unreliable-guides/.*
- Unificado de Modelado. Manual de Referencia; Addison Wesley Ed. 2000. ISBN: 84-7829-037-0.
- VASUDEVAN, ALAVOOR; CVS-RCS-HOWTO Document for Linux; *http://www.tldp.org/HOWTO/CVS-RCS-HOWTO.html.*
- WRIGHT, GARY R.; STEVENS, W. RICHARD; TCP/IP Illustrated, Volume 1 The Protocols; Addison Wesley Ed.; 1994. ISBN: 0-201-63346-9.i.
- WRIGHT, GARY R.; STEVENS, W. RICHARD; TCP/IP Illustrated, Volume 2 The Implementation; Addison Wesley Ed.; 1995. ISBN: 0-201-63354-X.

Anexos

Anexo A

ANEXOS A

DESCRIPCIÓN DEL DIAGNOSTICO Y ANÁLISIS REALIZADO EN BASE A ENCUESTA Y OBSERVACIÓN



UNIVERSIDAD AMAZÓNICA DE PANDO

"La preservación de la Amazonía es parte de la subsistencia de la vida, del progreso y desarrollo de la bella tierra Pandina"

Encuesta del sistema siringuero dirigida a docentes, estudiantes y comunidad universitaria

Nombre:

Cargo o Profesión:

(Marca con una "x" en el cuadro que corresponda tu respuesta.)

I. Uso del sistema siringuero por tiempo.

1) ¿Cuánto tiempo al día accede al sistema siringuero?

a) 10 a 30 minutos ☐ b) 30 a 60 minutos ☐ c) 1 a 3 horas ☐

d) 2 a 4 horas ☐ d) 4 a 8 horas ☐

2) ¿En qué horario accede al sistema siringuero generalmente?

a) 08:00-12:00 ☐ b) 15:00-18:30 ☐ c) 18:30-23:00 ☐

d) 23:00-08:00 ☐

II. Uso del sistema siringuero.

1) ¿Conoce bien el sistema siringuero?

Si ( ) No ( )

2) ¿En qué le facilita el uso del sistema siringuero en su trabajo?

Mucho ( ) Poco ( ) Nada ( )

3) ¿Utiliza constantemente el sistema siringuero?

Si ( ) No ( )

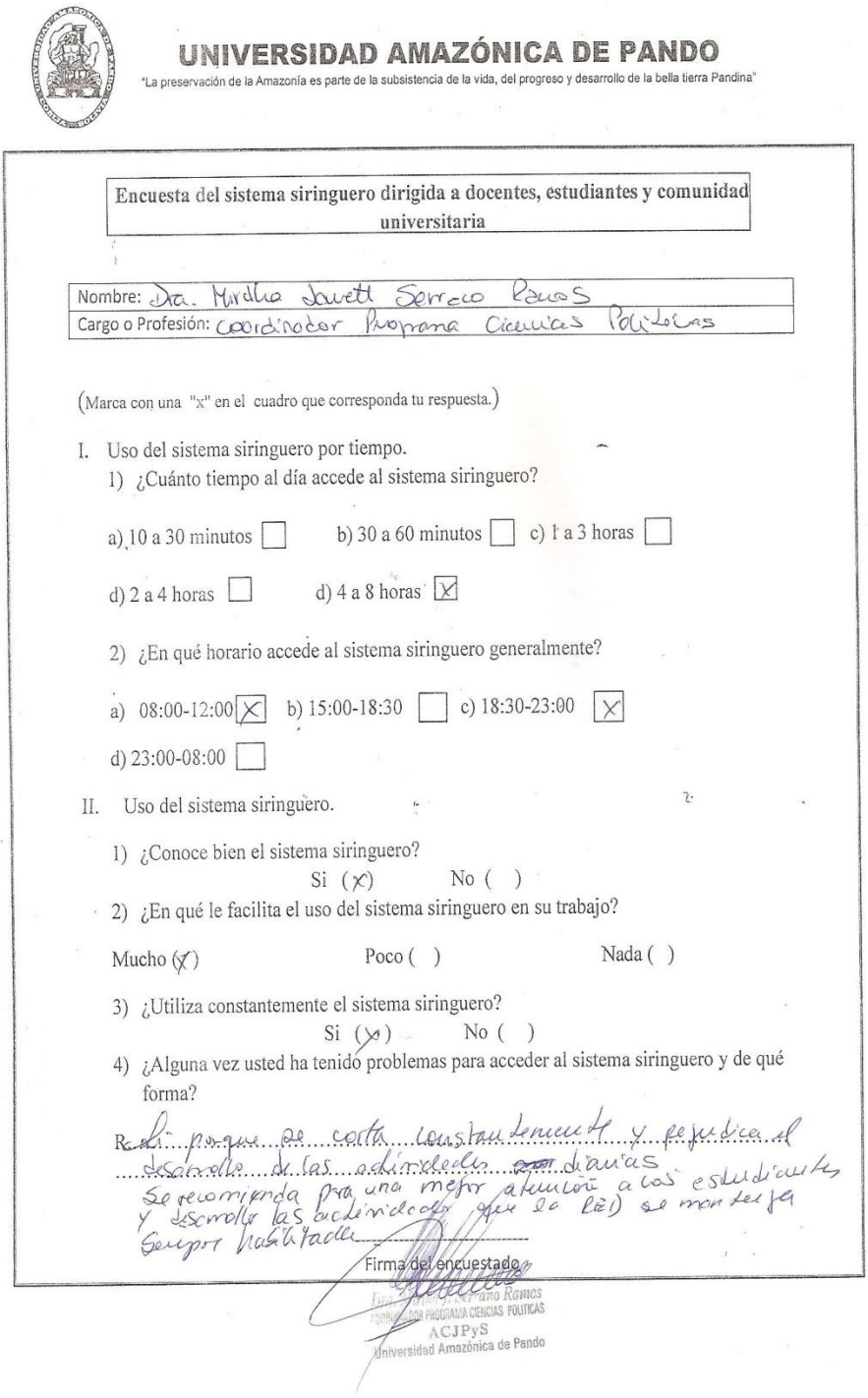
4) ¿Alguna vez usted ha tenido problemas para acceder al sistema siringuero y de qué forma?

R.....

.....

Firma del encuestado

Figura 1: *Formato de la encuesta elaborada*
Fuente: *Elaboración Propia*



UNIVERSIDAD AMAZÓNICA DE PANDO

"La preservación de la Amazonía es parte de la subsistencia de la vida, del progreso y desarrollo de la bella tierra Pandina"

Encuesta del sistema siringuero dirigida a docentes, estudiantes y comunidad universitaria

Nombre: Dra. Martha Lovett Serrano Ramos

Cargo o Profesión: Coordinador Programa Ciencias Políticas

(Marca con una "x" en el cuadro que corresponda tu respuesta.)

I. Uso del sistema siringuero por tiempo.

1) ¿Cuánto tiempo al día accede al sistema siringuero?

a) 10 a 30 minutos [ ] b) 30 a 60 minutos [ ] c) 1 a 3 horas [ ]

d) 2 a 4 horas [ ] d) 4 a 8 horas [X]

2) ¿En qué horario accede al sistema siringuero generalmente?

a) 08:00-12:00 [X] b) 15:00-18:30 [ ] c) 18:30-23:00 [X]

d) 23:00-08:00 [ ]

II. Uso del sistema siringuero.

1) ¿Conoce bien el sistema siringuero?

Si (X) No ( )

2) ¿En qué le facilita el uso del sistema siringuero en su trabajo?

Mucho (X) Poco ( ) Nada ( )

3) ¿Utiliza constantemente el sistema siringuero?

Si (X) No ( )

4) ¿Alguna vez usted ha tenido problemas para acceder al sistema siringuero y de qué forma?

Si porque se corta constantemente y perjudica el desarrollo de las actividades diarias

Se recomienda para una mejor atención a los estudiantes y desarrollo las actividades que se han) se mantenga siempre habilitada

Firma del encuestado

ACJPyS
Universidad Amazónica de Pando

Figura 2: *Encuesta Llenada Nº 25*
Fuente: *Elaboración Propia*

ESTADISTICAS DEL USO DEL SISTEMA SIRINGUERO

1. ¿Cuánto tiempo al día accede al sistema siringuero??

A) 10-30min	**7**
B) 30-60min	**3**
C) 1-3hrs.	**2**
D) 2-4hrs.	**2**
E)4-8hrs	**8**

2. ¿En que horario accede al sistema siringuero?

08:00-12:00	**19**
15:00-18:30	**14**
18:30-23:00	**1**
23:00-08:00	**0**

3. ¿conoce bien el sistema siringuero?

SI	**14**
NO	**8**

4. ¿En qué le facilita el uso del sistema siringuero en su trabajo?

Mucho	**17**
Poco	**3**
Nada	**2**

5. ¿Utiliza constantemente el sistema siringuero?

SI	**15**
NO	**7**

6. ¿Alguna vez usted ha tenido problemas para acceder al sistema siringuero y de qué forma?

LA RED	**13**
TARJETA MAGNETICA.	**2**
LO APAGAN EL SIRINGUERO	**2**
SISTEMA	**1**
NADA	**4**

Numero de Encuestas Realizadas

TOTAL DE PERSONAS QUE ACCEDEN AL DIA AL SIRINGUERO	***93***	***100%***
TOTAL DE PERSONAS ENCUESTADAS	***22***	***52%***

Figura 3: *Tabla de resultado cuantitativo de encuestas realizadas*
Fuente: *Elaboración Propia*

RESULTADOS DE LA ENCUESTA SOBRE EL USO DEL SIRINGUERO DE LA UNIVERSIDAD AMAZONICA DE PANDO

Pregunta 1: Cuanto tiempo al día accede al sistema siringuero?

Ya que la pregunta fue directa a todas las personas que acceden al siringuero, según la encuesta el mayor promedio de acceso diario por persona al sistema siringuero es 4:8 hrs. Diarios.

Figura 4: *Torta grafica de pregunta 1*

Fuente: *Elaboración Propia*

Pregunta 2: En que horario accede al sistema siringuero?

El 56% de las personas dijeron que acceden en la mañana, pero 41% dijeron que acceden en las tardes. En síntesis el acceso de la mayoría de los usuarios al siringuero lo hacen en horarios de oficinas.

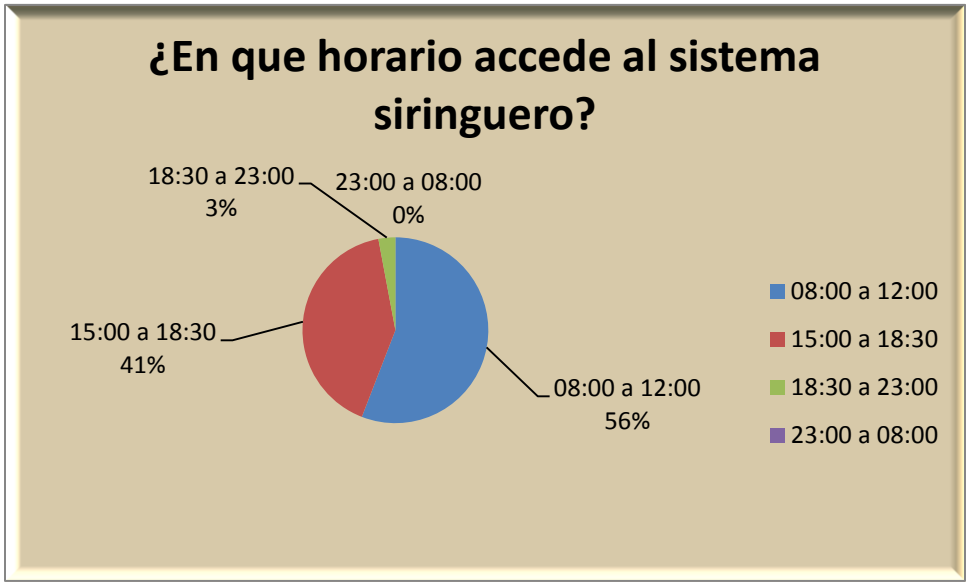


Figura 5: *Torta grafica de pregunta 2*
Fuente: *Elaboración Propia*

Pregunta 3: Conoce bien el sistema siringuero?

El 64% respondió que sí conoce el sistema siringuero y el 36% que no conoce.

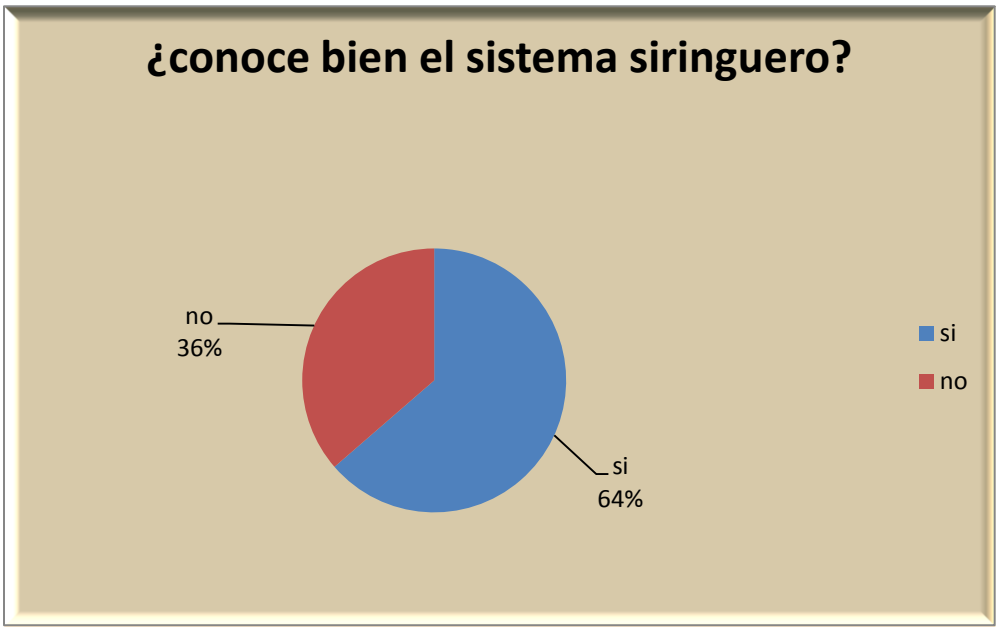


Figura 6: *Torta grafica de pregunta 3*

Fuente: *Elaboración Propia*

Pregunta 4: En que le facilita el uso del sistema siringuero en su trabajo?

La mayoría de los Usuarias en un 77% respondió que si le facilita mucho en su labor cotidiana y que es muy importante el sistema siringuero, 14% respondieron que muy poco le ayuda. El 9% que no les ayuda en nada, por lo que se observa que el sistema siringuero de la Universidad Amazónica de Pando es muy importante.

Figura 7: *Torta grafica de pregunta 4*

Fuente: *Elaboración Propia*

Pregunta 5: Utiliza constantemente el sistema siringuero?

Un 68% respondió que si utiliza constantemente, pero 32% que no.

Figura 8: *Torta grafica de pregunta 5*

Fuente: *Elaboración Propia*

Pregunta 6: Alguna vez usted ha tenido problemas para acceder al sistema siringuero y de qué forma?

En esta encuesta se tomó en cuenta a las respuestas más repetidas ya que es una pregunta abierta, en la que 59% respondió que el su problema que tuvo fue por la conexión de red, pero 18% que no tuvo ningún tipo de problema.

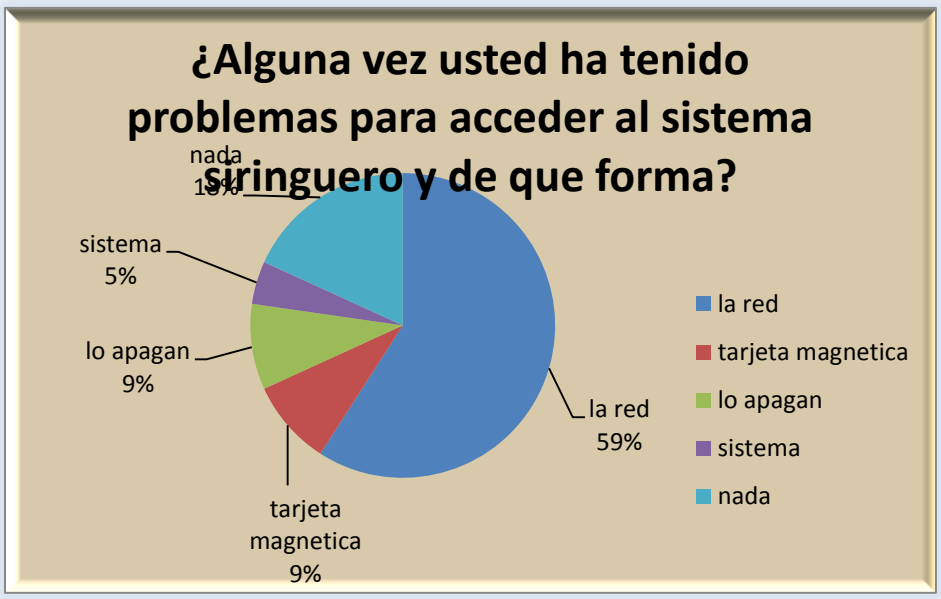


Figura 8: *Torta grafica de pregunta 5*

Fuente: *Elaboración Propia*

Anexo B

ANEXOS B

FORMULARIO DE FORMAS DE MANEJO DE INCIDENTES

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 C

ANEXOS C

POLITICAS DE SEGURIDAD DE SISTEMAS DE INFORMACION

UNIVERSIDAD AMAZÓNICA DE PANDO

VICE-RECTORADO

Unidad de Sistemas Académicos

“POLITICAS DE SEGURIDAD DE SISTEMAS DE INFORMACION”

Autor: David Calliconde Montero

Tutor: Ing. Freddy Morales Blanco

Cobija, Julio de 2014

Pando – Bolivia

2014

INDICE DE CONTENIDO

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCION

El propósito de establecer este Plan de Seguridad de Sistemas de Información en la Universidad Amazónica de Pando, es proteger la información y los activos de la organización, 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, de tal forma que permitan a la U.A.P. cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso de esta institución, 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, por que los servidores con los que cuenta la U.A.P. Son de vital importancia y contienen información confidencial para toma de decisiones academias 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 dichas instalaciones, de la misma manera son de vital importancia proteger contra accesos externos no autorizados, ya que se suministran notas de calificaciones academias 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 criticas 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 últimos

meses 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 la implementación del presente Plan de Seguridad de Sistemas de Información para la Universidad Amazónica de Pando en donde se definen los lineamientos con el fin de establecer una cultura de la seguridad en la Universidad Amazónica de Pando. Asimismo establece los requisitos a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por este plan

ALCANCE DE LAS POLÍTICAS

Las políticas definidas del presente documento se aplicara para todos los funcionarios, administrativos, docentes, estudiantes y trabajos dirigidos de la Unidad de Sistemas de Información Académica, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos del Sistema SIRINGUERO.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

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

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.

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.

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

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

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.

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.

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".

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

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.

DESCRIPCIÓN DE LAS POLITICAS

POLITICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios administrativos, docentes, estudiantes y trabajos dirigidos que laboran para el U.A.P. 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 Secretaria General, Subdirectores, jefes de unidades y responsable de Unidad de Sistemas de Información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la Universidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad

Docentes y Estudiantes solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

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.
Mediante el registro de eventos en los diversos recursos informáticos de la Unidad de Sistemas de Información Académica se efectuará un seguimiento a los accesos realizados por los usuarios al Sistema 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 se deberán documentar y realizar las acciones tendientes a su solución, así mismo se registrará los IP's de los usuarios con los cuales acceden al sistema.

POLITICA 2: ADMINISTRACION DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte el sistema Siringuero, debe ser requerido por los usuarios del Sistema Siringuero 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 de los accesos tendrá la facultad de aceptar o rechazar la solicitud.
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, modificación o mejoras solicitado en base al procedimiento y formato aprobado.

Cualquier tipo de cambio en el sistema 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 a un recurso informático de la Unidad de Sistemas de Información Académica 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, por la Ley para protegerla y evitar pérdidas, 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 Siringuero a entes externos sin las autorizaciones respectivas del Vicerrectorado o Rectorado.

Todo funcionario que utilice el Sistema 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 deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Universidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez cumplida su contrato y/o cesado su cargo, deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la U.A.P., 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 (Rector y Vicerrector).

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

El sistema de correo electrónico, sms, grupos de charla y utilidades asociadas de la Universidad Amazónica de Pando debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratados, docentes y estudiantes.

La U.A.P juntamente con la Unidad de Sistemas de Información Académica. se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema, correo electrónico para cualquier propósito. Para este efecto, el funcionario, docentes y estudiantes autorizará a la U.A.P. para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

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 ó 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 fuentes, 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 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 Universidad Amazónica de Pando.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la USIC, 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 e 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 Siringuero y otros recursos informáticos y sistemas de informatizados. 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 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. También deben permitir que un rol de usuario administre el Administración de sistemas.

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

Las puertas traseras: Las puertas traseras son entradas no convencionales al sistema 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 Siringuero y otros sistemas informatizados de la Universidad 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 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 es

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

El nivel de súper usuario del sistemas 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.

Toda la información del servidor del Sistema 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’s internas, topologías, configuraciones e información relacionada con

el diseño de los sistemas de comunicación, seguridad y cómputo de la Universidad Amazónica de Pando, 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 Universidad, 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.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

Los computadores de la U.A.P. 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 a demás previa autorización del personal de seguridad informática y/o la Unidad de Sistemas de Información Académica.

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

Los dueños de los Recursos Informáticos que no sean propiedad de la U.A.P. y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente deben definir un documento de acuerdo y su uso oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de la U.A.P. para el funcionamiento de recursos que no sean propios de la U.A.P. y que deban ubicarse en sus instalaciones, los recursos serán administrados por los personeros del Sistema de Información Académica o del Área técnica de la U.A.P.

Los usuarios terceros tendrán acceso al Sistema 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 deberán firmar el acuerdo de buen uso de los mismos.
Si se requiere un equipo con módem, este equipo no podrá en ningún momento estar conectado a la Red al mismo tiempo.
La conexión entre sistemas internos de la U.A.P. y otros de terceros debe ser aprobada y certificada por el personal de Seguridad Informática y/o Unidad de Sistemas de Información Académica con el fin de no comprometer la seguridad de la información interna de la U.A.P.
Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la U.A.P. aprobado por las instancias superiores.
Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la Universidad Amazónica de Pando. La U.A.P. se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La U.A.P. se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la Universidad.

POLITICA 8: SOFTWARE UTILIZADO

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 de Información Académica o reglamentos internos de la U.A.P.
Todo el software y/o sistemas de manejo de datos que utilice la U.A.P. dentro de las Unidades de Sistemas de Información ya se 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 Universidad que garantice el conocimiento por parte de los funcionarios administrativos, docentes, estudiantes y personas de apoyo de las implicaciones que tiene el instalar software ilegal en los computadores de la U.A.P.

Existirá un inventario de las licencias de software de usos oficial de la U.A.P. 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.A.P.

POLITICA 9: ACTUALIZACION DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos Servidores del Sistema Siringuero y otros equipos de computo ubicado dentro y fuera de la Unidad de Sistemas de Información Académica de la U.A.P. (cambios de procesador, adición de memoria o tarjetas, etc.) debe tener previamente una evaluación técnica y autorización de la misma Unidad y/o USIC.
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, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador de la Unidad de Sistemas de Información

POLITICA 10: ALMACENAMIENTO Y RESPALDO

La información que es soportada por el Sistema Siringuero y otros sistemas de información de la U.A.P. deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.
Debe existir una definición formal de las estrategias de generación, retención y rotación de las copias de respaldo.
La U.A.P. definirá la custodia de los respaldos del Sistema Siringuero y otros sistemas de información 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 U.A.P., esto de acuerdo con la importancia de la información para el funcionamiento correcto y la operación de la U.A.P.

La Unidad de Sistemas de Información Académica en conjunto con los administradores de los sistemas definirán las estrategias a seguir para el respaldo de la información.
Los funcionarios administrativos, docentes, estudiantes y personal de apoyo son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas por la USIC. Y ésta será la autorizada para realizar el seguimiento y control de esta política.

POLITICA 11: CONTINGENCIA

El administrador del sistema Siringuero. conjuntamente con la U.A.P. debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita al sistema Siringuero, aplicaciones y comunicación consideradas como críticas o valiosas estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

POLITCA 12: AUDITORIA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la UAP, como son sistema Siringuero, otros sistemas de información, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.
Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.
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 previa autorización de la autoridad competente de la suministración y/o administración y custodia.
Todos los computadores de la Universidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

POLITICA 13: SEGURIDAD FISICA

La U.A.P. deberá contar con los mecanismos de control de acceso hacia los servidores del Sistema Siringuero, sistemas de base de datos, y otras aplicaciones tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la Universidad considere críticas.

Las instalaciones donde se alojen los equipos servidores, equipos de computo, 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 computo.

Los visitantes hacia las Unidades de Sistemas de Información Académica 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 al área restringida y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo administrativos, antiguos empleados, docentes, miembros de la familia del trabajador, personal de apoyo, etc. Siempre que un personal de la U.A.P. se dé cuenta que un visitante no escoltado se encuentra dentro de la Unidad de Sistemas de Información Académica de la Universidad, 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 jefe de la Unidad de Sistemas, y esta situación debe ser documentada para posteriores percances.

La Unidad de Sistemas de Información Académica y administrativa y centros de cómputo o áreas que la U.A.P. considere criticas, las cintotecas deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal de la Unidad que labora cotidianamente en estos lugares.

Toda persona que se encuentre dentro de la Universidad deberá portar su identificación en lugar visible.

En las Unidades de Sistemas de la U.A.P. o áreas que se considere críticas deberán estar equipadas con elementos de control de incendio, inundación y alarmas.

Las Unidades de Sistemas o áreas que la U.A.P. 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.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar las instalaciones de la Universidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la Unidad de Sistemas e informática.

Todas las personas externas y/o funcionarios de la U.A.P. visitantes a las Oficinas de Sistemas de Información Académica 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 la Universidad.

Los equipos de microcomputadores (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa, de los personeros de Sistemas de Información Académica y/o USIC.

Los funcionarios de la U.A.P. administrativos, docentes, estudiantes y personal de apoyo se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de computo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipos que generen caídas de la energía.

Los particulares en general, entre ellos, los familiares de los funcionarios de la U.A.P., no están autorizados para utilizar los recursos informáticos de la Universidad.

POLITICA 14: ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, USB memoria key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

POLITICA 15: ADMINISTRACION DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los sistemas de información y los Recursos Informáticos se debe ejecutar al menos una vez cada dos años. 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 a los responsables de la Unidad de Sistemas de Información Académica y/o USIC. O personal 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 de Información Académica y personal de seguridad informática.

El personal 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 Sistemas

Anexo D

ANEXOS D

INSTALACIONES DEL SOFTWARE, EN BASE A CAPTURAS DE PANTALLA.

Descarga de la .iso de la versión 2.5.1 da la web (www.endian.com)

Descargar de la .iso de ENDIAN:

Como sistema base usaremos un sistema Linux compacto que ya nos trae instalado todo lo que necesitamos. Este sistema es funcional por sí mismo, en el momento de instalarlo y configurarlo ya tendremos el 60 % de nuestro sistema operativo.

Para obtenerlo es bastante con acceder a la web y bajarnos la versión que deseemos.
Actualmente tenemos disponible hasta la 3.0 aunque para instalarla usaremos la 2.5.1 que es la más estándar para instalar y después actualizaremos algunas aplicaciones.

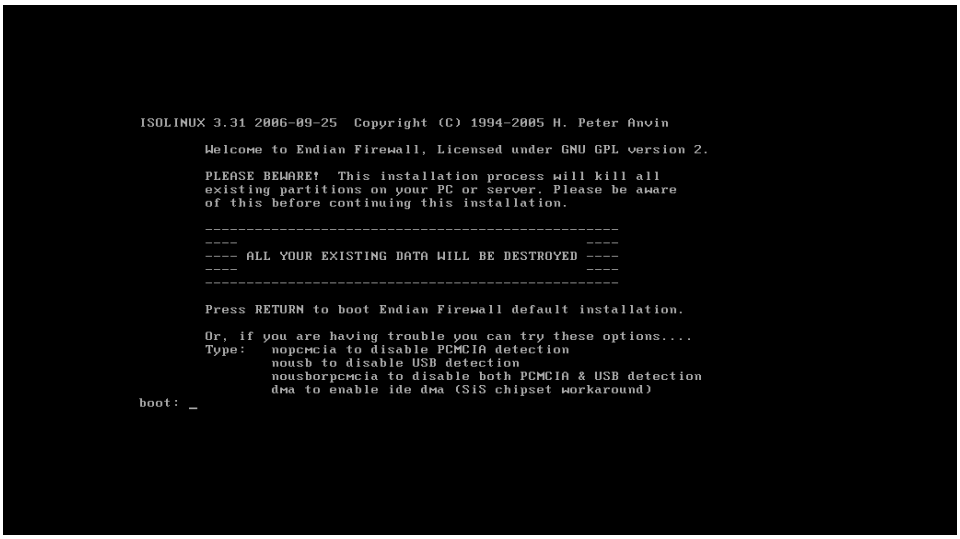
Nos descargaremos la ISO desde la web de ENDIAN (www.endian.com) y la grabaremos en un CD para comenzar la instalación.

Iniciar desde CD:

Pantalla del Boot Menú poco después de iniciar.

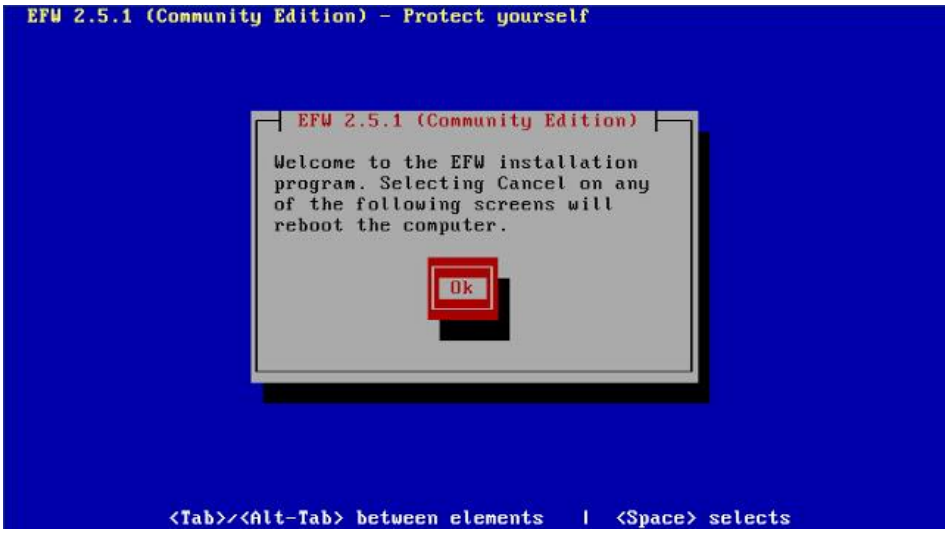
- El Tiempo es de 15 segundos. Si no selecciona una opción el instalador ingresará de manera automática a la primera opción.

Lo primero que veremos al arrancar el equipo es esta pantalla:

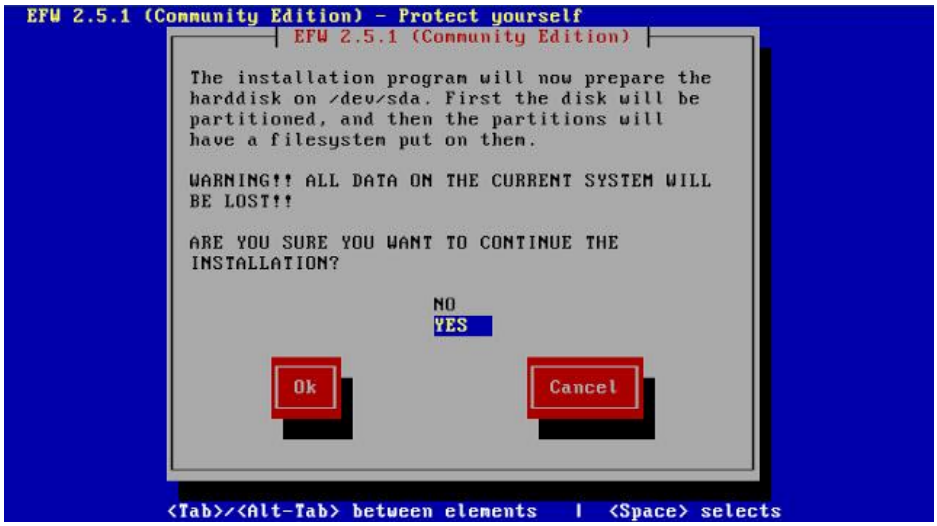


Tras pulsar “Enter” nos pedirá el idioma:

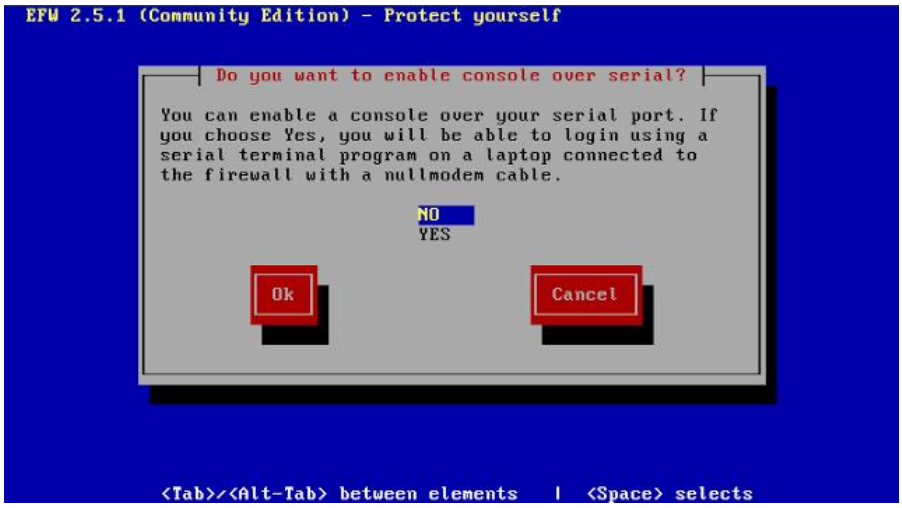
En esta pantalla debe seleccionar el idioma de la instalación Endian.



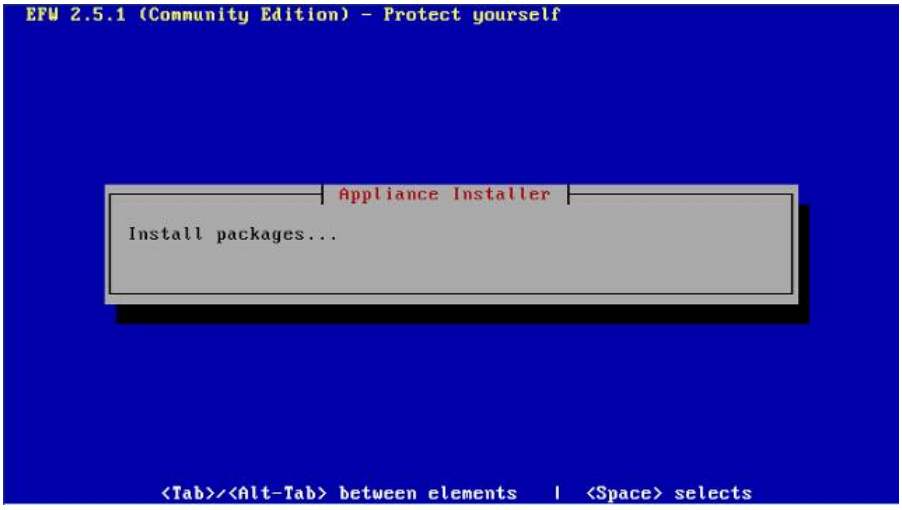
Pantalla de bienvenida... <Entrar> para continuar.



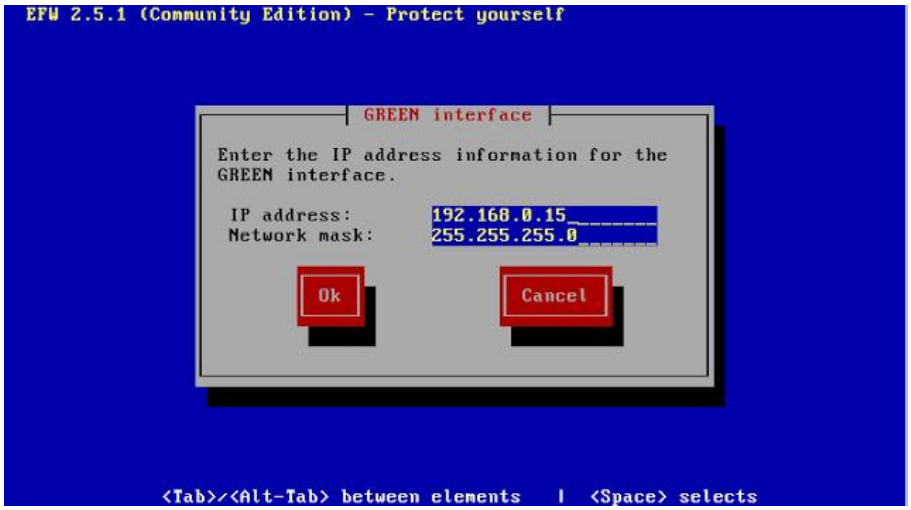
Se trata de una pantalla de advertencia. Se informa que se perderán todos los datos contenidos en la computadora de alta definición. Si marca la opción "NO", que saldrá de la instalación. Si marca "SÍ" se va a proceder con la instalación. Marque "Sí" con las teclas de flecha y pulse <enter>.



Desde esta pantalla se le pregunta si desea activar el puerto de la consola en el puerto serie del ordenador. Marque "No" y pulse <enter>.

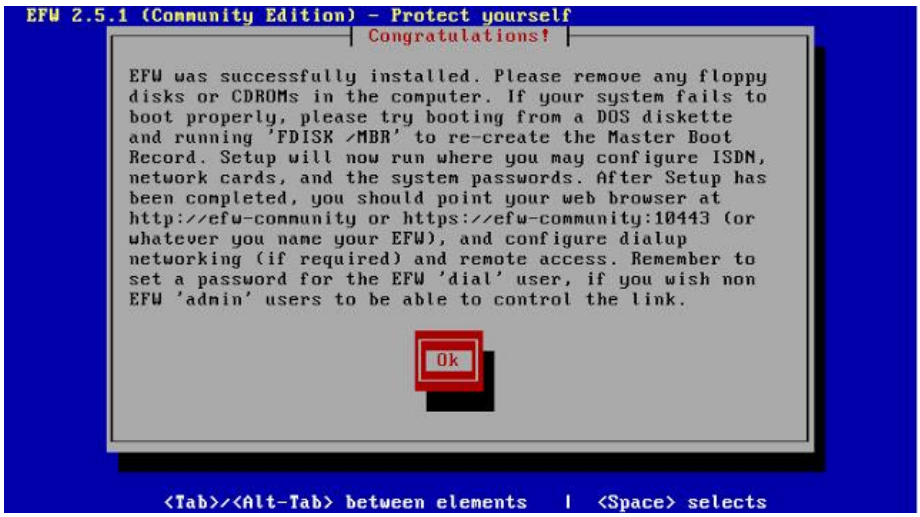


La instalación de la pantalla de los paquetes necesarios para Endian Firewall.



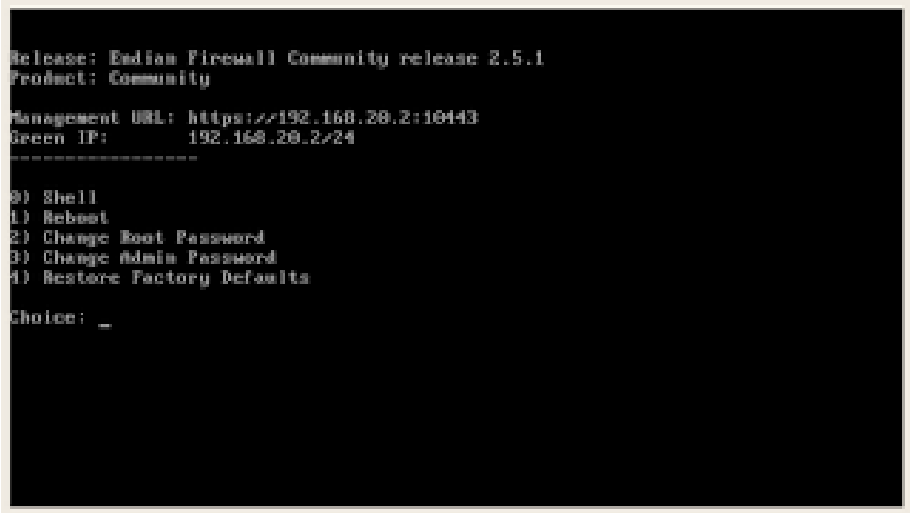
Después de unos momentos, aparecerá la pantalla para configurar la IP de la interfaz de red de color verde. Elija una dirección IP dentro del rango de IP de su red interna y no está siendo utilizado por cualquier dispositivo. Una vez más, esto va a ser la dirección IP, debe configurar el campo de puerta de enlace de las computadoras en las interfaces de red.

Importante: El Endian Firewall utiliza un concepto de color para diferenciar las interfaces de red. Una tarjeta de red o interfaz de red Verde se reúne la red interna, la interfaz de red de color rojo se reúne la red externa (enlace a internet), interfaz de red de naranja se encuentra con el DMZ (red de seguimientos accesibles a través de Internet) y la interfaz de red azul sirve usuarios de redes inalámbricas.

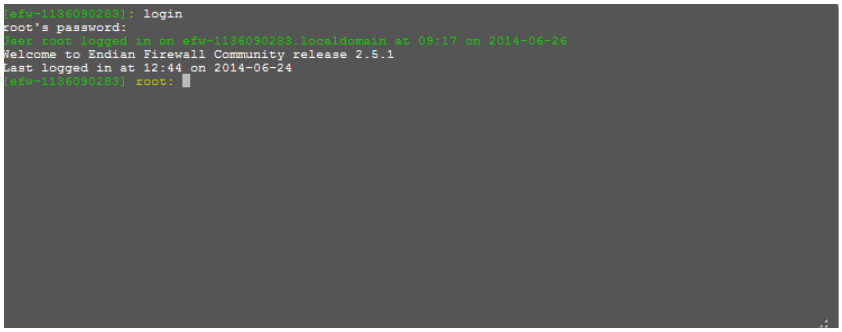


El Endian ha sido instalado con éxito. Apriete <enter> por lo que arrancar el ordenador y cargar el firewall.

En estas dos imágenes nos muestra cuando está terminando la instalación del ENDIAN.



Tras el reinicio de la máquina, escogemos la opción de la shell que es (0), y hacemos enter.



Después al escoger la opción de la shell nos logeamos con el comando LOGIN y la contraseña. Para poder entrar como root.

Listo. A partir de aquí ya puedes entrar por web.

Anexo E

MANUAL DE USUARIO DEL SERVIDOR DE ADMINISTRACIÓN DE SEGURIDAD PARA EL SISTEMA DE INFORMACIÓN (SIRINGUERO).

Es un software que nos brinda una interfaz gráfica, de los servicios y funciones que se requieren para la administración de la seguridad de la red de datos del sistema siringuero, el cual este manual de tallara de una manera práctica y resumida los procesos más importantes del manejo de dicho servidor, bajo pantallas capturadas.

1. ACCEDIENDO AL ENTORNO WEB DEL SERVIDOR ENDIAN

Una de las primeras instancia es seleccionar un navegador web el ENDIAN soporta la mayoría de los navegadores ya sea Firefox, Opera, Safari, etc. En este caso usaremos como navegador predeterminado el Firefox, primeramente debemos colocar la dirección en el navegador en este caso es, **https://192.168.9.x:10443/,** verá el siguiente mensaje"Error Certificado: Navegación bloqueada ", haga clic en"Continuar con estesitio web (no recomendado)"para acceder a la página de Endian

Ver. (Figura 1) y (Figura 2).

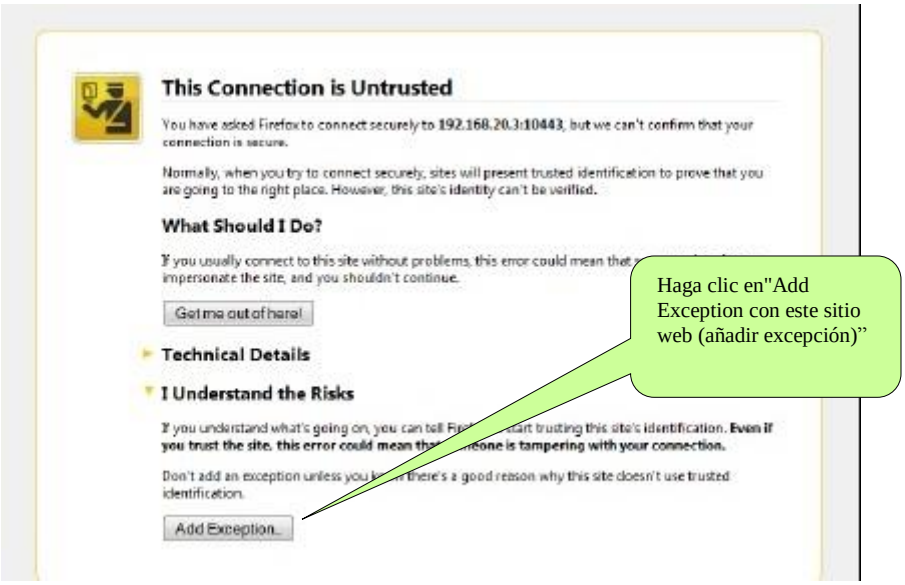


Figura 1.

Figura 2.

Después de aparecer haga clic en Endian en tu página de inicio en "Conectar", como Figura3. Se le pedirá la contraseña del usuario administrador Endian, este usuario tiene el poder de hacer que la administración de Endian. Digitar admin y la contraseña que se ha introducido en la instalación.

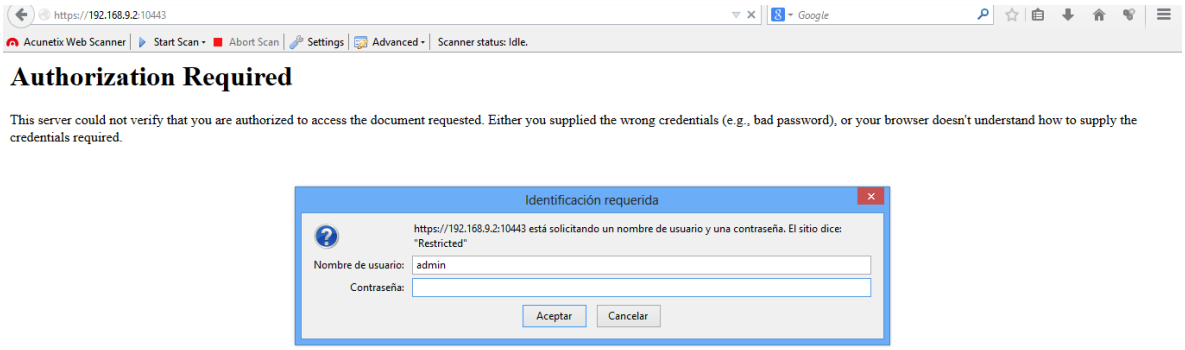


Figura 3.

A continuación aparecerá la bienvenida a la configuración de Endian. Para continuar damos clic en >>>

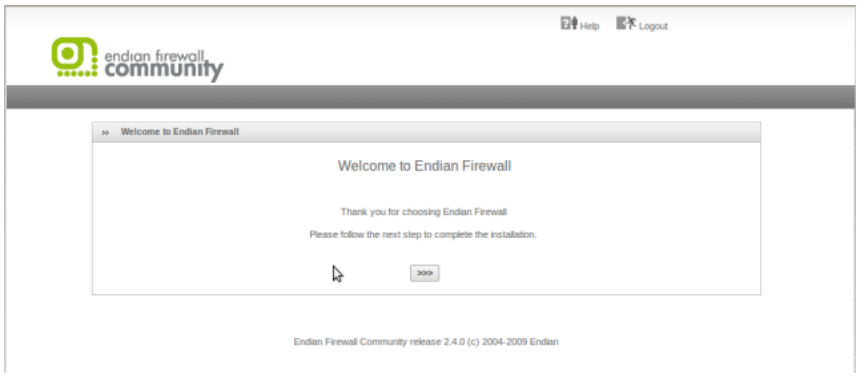


Figura 4.

Ahora vamos a escoger el idioma con el cual queremos configurar Endian, también tenemos la opción de configurar la zona horaria según nuestra ubicación.

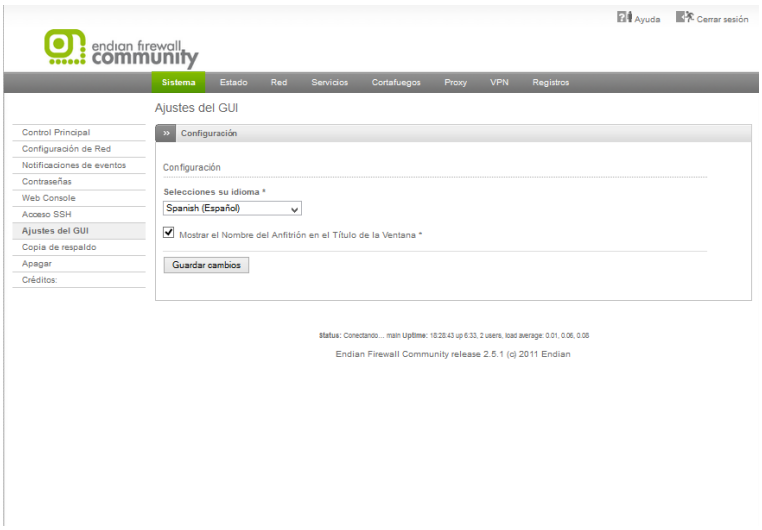


Figura 5.

Aceptamos el acuerdo de licencia sobre el uso de Endian

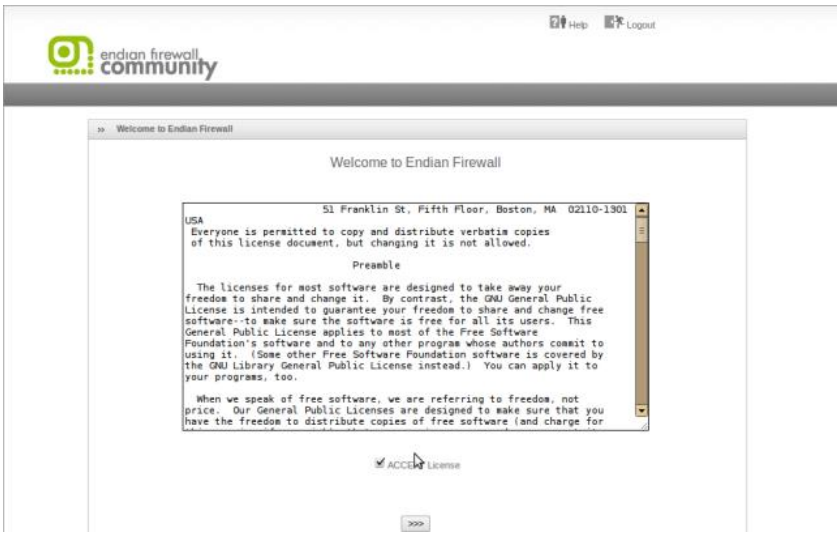


Figura 6.

Endian ahora nos pregunta que si queremos restablecer la configuración desde un archivo de respaldo o backup, pero como es primera vez que lo instalamos entonces dejemos la opción no y continuamos.

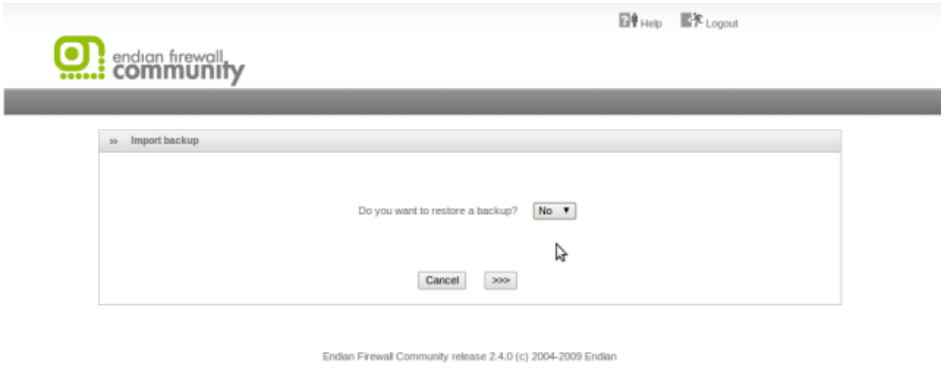


Figura 7.

En la siguiente pantalla debemos configurar las contraseñas para la administración de la interfaz web y del usuario root, cabe recalcar que entre más seguras sea nuestra contraseña más difícil le hacemos el trabajo al atacante.

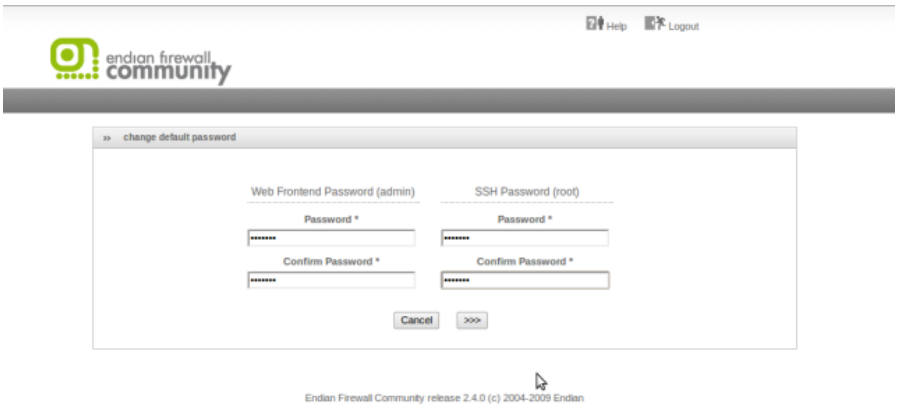


Figura 8.

Ahora vamos a configurar el tipo de conexión que tendrá la interfaz o tarjeta de red que va a estar conectados hacia el cable de red de datos, en el diagrama de la red podemos ver que estamos utilizando 4 tarjetas de red, la primera está conectada a la LAN (Azul), la segunda es la que vamos a configurar en este momento (Naranja), seleccionamos la opción que más se ajuste a nuestras necesidades. En este caso escogemos ETHERNET POR DHCP, al seleccionar esta opción quiere decir que más adelante vamos a colocarle una dirección IP por dhcp a esta interfaz (RED).

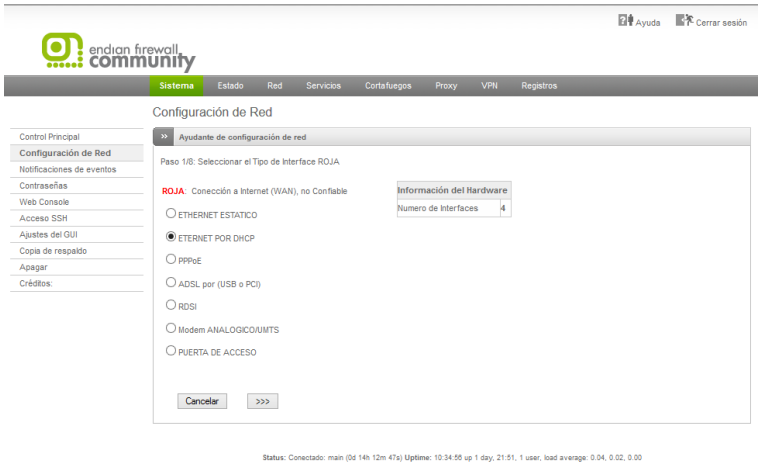


Figura 9.

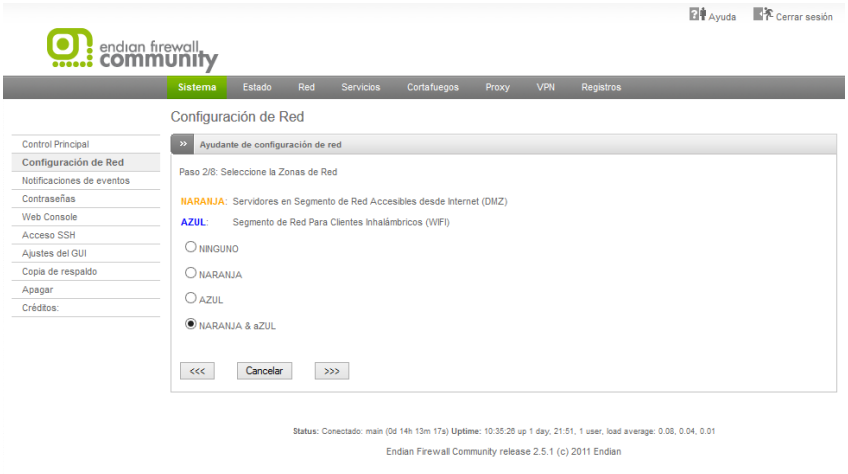


Figura 10.

Aquí configuramos la red (GREEN) y en esta ocasión le colocamos el IP 192.168.7.1/24

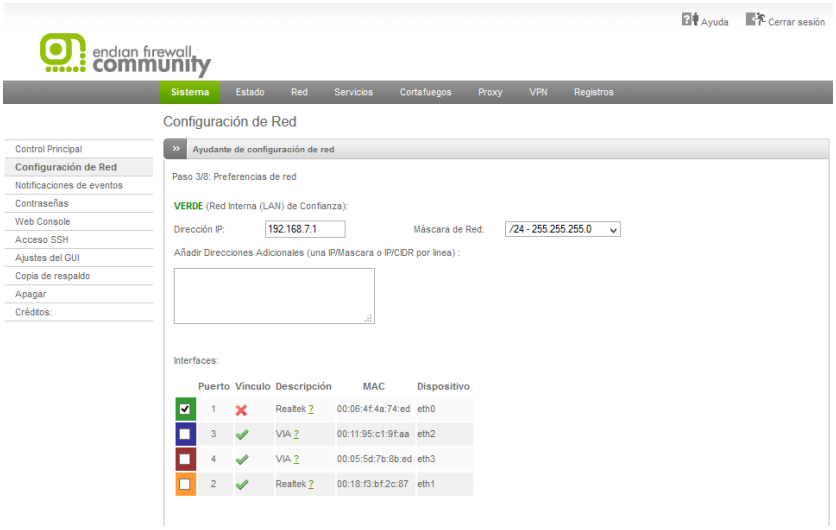


Figura 11.

Configuramos ahora a red (NARANJA) con el IP 10.10.10.1/24

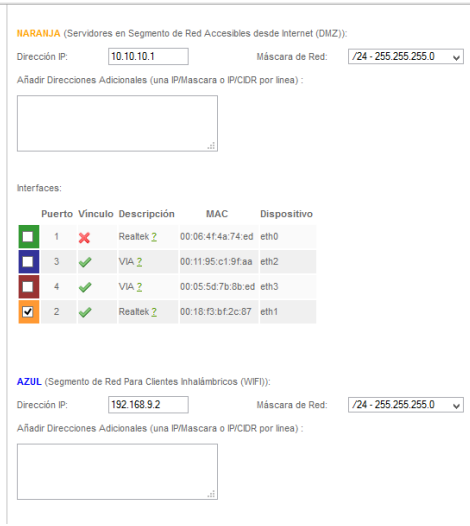


Figura 12.

Configuramos la red (AZUL) con el IP 192.168.9.2/24

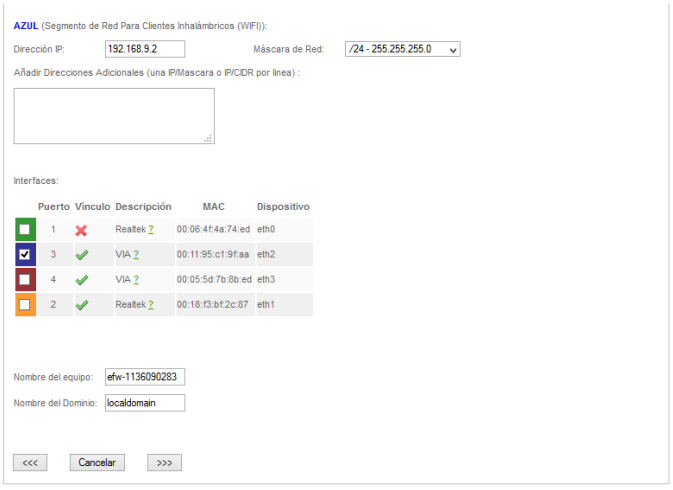


Figura 13.

Y por último la red (ROJA) conexión a internet (WAN) no confiable como lo hemos puesto DHCP no nos pide IP

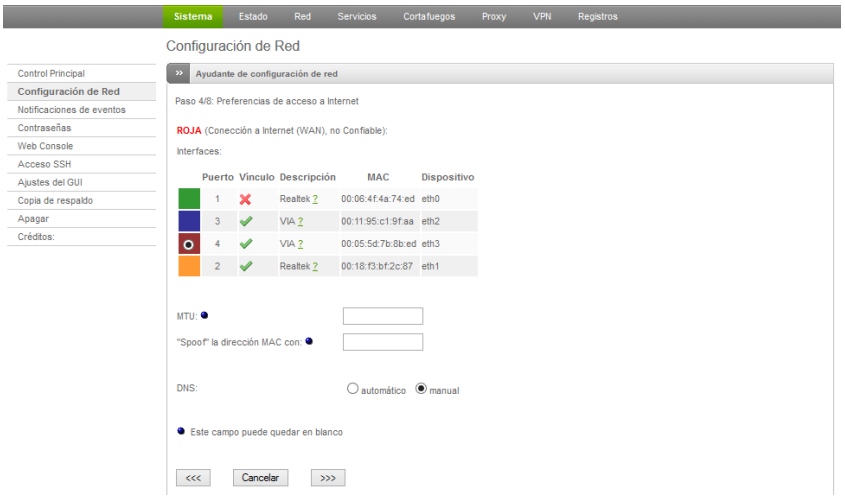


Figura 14.

En esta parte configuraos los DNS respectivo de acuerdo a la red que tengan en esta caso es 192.168.9.1

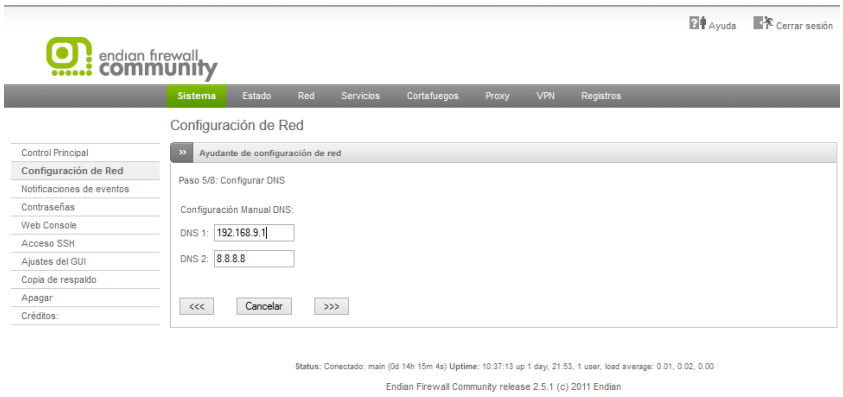


Figura 15.

Configuramos el correo electrónico administrativo.

Figura 16.

Aplicamos la configuración y le damos aceptar.

Figura 17.

Y ya tenemos configurado la red.

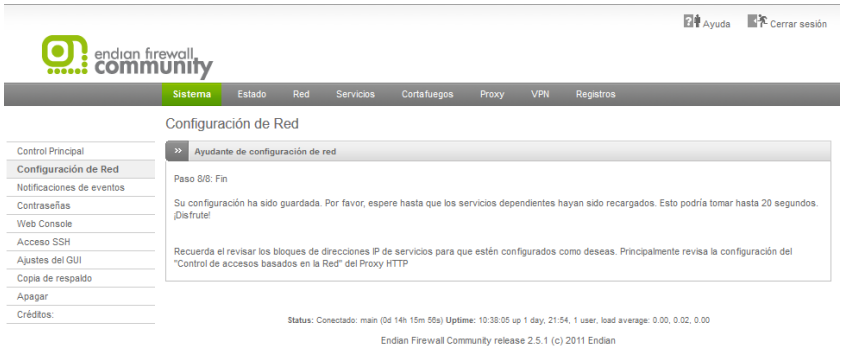


Figura 18.

COPIA DE RESPALDO

Ahora configuraremos las copias de respaldo Entramos en el control principal del firewall. Puedes sacar un backup de la configuración para futuros percances.

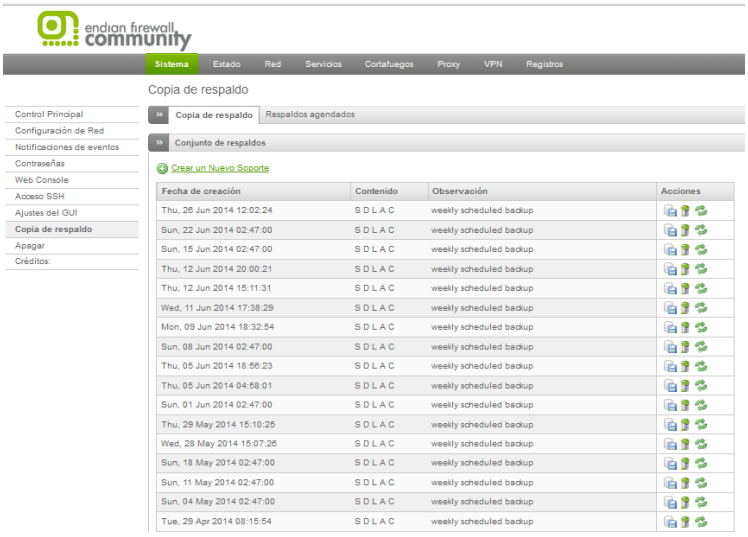


Figura 19.

También lo configuramos los respaldos agendados por semanas donde nos sacara copias de registros base datos y la configuración.

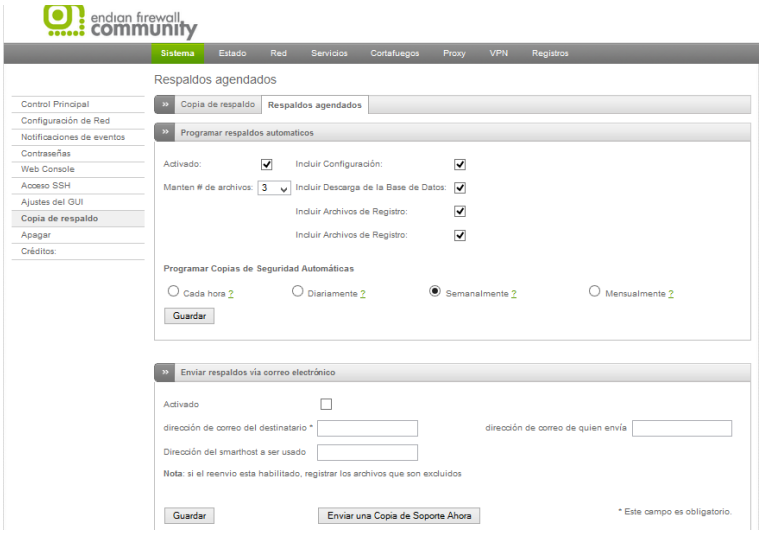


Figura 20.

ESTADO DEL SISTEMA:

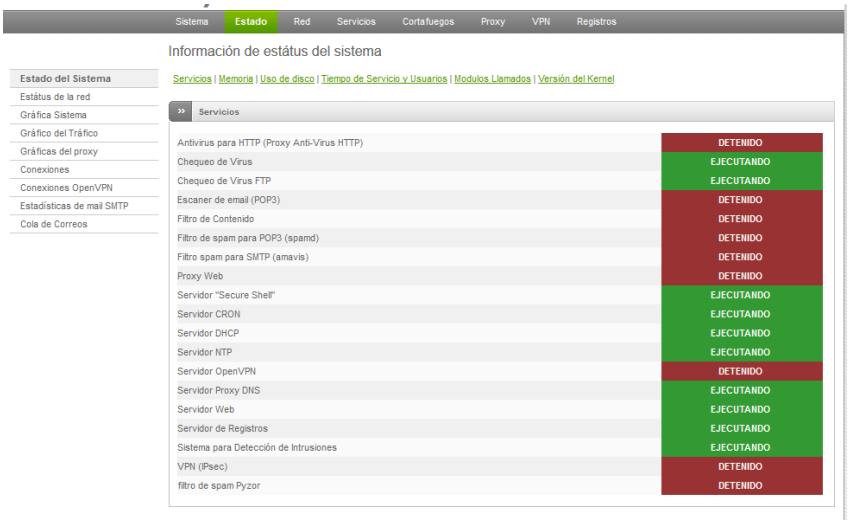


Figura 21.

CORTAFUEGO:
Haciendo NAT

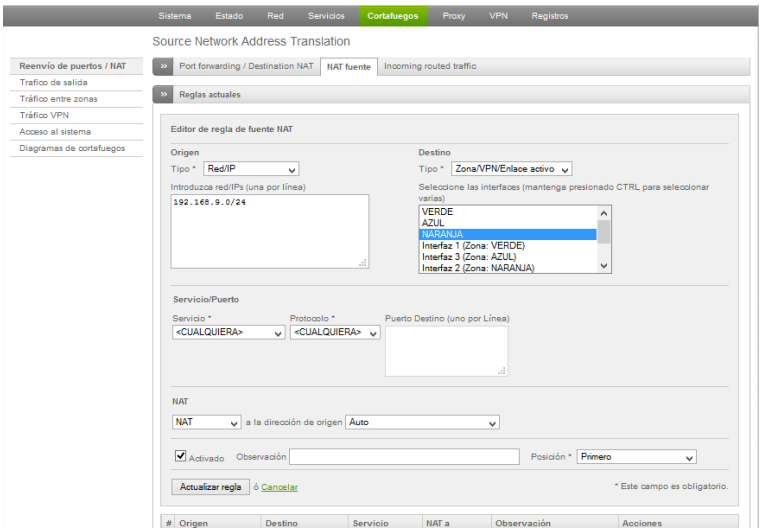


Figura 22.

ASIGNACIÓN DE REGLAS

A continuación vamos a dar clic en la pestaña firewall y en la opción de trafico saliente podemos ver la reglas por defecto que trae el firewall.

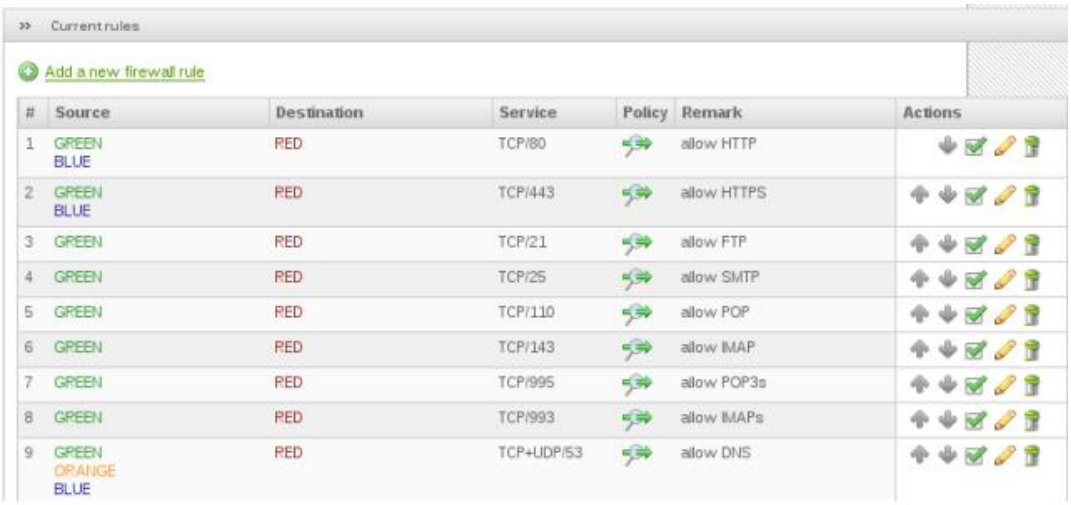


Figura 23.

Voy a crear dos regla de la lista, la me permite el ping de las zonas verde, naranja y azul hacia la red roja la segunda regla me da conexión al siringuero por el puerto 8080 desde mi red local hacia roja.

Para poder editar la regla debemos hacer clic encima del lápiz que se encuentra al final de cada regla.

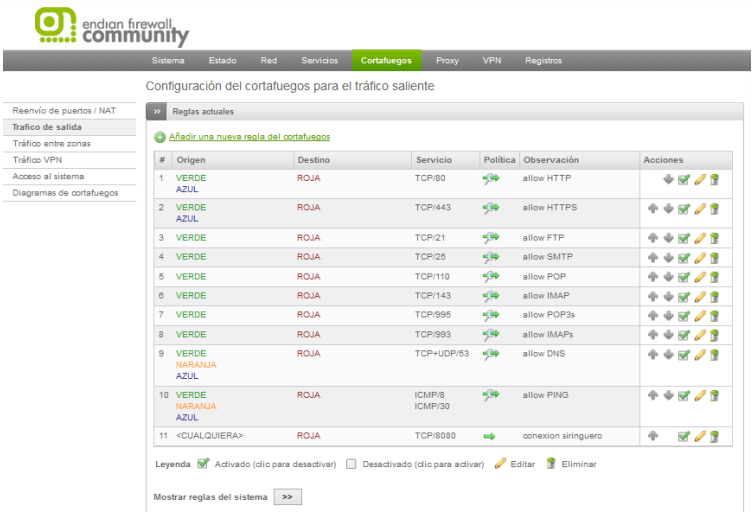


Figura 24.

Configuramos las reglas de acceso para las inter-zonas (LAN y DMZ) hacemos clic en "trafico inter-zonas" en la parte izquierda y luego en "agregar una nueva regla de cortafuegos inter-zonas".

Donde le damos permiso entre zonas. Y creamos una regla donde negamos el ping al sistema siringuero 10.10.10.2

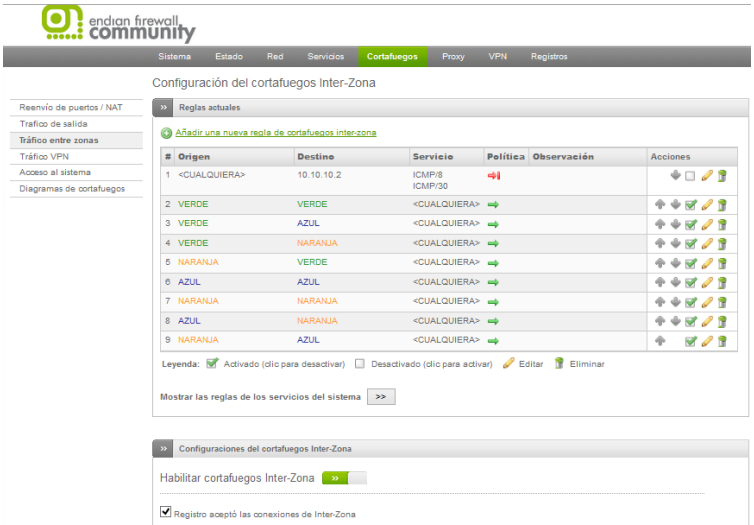


Figura 25.

A continuación vamos a configurar añadiendo una regla de acceso al sistema de la red de datos de la U.A.P y una regla de negación de ping a la IP 192.168.9.2.

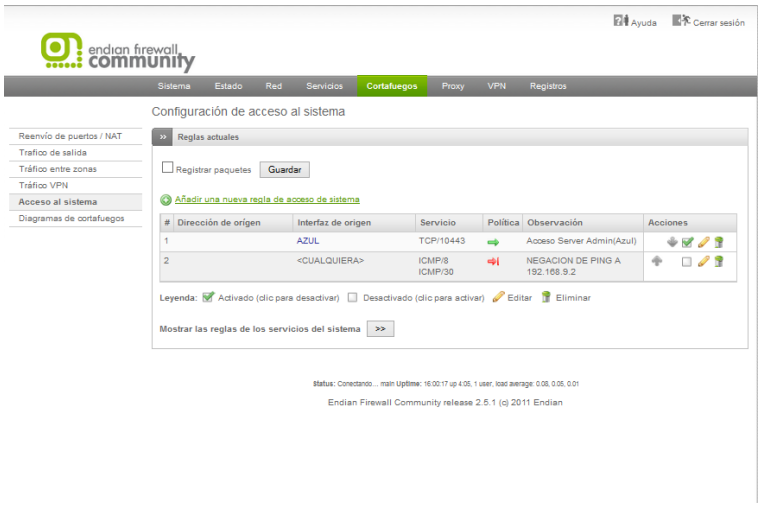


Figura 26.

Añadiendo una regla de acceso al sistema de la red de datos de la U.A.P. 192.168.9.2. con la red AZUL con el puerto 10443.

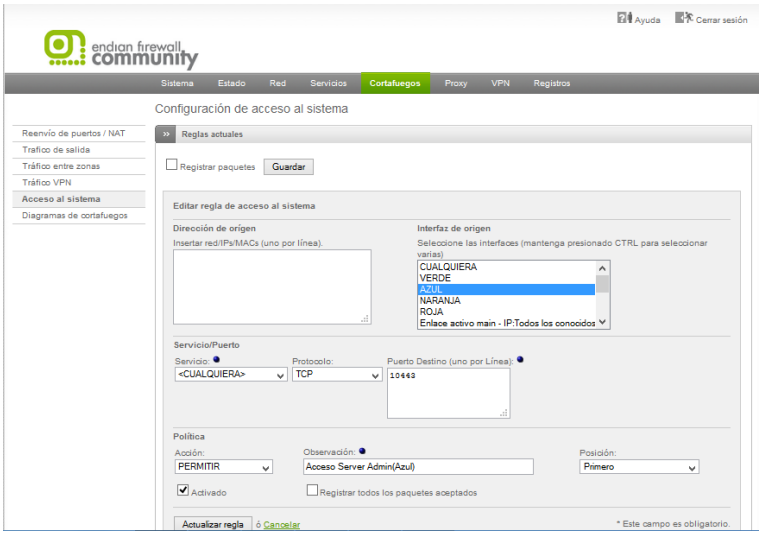


Figura 27.

REGISTROS:

En esta parte seleccionamos los registros que deseamos que tenga el ENDIAN.

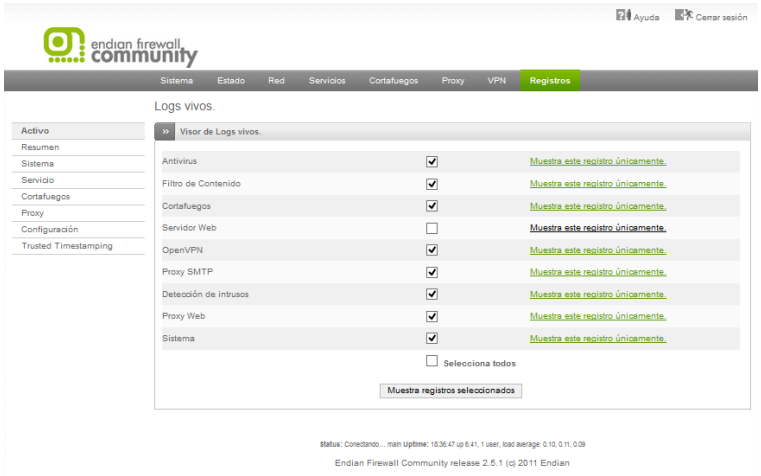


Figura 28.

En esta imagen nos muestra los registros del Antivirus en acción.

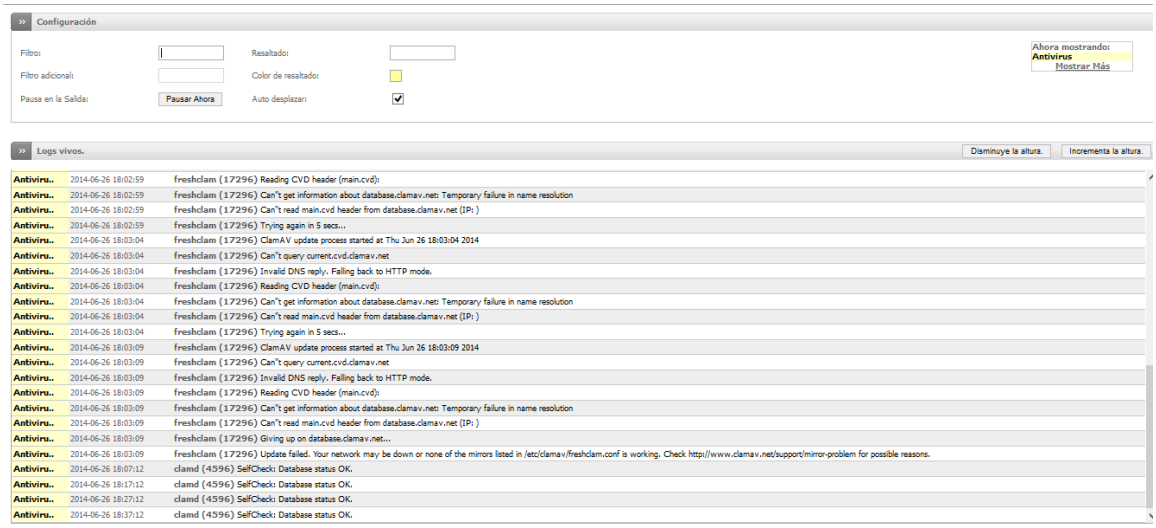


Figura 29.

En esta imagen nos muestra los registros del Cortafuegos en acción.

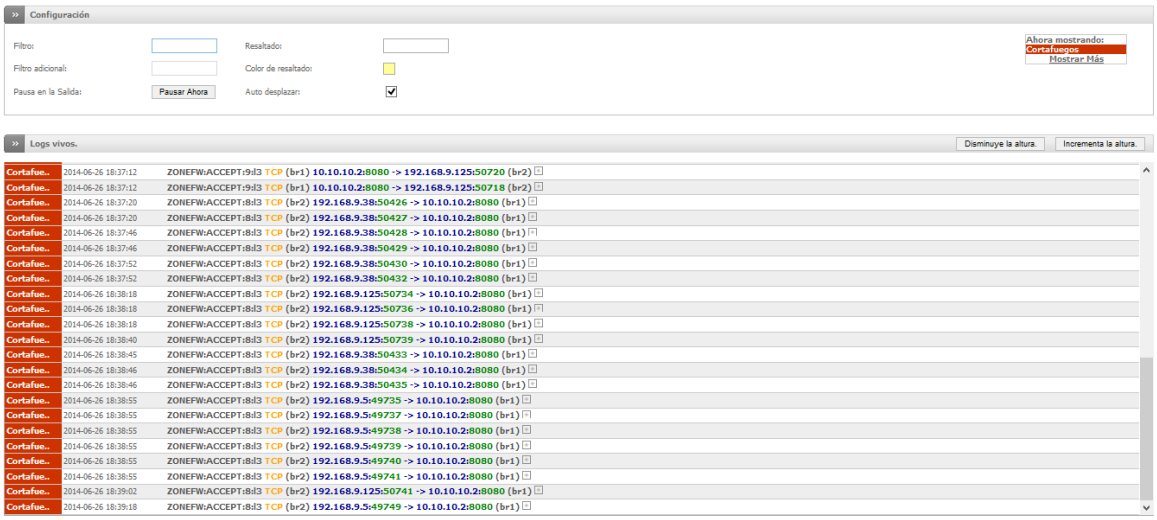


Figura 30.

En esta imagen nos muestra los registros de Detección de Intrusos en acción.

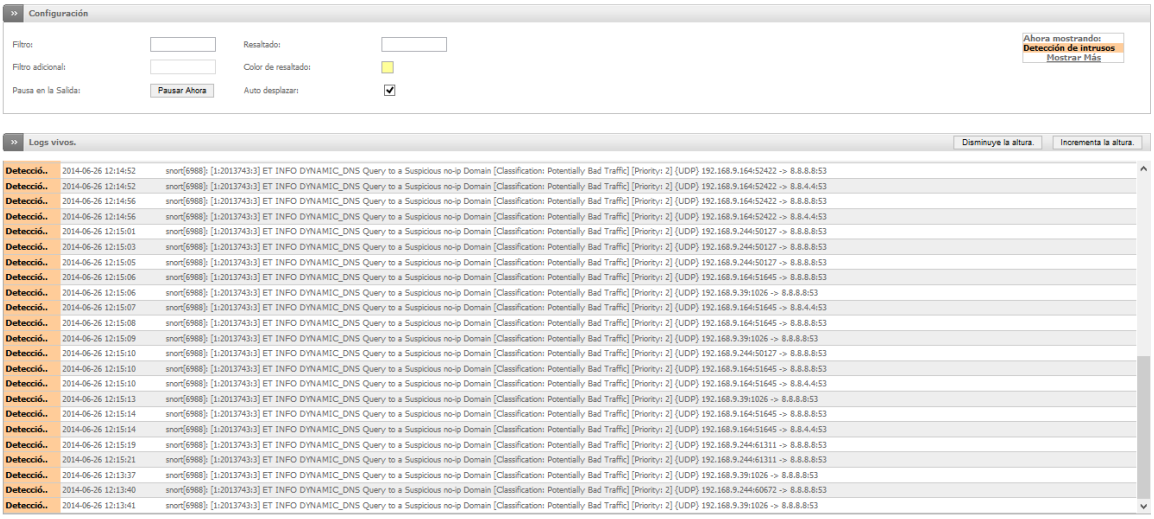


Figura 31.

y aquí tenemos el panel del control central del Firewall Endian 2.5.1

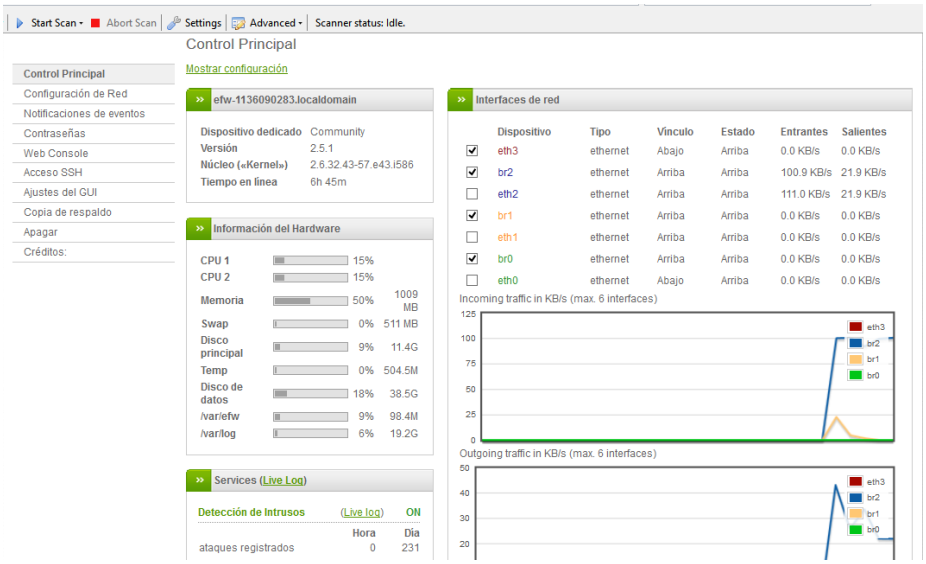

Start Scan
Abort Scan
Settings
Advanced
Scanner status: Idle.
Control Principal
Mostrar configuración
Control Principal
Configuración de Red
Notificaciones de eventos
Contraseñas
Web Console
Acceso SSH
Ajustes del GUI
Copia de respaldo
Apagar
Créditos:
efw-1136090283.localdomain
Dispositivo dedicado Community
Versión 2.5.1
Núcleo («Kernel») 2.6.32.43-57.e43.i586
Tiempo en línea 6h 45m
Información del Hardware
CPU 1 15%
CPU 2 15%
Memoria 50% 1009 MB
Swap 0% 511 MB
Disco principal 9% 11.4G
Temp 0% 504.5M
Disco de datos 18% 38.5G
/var/efw 9% 98.4M
/var/log 6% 19.2G
Services (Live Log)
Detección de Intrusos (Live log) ON
Hora Día
ataques registrados 0 231
Interfaces de red
Dispositivo Tipo Vínculo Estado Entrantes Salientes
eth3 ethernet Abajo Arriba 0.0 KB/s 0.0 KB/s
br2 ethernet Arriba Arriba 100.9 KB/s 21.9 KB/s
eth2 ethernet Arriba Arriba 111.0 KB/s 21.9 KB/s
br1 ethernet Arriba Arriba 0.0 KB/s 0.0 KB/s
eth1 ethernet Arriba Arriba 0.0 KB/s 0.0 KB/s
br0 ethernet Arriba Arriba 0.0 KB/s 0.0 KB/s
eth0 ethernet Abajo Arriba 0.0 KB/s 0.0 KB/s
Incoming traffic in KB/s (max. 6 interfaces)
125
100
75
50
25
0
eth3
br2
br1
br0
Outgoing traffic in KB/s (max. 6 interfaces)
50
40
30
20
eth3
br2
br1
br0

Figura 32.