INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA

PROYECTO DE GRADO A LA OBTENCIÓN DEL TÍTULO DE TECNOLOGÍA EN ANÁLISIS DE SISTEMA

TEMA:

DISEÑO DE UN SERVIDOR FIREWALL MEDIANTE USO DE HERRAMIENTAS OPEN SOURCE, PARA EL CENTRO DE SALUD SAN JOSÉ DE ANCÓN DE LA DIRECCIÓN DISTRITAL DE SALUD DE SANTA ELENA.

AUTOR:

LUIS ANTONIO AGUALONGO DOMÍNGUEZ

TUTOR

LSI. ERICK ORLANDO GUERRERO ZAMBRANO, MSC

Guayaquil, Ecuador

2016

INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA

CERTIFICACIÓN DE LA ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del Proyecto de Investigación, nombrado por el Consejo Directivo del Instituto Superior Tecnológico Bolivariano de Tecnología.

CERTIFICO:

Que he analizado el proyecto de investigación con el tema: **"Diseño de un servidor firewall mediante uso de herramientas Open Source, para el Centro de Salud San José de Ancón de la Dirección Distrital de Salud de Santa Elena.",** presentado como requisito previo a la aprobación y desarrollo de la investigación para optar por el título de:

TECNOLOGÍA EN ANALISIS DE SISTEMAS

El problema de investigación se refiere a: **¿Cómo optimizar recursos y controlar el manejo de la web; para garantizar servicios informáticos requeridos por los funcionarios del centro de Salud Ancón?** El mismo que considero debe ser aceptado por reunir los requisitos legales y por la importancia del tema:

Presentado por el Egresado: **Luis Antonio Agualongo Domínguez**

Tutor**:** **Lsi. Erick Guerrero Zambrano. Msc.**

AUTORÍA

Los criterios e ideas expuestos en el presente trabajo de graduación con el tema: **Diseño de un servidor firewall mediante uso de herramientas Open Source, para el Centro de Salud San José de Ancón de la Dirección Distrital de Salud de Santa Elena**, de la carrera Análisis de sistemas del Instituto Superior Tecnológico Bolivariano de Tecnología, son de absoluta responsabilidad del autor y no constituye copia o plagio de otra tesis presentada con anterioridad.

DEDICATORIA

Dedicar primero a Dios por permitirme continuar con mi proyecto de vida, que a pesar las dificultades y adversidades aún me da la posibilidad de lograr mis objetivos con paciencia, dedicación y la sabiduría para cumplir esta parte de mi carrera profesional, ya que aún quedan muchas más por continuar. Dedicarles parte de este objetivo a mis padres quienes siempre confiaron en mí y por el apoyo incondicional, a mi esposa e hijos que a pesar de mis ausencias siempre estuvieron hay brindándome su apoyo. Y es a ellos a quienes dedico este proyecto por estar siempre conmigo.

A mis padre Luis y Rosa, A mi Esposa Jennifer y mi hijos Cristina y Luis, esto es por ustedes.

Luis Antonio Agualongo Domínguez

AGRADECIMIENTO

A nuestro padre celestial Dios, quien me brinda la oportunidad de cumplir con uno de mis objetivos. A mi familia que gracias a ellos llego a culminar una parte de lo que será mi vida profesional. A mis compañeros de clase y amigos quienes hemos avanzado en esta dura tarea de ser profesionales y poder superar los momentos más difíciles. Agradecer a los profesores quienes nos inculcaron el valor del estudio y aprovechar las oportunidades que en la vida se presentan y formar profesionales para ser exitoso en mi carrera.

Luis Antonio Agualongo Domínguez

INSTITUTO SUPERIOR TECNOLOGICO BOLIVARIANO DE TECNOLOGÍA

TECNOLOGÍA EN ANÁLISIS DE SISTEMAS

Proyecto previo a la obtención del título de: Tecnólogo en Análisis de Sistemas

Tema

"Diseño de un servidor firewall mediante uso de herramientas Open Source, para el Centro de Salud San José de Ancón de la Dirección Distrital de Salud de Santa Elena.''

Autor: Agualongo Domínguez Luis Antonio

Tutor: Lsi. Erick Guerrero Zambrano. Msc.

RESUMEN

Este trabajo tiene como objetivo principal el diseño de un servidor firewall mediante el uso de herramientas Open Source para el Centro de Salud San José de Ancón tipo A. Una vez realizado el análisis durante el proceso de la investigación en el lugar se observaron las diferentes necesidades con respecto al uso de la web, al contar con un centro de salud completamente nuevo que cumple con las normar estándares dentro del cableado estructurado y equipamiento tecnológico, el libre acceso al servicio web, la forma empírica de compartir archivos que conlleva a ser vulnerable el software de cada uno de los equipos de las estaciones de trabajo. Debido a esto se planteó como solución la instalación de un servidor proxy bajo plataforma Linux que sirvió también para la implementación de un servidor de archivos en la nube. Con esto se evita vulnerabilidades y ataques externos en información confidencial que es usada en el centro de salud, el uso de los recursos web y la navegación sea más rápida al usar las aplicaciones web del ministerio de salud pública siempre y cuando guiados por las políticas de seguridad de la Dirección Nacional de Tecnología de la Información del ministerio de Salud Pública. Para la implementación de este diseño se usó la instalación del sistema Operativo Centos 6.0 como versión más estable, la instalación de varios paquetes y servicios como el Squid, DHCP y Owncloud, esto ayuda a mejorar el uso de los recursos web y la concentración de los funcionarios, mejorar el acceso a las aplicaciones web del ministerio, mejorar el almacenamiento y compartición de los archivos dentro del centro de Salud.

Servidor Proxy | Filtrado de contenido | Servidor de Archivo

INSTITUTO SUPERIOR TECNOLOGICO BOLIVARIANO DE TECNOLOGÍA

TECNOLOGÍA EN ANÁLISIS DE SISTEMAS

Proyecto previo a la obtención del título de: Tecnólogo en Análisis de Sistemas

Tema

"Diseño de un servidor firewall mediante uso de herramientas Open Source, para el Centro de Salud San José de Ancón de la Dirección Distrital de Salud de Santa Elena. ''

Autor: Agualongo Domínguez Luis Antonio

Tutor: Lsi. Erick Guerrero Zambrano. Msc.

ABSTRACT

This work has as main objective the design of a firewall server using Open Source tools for the Health Center San José de Ancon type A. Once the analysis conducted during the investigation at the scene observed the different needs regarding the use of the web, by having a center completely new health meets regulate standards within the structured cabling and technological equipment, free access to the web service, empirical way to share files involved to be vulnerable the software of each equipment workstations. Because of this solution was raised as installing a proxy server under Linux platform that also served to implement a file server in the cloud. With this vulnerabilities and external attacks on confidential information that is used in the health center is avoided, the use of web resources and navigation faster when using web applications ministry of public always health and when guided by policies security National Information Technology ministry of Public Health. To implement this design the operating system installation Centos 6.0 as more stable version, the installation of several packages and services such as Squid, DHCP and Owncloud was used, this helps to improve the use of web resources and the concentration of officials, improve access to web applications ministry, improve storage and sharing files within the health center.

Proxy Server | Content filtering | File Server

INDICE DE CONTENIDO

Contenido **Páginas**

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPITULO I
EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

1.1. Ubicación del problema

La conexión al servicio web se la realiza de manera directa con el proveedor del servicio (CNT), sin la ayuda de un servidor que restringen ciertos accesos que sea intermediario entre la red Local y la red externa

Desde el punto de vista tecnológico y a las seguridades informáticas actuales, existiendo muchos fraudes cibernéticos o hackers, quienes buscan vulnerabilidades en las redes informáticas en las instituciones públicas y privadas, es necesario cierto control sobre el uso que se hace del internet y elegir la implementación de un recurso gratuito de protección y control web, al igual que de sus archivos confidenciales.

1.2. Situación conflicto

Al realizar la conexión directa al Internet, sin la implementación de un servidor Proxy que haga de intermediario entre la red local y el servicio web, se presentan los siguientes problemas:

- Los funcionarios pueden acceder a todo tipo de contenido en la Web en sus máquinas sin un firewall que filtre el contenido de acceso.
- Las descargas de páginas Web se vuelve muy lenta, debido a que otros usuarios están usando recursos innecesarios (sean estos Youtube, Facebook, Twitter, entre otras redes sociales).
- Las descargas de contenido Web se vuelven peligrosas por la gran cantidad de virus existentes en el contenido Web.

1.3. Delimitación del problema

Un servidor proxy y servidor de archivo, debe cumplir con las políticas ITIL solicitadas por la coordinación zonal de salud, cumpliendo con los requisitos y parámetros dentro de las políticas de seguridad.

Para poder seleccionar un Servidor Proxy se valora varios aspectos técnicos complejos, y también aspectos como la facilidad de la instalación.

El Servidor Proxy debe cumplir con características detalladas a continuación:

- Registro de Sistema (Log).
- Permisos y Restricción de Acceso en función de la Dirección y URL de destino.
- Permisos y Restricción de Acceso en función de la Dirección de Origen.
- Dirección IP dinámica.

1.4. Formulación del problema

¿Cómo optimizar recursos y controlar el manejo de la web; para garantizar servicios informáticos requeridos por los funcionarios del centro de Salud Ancón?

1.5. Variables de la investigación

Variables dependientes: Optimización de recursos y controlar el manejo de la web.

Variables independientes: Servicios Informáticos requeridos por los funcionarios.

1.6. Objetivos

1.6.1. Objetivo general

Diseñar un servidor en plataforma Linux Centos que pueda controlar los servicios de firewall y servidor de archivos en la nube, con el fin de mejorar el control del contenido Web al que acceden los funcionarios y dar seguridad a la información de la documentación digital con que cuenta el centro de salud.

1.6.2. Específicos

- Fundamentar las diferentes distribuciones del sistema operativo Linux con sus versiones, que servirán de plataforma para la implementación del servidor Proxy.
- Determinar las características necesarias para la implementación de un servicio Proxy.
- Instalar la versión más apropiada del sistema operativo Linux, donde se pueda instalar el servicio Proxy.
- Implementar el servicio de control de contenido Web mediante el firewall.
- Implementar servidor de archivos en la nube (Owncloud).

1.7. Justificación

El centro de salud contaría con un servidor proxy que permita generar los servicios de transferencias de archivos y firewall, lo que permitirá la optimización de los recursos Web en el Centro de Salud, además de mejorar y optimizar las actividades cotidianas.

El centro de salud contaría con un filtrado de información que asegurara el correcto funcionamiento del servicio.

La propuesta es instalar y poner en marcha un servidor bajo plataforma Linux, por lo que se implementara los siguientes servicios.

- Servidor Firewall (Servidor Proxy)
- Servidor de archivo en la nube (Owncloud)

Las distracciones constantes, tanto del uso de la web como las redes sociales que son causantes de distracciones de los funcionarios y de las personas en general, causan desconcentración y optimización del trabajo, impidiendo cumplir con las actividades y metas diarias de la institución.

Por lo tanto un servidor que sirva de filtro de información, permitiendo restringir acceso web y control de los equipos de cada funcionario permitiendo la ejecución de actividades predeterminadas, sin causar distracción alguna. La integración de un servidor no solo se verá reflejada como servidor proxy y servidor de archivos, sino ver a la ejecución de crecer en cuanto a la red y al avance tecnológico como las telefonías IP y las cámaras de video vigilancias IP.

Las distintas amenazas que existen en el mundo informático tales como robo, falsificación, fraudes y destrucciones hacen insegura una institución que no tenga un servidor Firewall.

CAPITULO II
MARCO TEÓRICO

En este capítulo se da a conocer los conceptos básicos y terminologías fundamentales usadas durante el desarrollo del trabajo investigativo. Con la finalidad de tener en claro los principales conceptos teóricos aplicados en la investigación sobre la cual que va a desarrollar el servidor firewall.

2.1. Antecedentes Históricos

2.1.1. Centro de Salud San José de Ancón Tipo A

La Dirección Distrital 24D01 Santa Elena – Salud, que desde inicio de su gestión en Julio del 2014 tienen a su cargo 25 unidades operativas, y entre ellos se encuentra el Centro de Salud San José de Ancón siendo este un centro de salud Tipo A, que según acuerdo ministerial 00004568 del 28 de Enero del 2013, entra en funcionamiento desde el mes de Febrero del 2016 prestando los servicios de Consulta Externa, Enfermería, Farmacia, Sala de procedimientos emergentes, área de Esterilización, Odontológica, Sala de actividades grupales, Sala de reuniones, Estadística, Sala de espera, Bodega general y de desechos contaminados, entre otros espacios.

El Centro de Salud tiene un área de construcción de 748,8 m2, brinda sus servicios a una comunidad de 11890 personas de las cuales el 70% a 80% acuden a los centros de salud estatales, las poblaciones que abarca son las comunas de Ancón, El Tambo, Prosperidad, Francisco de Orellana y San Joaquín.

La máxima autoridad de esta entidad Pública es la Dra. Carmen Berrones, Directora Distrital, El Dr. Edgar Rodríguez Director del Centro de Salud de Ancón quienes son los responsables de llevar el direccionamiento, control y normativas para el correcto funcionamiento de esta unidad de salud que cuenta con 2 Odontólogos, 5 Médicos

Generales, 3 Obstetras, 2 Auxiliares de Enfermería, 1 Auxiliar de Farmacia, 2 Enfermera, 1 Químico Farmacéutico, 1 Promotor Social, 1 Asistente de Atención y 2 Conserjes quienes llevan atención al usuario de la población correspondiente anexa al centro de salud.

Según el Acuerdo Ministerial 5212, en el Capítulo II del Primer Nivel de Atención en su Art. 5 menciona que “Los establecimientos de salud del Primer Nivel de Atención son los más cercanos a la población, facilitan y coordinan el flujo del usuario dentro del Sistema, prestan servicios de promoción de la salud, prevención de enfermedades, recuperación de la salud, rehabilitación y cuidados paliativos. Además, brindan atención de urgencia y emergencia de acuerdo a su capacidad resolutiva, garantizan una referencia, derivación, contrareferencia y referencia inversa adecuada, aseguran la continuidad y longitudinalidad de la atención. Promueven acciones de salud pública de acuerdo a normas emitidas por la Autoridad Sanitaria Nacional. Son ambulatorios y resuelven problemas de salud de corta estancia. El Primer Nivel de Atención es la puerta de entrada al Sistema Nacional de Salud”.

El proyecto de tesis a implementarse en esta centro de salud ya se encuentra implementado en la Dirección Distrital 24D01 Santa Elena y el Hospital Básico Manglaralto cumpliendo con las funcionalidades determinadas como filtrado de contenido, lo que ayuda bastante en la optimización de recursos ahorrando el uso del ancho de banda de su enlace dedicado y la navegación rápida de los diferentes servicios web.

En ambos lugares donde se ha dado la implantación de servidores firewall y filtrados de contenidos la infraestructura es la adecuada, cada una de los departamentos de tecnología de la información cuenta con un lugar específico para la ubicación de los servidores, además de la estructura del cableado.

2.2. Antecedentes Referenciales

En nuestros días un ordenador completamente aislado del mundo exterior es algo prácticamente inservible. Muchas tareas cotidianas como enviar y recibir emails, compartir ficheros o consultar una base de datos requieren una conexión externa. (Vásquez, 2010, p.66)

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la institución. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información, podrá únicamente autorizar el paso del tráfico y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Los Firewalls son una parte esencial de la seguridad en una red de computadoras. Son utilizados para proteger la red internas de ataques exteriores.

La efectividad de un Firewall no es el software en sí, sino quien lo administra y aplica las reglas, es decir que en un sistema de firewall implementado por software, las reglas deben estar bien aplicadas, y el riesgo a tener una intrusión externa dependerá de las vulnerabilidades del sistema operativo donde se esté corriendo el servicio de firewall.

Cuando se implementa un firewall, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los TCP, también los UDP, los ICMP, los GRE y otros protocolos vinculados a VPNS.

En los últimos 10 años se ha visto un incremento apreciable en la demanda de instalación de sistemas basados en Linux en Latinoamérica. En el caso específico del Ecuador, una gran cantidad de empresas ya tienen o necesitan tener Linux en sus servidores debido a su renombrada estabilidad, aunque muchas también se interesan porque su licencia de uso no tiene costo usualmente.

El gobierno del Ecuador mediante el Decreto 1014 ha solicitado que las instituciones del estado deben utilizar por política Software Libre, Linux es su exponente más visible y por lo tanto se ha incrementado la necesidad en instituciones estatales de utilizar Software Libre. A través de esta y muchas otras acciones, el uso de Linux en nuestro país ha ido incrementándose y por tanto los requerimientos de soporte, capacitación en este Sistema Operativo.

El uso de software libre en Ecuador ha crecido de una forma continua y a medida de su crecimiento las empresas buscan más seguridad y confiabilidad, además de que el uso a nivel mundial son usadas por empresas grandes que trabaja baja plataforma Linux como Facebook, Gmail, LinkedIn o Yahoo.

Una de las empresas ecuatorianas en usar es EMPRESA PROTECO COASIN S.A. de una infraestructura de servicios de red y resguardo de servidores Linux y clientes Windows junto con la integración de servicios con Active Directory de Microsoft es la base para comenzar con una infraestructura de red confiable y escalable, que permita en un futuro próximo continuar con los proyectos internos y mejorar la atención prestada a los usuarios internos y externos de la empresa. (León, 2012, pag5)

La implementación de servicios basados en Open Source continua de manera constante desarrollándose y mejorando de manera continua, en la parte económico de una empresa permite el ahorro en

licenciamiento y adquisición de hardware, ya que se usan los mismos equipos debido a la manejabilidad, y bajo consumo de recursos.

Ahora retomando el tema del Centro de Salud de Ancón, donde es nuestro punto principal para la solución del problema del tráfico de la red. El centro de Salud no cuenta con servidor Firewall que haga las veces de protección a los sistemas a implementarse.

Actualmente todos los equipos tienen una conexión directa al servicio web y se ha realizado las respectivas configuraciones manuales tales como cambiar el Hosts en cada una de las computadoras desde los usuarios administrador y la configuración de filtrado por Mac en cada uno de los routers. Esto implica no tener un control de tráfico de la red y del uso de las mismas, la proyección de este sistema está enfocada a futuro para su crecimiento en la instalación de un sistema Hospitalario SAIS (Sistema Atención Integral de Salud).

2.3. Marco Legal

Mediante Decreto Ejecutivo No. 1014 emitido el 10 de Abril de 2008, se dispone el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador. Es interés del Gobierno ecuatoriano alcanzar soberanía y autonomía tecnológica, así como un ahorro de recursos públicos. Anexo 1

Se decretó establecer como política pública la utilización de software libre en los sistemas y equipamientos informáticos de las Entidades de la Administración Pública Central, tomando como definición de Software Libre las cuatro libertades promulgadas por Richard Stallman, indica además, que se debe evaluar periódicamente los sistemas informáticos que utilizan software propietario con el fin de migrarlos a software libre.

El Plan nacional del Buen Vivir en su objetivo 11 señala que el país debe gestionar sus recursos automatización, la robótica y la

microelectrónica, contribuya al incremento generalizado del bienestar para sus habitantes. Esto se conseguirá mediante un conjunto de políticas para la sustitución de importaciones, la transferencia de tecnología, la generación de valor agregado local, la industrialización para la exportación, la redistribución de la riqueza y la implementación de industrias de producción de bienes intermedios y finales, dentro del territorio nacional.

Normativa Cloud en Ecuador

La nube informática es un modelo para permitir, desde cualquier lugar y a través de la red, el acceso a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) con un esfuerzo mínimo de gestión así como una mínima interacción con el proveedor del servicio.

Existen tres modelos de servicio que un proveedor de nube informática podría ofertar (Morocho, 2013):

1. Software como servicio (Saas), permite usar aplicaciones previamente instaladas.
2. Plataforma como servicio (PaaS), permite la creación de aplicaciones con herramientas e idiomas previamente definidos por el proveedor.
3. Infraestructura como servicio (IaaS), permite la instalación de cualquier tipo de software en un hardware remoto, también se lo conoce como máquina virtual.

El surgimiento del modelo de software como servicio es una tendencia a nivel mundial por considerarse una solución flexible, escalable, de bajo costo y fácil adopción (Jara, 2012; Zuñiga, 2014:62). Ecuador no es la excepción, en el sector de la pequeña y mediana empresa, por ejemplo, cerca del 40% hace uso de la nube informática (Armijos, 2013) y las páginas más visitadas por los usuarios finales, como Facebook, usualmente incorporan este tipo de servicios.

Este modelo de negocio ha despertado la preocupación de organizaciones comprometidas con la privacidad, ya que los operadores de las nubes podrían usar información privada de sus clientes sin su consentimiento (Kurbalija, 2014), adicionalmente un potencial atacante no tendría que infiltrarse en varios computadores para obtener la información de un grupo de personas, sino sólo en unas pocas (Ramos, 2014). La tendencia al monopolio en el mercado (Burch, 2014b) podría potencializar el número de posibles víctimas de estos ataques, como se ha evidenciado en casos recientes.

Según el fundador de la Free Software Foundation, el SaaS "equivale a ejecutar software que contiene código espía y una puerta trasera universal. Otorga al administrador del servidor un poder injusto sobre los usuarios" (Stallman, 2010). No obstante, es el segundo modelo de negocio más utilizado en el sector del software libre en Ecuador (Delgado, 2014), esto puede ser un claro indicador de su preponderancia de este modelo de negocio, considerando que entre los desarrolladores de software libre se tiene una mayor conciencia sobre los temas de privacidad (Appelbaum, 2014a) y a pesar de ello este modelo persiste como uno de los más importantes.

La adopción masiva de servicios en nube podría suponer que al haber una pérdida de conexión se comprometan una mayor cantidad de servicios, como redacción de texto o incluso cálculo simplificado (Kurbalija, 2014). La problemática de interoperabilidad entre nubes se volverá crítica, podría ser necesaria la creación de un nuevo estándar para mantener una correcta funcionalidad, así como para un mayor nivel de seguridad (Kurbalija, 2014; Fox et col., 2009).

Las revelaciones de Snowden han mitigado la migración a servicios en la nube, entre aquellas empresas que todavía no han adoptado este servicio (NTT Communications, 2014), la razón es que no existe suficiente confianza sobre la privacidad de los usuarios y la seguridad de la información, esta es también la principal preocupación en Ecuador

(Infantino, 2014). Según el ex-analista de la CIA, una forma en que los proveedores podrían recuperar a sus clientes es ofrecer sistemas en los cuales estos no puedan obtener acceso alguno a la información (Meyer, 2014). Este tipo de servicio se daría en una nube privada (Iaas).

A fin de aumentar el nivel de seguridad en la nube se debería también asegurar el cifrado en la transmisión de datos, entre otras características (Ramos, 2014; Morocho, 2013). La ubicación de los servidores también es una característica importante para los usuarios. En el sector privado, apenas un 5% de quienes toman las decisiones sobre TIC piensa que la ubicación de los servidores es intrascendente, de hecho entre el 92 – 97% refiere preferir que estos se encuentren en su propia región (NTT Communications, 2014). Esto también es cierto para los gobiernos, dado que la mayoría de granjas de servidores se encuentran en Estados Unidos (Kurbalija, 2014).

En noviembre de 2013, el en ese entonces Secretario Nacional de la Administración Pública, Cristian Castillo, declaró que “la premisa detrás de la política pública [ecuatoriana] siempre ha sido garantizar la soberanía tecnológica” (“Una Minga por la Libertad Tecnológica”, 2013), el reglamento emitido por la misma institución prohíbe a los servidores públicos el uso de nubes ubicadas fuera del territorio nacional.

Si bien es cierto que la seguridad informática es la principal preocupación, también debe considerarse la importancia de otras áreas como la gestión de la identidad, la gestión del control de acceso, la seguridad forense, la virtualización, la computación distribuida, entre otras (Salazar, 2013).

El 16 de marzo de 2010, se presentó ante la Asamblea Nacional el proyecto de “Ley de Protección a la Intimidad y a los Datos personales”, el Legislativo resolvió su archivo por considerar que varias de las normas propuestas ya constan en la Constitución y en la legislación secundaria existente (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, Ley de Transparencia y Acceso a la Información Pública),

esto a pesar de que la propia constitución señala que debe existir una ley de protección a datos privados en registros públicos (“Asamblea Nacional archiva el proyecto de Ley de Protección a la Intimidad y a los Datos Personales”, 2010).

Debido a la falta de una regulación específica para la Nube, los contratos o acuerdos de Nivel de Servicio representan el principal elemento de cumplimiento. Salazar (2013:108) propone una serie de principios para ser incluidos en un nuevo marco regulatorio específico para Ecuador, que abarque la protección de datos en la Nube:

Aprobación: Considerar si el tratamiento de datos necesita el consentimiento del titular, responsable de los datos, interesado de los datos, etc.

- Delimitación de responsabilidades: Esclarecer cuáles son las responsabilidades específicas de las partes en un servicio de Cloud Computing.
- Finalidad: Cual será la finalidad determinada para utilizar la plataforma de Cloud Computing, y si debe o no extenderse hacia otra finalidad.
- Seguridad: Qué medidas técnicas y organizativas deben adoptarse para el tratamiento de datos en un entorno de Cloud. Si es posible establecerlo como un requisito para los proveedores de la Nube.
- Transferencias Internacionales: Cómo debería realizarse el flujo transfronterizo de los datos personales y los niveles de protección que deben presentar los involucrados. Qué se reconoce por un adecuado nivel de protección.

Intervención de terceras partes que afecten el tratamiento de los datos: Qué requisitos deben cumplir las terceras partes cuando intervengan en un ambiente de Nube. Comunicación al cliente de quienes intervienen en el tratamiento de datos en la Nube.

- Comunicación: Comunicación a los clientes acerca de todos los cambios y modificaciones importantes que se den en la plataforma de la Nube, que afecten el servicio, siendo claros y transparentes.
- Indemnizaciones, garantías y sanciones: Cómo retribuyen los proveedores de servicios de la Nube al cliente en el caso de provocarle daños irreparables en el tratamiento de los datos.
- Propiedad intelectual: Cómo se interpreta la propiedad intelectual de los datos colocados en una infraestructura de Nube. Qué sanciones se colocarían al mal uso o abuso de contenido con derechos de autor.

La responsabilidad de desarrollar este marco regulatorio, según la normativa actual, recaería sobre la Dirección de Regulación, Integración y Control de la Subsecretaría de Informática de la Secretaría Nacional de Administración Pública.

2.4. Marco Conceptual

2.4.1. Internet

Internet es una red internacional de redes: Internacional Network, lo define como un método de interconexión descentralizada de redes de computadoras implementado en un conjunto de protocolos TCP/IP y garantiza que redes físicas heterogéneas funcionen como una red lógica única, de alcance mundial. Dicho de modo más sencillo, se trata del conjunto de ordenadores que se encuentran conectados entre sí y que lo hacen generalmente a través de la línea telefónica. (Dr. J. Arranz, 2007)

La web es utilizado fundamentalmente para intercambiar datos entre software aplicativos las redes mediante estándares y protocolos. De esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "red global". Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes; este

lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP.

2.4.1.1. Ventajas del Internet

- Hace la comunicación mucho más sencilla.
- Es posible conocer e interactuar con muchas personas de todas partes del mundo.
- La búsqueda de información se vuelve mucho más sencilla, sin tener que ir forzadamente a las bibliotecas tradicionales.
- Es posible encontrar muchos puntos de vista diferentes sobre alguna noticia.
- Es posible la creación y descarga de software libre, por sus herramientas colaborativas.
- La computadora se actualiza periódicamente más fácil que si no tuviéramos internet.
- Es posible encontrar soporte técnico de toda clase sobre alguna herramienta o proceso.
- El seguimiento de la información a tiempo real es posible a través del Internet.
- Y es posible compartir muchas cosas personales o conocimientos que a otro le puede servir, y de esa manera, se vuelve bien provechoso.

2.4.2. Linux

GNU/Linux es un equipamiento lógico libre o Software Libre. Esto significa que el usuario tiene la libertad de redistribuir y modificar a de acuerdo a necesidades específicas, siempre que se incluya el código fuente, como lo indica la Licencia Publica General GNU (acrónimo de GNU is Not Unix), que es el modo que ha dispuesto la Free Software Foundation (Fundación de equipamiento lógico libre). Esto también incluye el derecho a poder instalar el núcleo de GNU/Linux® en cualquier

número de ordenadores o equipos de cómputo que el usuario desee. (Barrios, 2015, p39).

Linux es un sistema operativo de la familia Unix, gratuito, creado mediante la política de “código abierto”. Estas características implican un gran ahorro en los costos de instalación de los equipos, pero también una mayor especialización por parte del personal informático. En todo sistema Unix existe un usuario administrador (root), que controla el funcionamiento completo del sistema, tiene acceso universal y puede realizar cualquier operación con los datos y los dispositivos de la máquina.

2.4.3. Servidores de Correo

El correo electrónico, se ha convertido en el medio más rápido, seguro, barato y compatible, de transmisión de información. En 1962 un ingeniero inglés llamado Ray Tomlison, inventó el correo electrónico. Él fue quien ideó usar elcarácter “@”, tan de moda hoy en día, para delimitar la dirección de correo electrónico, del espacio de nombres al que pertenece. Trabajaba para BBN, una empresa tecnológica estadounidense, y según parece en un primer momento no confío en que su invento tuviese ningún futuro. (Carazo, 2011)

El correo electrónico (correo-e, conocido también como e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos.

El correo electrónico gira alrededor del uso de las casillas de correo electrónico. Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico de destino. Más precisamente, el mensaje se envía al servidor del correo electrónico (llamado MTA, del inglés Mail Transport Agent [Agente de Transporte de Correo]) que tiene la tarea de transportarlos hacia el MTA del destinatario. En Internet, los MTA se comunican entre sí usando el protocolo SMTP, y por lo tanto se los llama servidores SMTP (o a veces

servidores de correo saliente). Para su funcionamiento necesitan de los servidores DNS que les indican cuales son los servidores de correo de un determinado domino.

2.4.4. Redes

Una red puede definirse como un conjunto de puntos (objetos, nodos) que interactúan de algún modo entre sí. Su visualización suele realizarse apelando al auxilio de grafos, tal como lo serán casi todas las imágenes que expondré en este post. Del mismo modo, un sistema jerárquico no es más que una red cuya configuración obedece a un conjunto de reglas específicas. Existen otras muchas tipologías. Juan Ibañez (25 de marzo del 2008), http://www.madrimasd.org/blogs/universo/2008/03/25/87333.

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.

2.4.4.1. Tipos de Redes

Los tipos de redes varían por el tamaño, la cantidad de usuarios conectados, y los diferentes servicios que presten.

2.4.4.1.1 Redes LAN

Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología (la más utilizada es Ethernet).

Una red de área local es una red en su versión más simple. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps (por ejemplo, en una red Ethernet) y 1 Gbps (por ejemplo, en FDDI o Gigabit Ethernet). Una red de área local puede contener 100, o incluso 1000, usuarios.

2.4.4.1.2. 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 estratégicos en el marco de una inserción internacional, que permita que el ciclo tecnológico actual basado en la

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. esta redes pueden ser pública o privada.

2.4.4.1.3. Redes WAN

WAN (Wide Área Network) al igual que las redes LAN, estas redes permiten compartir dispositivos y tener un acceso rápido y eficaz, la que la diferencia de las demás es que proporciona un medio de transmisión a larga distancia de datos, voz, imágenes, videos, sobre grandes áreas geográficas que pueden llegar a extenderse hacia un país, un continente o el mundo entero, es la unión de dos o más redes LAN.

Una red de área amplia o WAN (Wide Área Network) se extiende sobre un área geográfica extensa, a veces un país o un continente, y su

función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí.

2.4.4.1.4. Redes WLAN

Es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

Como son redes inalámbricas, las WLAN suelen posibilitar que los usuarios tengan una amplia movilidad, ya que no dependen de cables o elementos físicos para permanecer en la red. La ausencia de cables también contribuye a mantener un orden o una organización en la oficina o el ambiente en cuestión.

2.4.4.1.5. Redes VLAN

Es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

2.4.5. Proxy

Es un programa u ordenador que hace de intermediario entre dos ordenadores. Uno de los mejores ejemplos que puede implementar este autor seria “Supongamos que nosotros nos identificamos como “juanito” y queremos hacer una petición al servidor llamado “pepito”. Si la petición

la hacemos directamente, “pepito” sabe que “juanito” le hizo una petición. En cambio, si usamos un proxy que sería un intermediario que por ejemplo podemos llamar “manolito”, la petición se la haríamos a manolito y éste se la haría a pepito”. De esta manera, pepito no sabe que quien realmente ha hecho la petición es juanito. A su vez, el intermediario puede bloquear determinadas peticiones. Por ejemplo, si pedimos a un proxy que tiene bloqueadas las extensiones .xxx, que nos muestre la página web “amanecer.xxx”, dicha página web no se nos mostrará porque el proxy actúa bloqueándola. (Sierra, 2006)

Un proxy es un Software que realiza una tarea acceso a Internet en lugar de otro ordenador, siendo este un punto intermedio entre un ordenador conectado a Internet y el servidor que se está accediendo. Cuando navegamos a través de un proxy, en realidad no se está accediendo directamente al servidor, sino que se realiza una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y devuelve el resultado de la solicitud.

Cuando se conecta al proxy, el servidor al que se accede en realidad recibe la solicitud del proxy, en vez de recibirla directamente desde el ordenador. Puede haber sistemas proxy que interceptan diversos servicios de Internet. Lo más habitual es el proxy web, que sirve para interceptar las conexiones con la web y puede ser útil para incrementar la seguridad, rapidez de navegación o anonimato.

Utilizar un proxy también tiene sus desventajas, como posibilidad de recibir contenidos que no están actualizados, tener que gestionar muchas conexiones y resultar un cuello de botella, o el abuso por personas que deseen navegar anónimamente. También el proxy puede ser un limitador, por no dejar acceder a través suyo a ciertos protocolos o puertos.

2.4.5.1. Tipos de Servidores Proxy

Existen varios tipos de proxy, según el lugar donde se instalan y quién establece la política del proxy. Por ejemplo:

- **Los proxys internos o locales:** que se instalan en un ordenador cliente y están sobre todo orientados a controlar el tráfico y evitar que la información privada de un ordenador o una red salga de la computadora. Los llamamos también proxys de filtrado.
- **Los proxys externos:** se instalan en una entidad externa al ordenador u ordenadores desde el que se realizan las conexiones. Podemos montarlo nosotros mismos en un servidor propio, o utilizar un servidor dedicado. Hay servidores dedicados baratos que puedes administrar tú mismo y utilizar como pasarela.

2.4.6. DNS

El DNS es una base de datos distribuida usada por aplicaciones TCP/IP para mapear entre nombres de hosts, también provee a los correos electrónicos información de ruteo.

DNS es una abreviatura para Sistema de nombres de dominio, un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

2.4.7. DHCP

Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración en forma dinámica. Sólo tiene que especificarle al equipo mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El DHCP permite a un equipo que se configura de forma automática, eliminando la necesidad de la intervención de un administrador de red, además proporciona una base de datos central para hacer el seguimiento de los equipos que se han conectado a la red. Con esto se evita que dos ordenadores de forma accidental se configuren con la misma dirección IP.

En ausencia del servicio DHCP, las computadoras se pueden configurar de forma manual con una dirección IP.

2.4.8. FTP

El acrónimo de FTP es un protocolo de transferencia de ficheros (File Transfer Protocol) y es un software cliente/servidor que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP.

El funcionamiento es sencillo. Una persona desde su ordenador invoca un programa cliente FTP para conectar con otro ordenador, que a su vez tiene instalado el programa servidor FTP. Una vez establecida la conexión y debidamente autenticado el usuario con su contraseña, se pueden empezar a intercambiar archivos de todo tipo con los privilegios designados.

Además de las direcciones IP, DHCP también proporciona información de configuración, sobre todo las direcciones IP de los locales de almacenamiento en caché de resolución de DNS.

2.4.9. Seguridad de la Información

Cuando se habla de seguridad de la información se está indicando que dicha información tiene una relevancia especial en un contexto determinado y que, hay que proteger. La seguridad de información de una empresa debe considerar las medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información, basándonos en las políticas ITIL del ministerio de salud Pública.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Existen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca por el camino. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Esto hace que los ataques sean más sofisticados y ello aumenta la complejidad de la solución, pero la esencia es la misma.

2.4.10. Firewall

Un firewall de filtrado de paquetes se implementa dentro del sistema operativo y funciona en las capas de transporte y red de la red IP. Protege el sistema realizando las decisiones de enrutamiento después

de filtrar los paquetes basándose en la información del encabezado del paquete IP. (Ziegler, Firewalls Linux, pag19)

Un firewall (llamado también "corta-fuego"), es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet). El firewall es un sistema que permite filtrar los paquetes de datos que andan por la red. Se trata de un "puente angosto" que filtra, al menos, el tráfico entre la red interna y externa. Un firewall puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.

Si el tráfico entrante o saliente cumple con una serie de Reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

Por lo tanto a partir de la definición podemos asegurar que con un firewall bien configurado podemos evitar intrusiones no deseadas en nuestra red y ordenador así como también bloquear cierto tipo de tráfico saliente de nuestro ordenador o nuestra red.

Un firewall proxy se suele implementar como aplicación independiente para cada servicio con el que se desea usar un proxy. Cada aplicación proxy aparece ante el servidor como el programa cliente y ante el cliente como el servidor real. (Ziegler, Firewalls Linux, pag19)

2.4.10.1. Funcionamiento de un sistema Firewall

Un sistema firewall contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (allow);
- Bloquear una conexión (deny);
- Redireccionar un pedido de conexión sin avisar al emisor (drop).

- El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la Entidad. Se distinguen **habitualmente dos tipos de políticas de seguridad que permiten:**

Únicamente las comunicaciones autorizadas explícitamente: "Todo lo que no es autorizado explícitamente está prohibido".

Impedir cualquier comunicación que fue explícitamente prohibida.

2.4.10.4. Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

- **Usuarios internos** con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
- **Usuarios externos** con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

CAPITULO III
METODOLOGÍA

3.1. Tipo y Diseño de la Investigación

La parte principal y fundamental de este capítulo, es la de realizar la propuesta para la implementación de un servidor Firewall para la protección de ataques externos y controlar el tráfico de la red interna para el uso de la web, además de un servidor de Archivos para el control interno y la confidencialidad de los archivos internos y de cada departamento del Centro de Salud San José de Ancón Tipo A del Cantón Santa Elena.

La metodología de investigación utiliza se plantea a continuación:

3.1.1. Investigación Exploratoria

Estas investigación, exigen del investigador una extraordinaria creatividad y capacidad de improvisación, ya que implica la ausencia de guías teóricas que faciliten la comprensión del tema de estudio, aparte de la incertidumbre respecto a los resultados que seguramente provocará. “son previsibles reacciones negativas tanto de los organismos que evalúan los proyectos de investigación como de los jurados examinadores, y el estudiante se expone a riesgos que en realidad no tiene por qué correr”. (Sabino, 1996, p.108).

Como se manifiesta en la cita según autor Sabino, esta parte de la investigación exige creatividad y la capacidad de improvisar mediante la investigación in situ, donde se tendrá una idea precisa del cual saber a qué problema nos enfrentamos y obtener la respectiva solución adecuada al caso.

Al utilizar la investigación exploratoria para el levantamiento de información del centro de salud y al ser un centro de salud nuevo, tanto en infraestructura como en ubicación, se procedió a realizar los

respectivos procedimientos y visualizar el entorno que presenta actualmente el Centro de Salud San José de Ancón Tipo A del Cantón Santa Elena.

Se recopilo la información necesaria y poder desarrollar el tema adecuado para la elaboración para del presente proyecto, donde se debió indagar e investigar acerca de las políticas de control de acceso web, políticas ITIL implementada por la Dirección Nacional de Tecnología de la Información. Actualmente el acceso web de todas las computadoras es libre, es decir tienen acceso a todo en la web sin restricción de acceso y sin control de navegación o filtrado de acceso web en cada área de este Centro de Salud. Debido de contar con una infraestructura tecnológica adecuada y poder aprovechar los recursos implementados mediante plataforma Linux aseguraría de un trabajo acorde bajo la misma plataforma, además de que la información de los archivos aún se comparten de la manera tradicional y se resguarda en cada computador personal de cada usuarios sin tener un lugar de almacenaje con las respectivas políticas de protección de la información confidencial de este Centro de Salud.

Una vez realizada la investigación exploratoria se puede detectar las falencias, necesidades y fortalezas de los campos de estudio en el Centro de Salud San José de Ancón Tipo A del Cantón Santa Elena. Al diagnosticar el problema podemos identificar que no existe un sistema de control de acceso web y un servidor de archivos que resguarde la información confidencial.

En el desarrollo de la parte de la etapa de diagnóstico del entorno, se emplearon los métodos empíricos, tales como la técnica de recopilación de información mediante entrevistas y la observación para poder hacer el trabajo de campo. Además de tener presente los datos investigados con anterioridad que son primordiales como referencia en el estudio del problema en el Centro de Salud San José de Ancón Tipo A del Cantón Santa Elena.

El haber analizado el diagnostico se puede reconocer como está estructurado en cableado interno y de la distribución de los equipos tecnológicos que forman parte de cada uno de los departamento, estudiar a profundidad el lugar donde se implementará el proyecto de tesis se observa las facilidades y recursos con el cual cuenta el Centro de Salud San José de Ancón Tipo A del Cantón Santa Elena.

Metodología de análisis

Realizado el respectivo análisis según las investigaciones realizadas con los responsables de la unidad de salud y dentro de los requisitos establecidos en las políticas para la ejecución de cualquier proyecto a implementar dentro de lo que es tecnología de la información, se procede a utilizar los métodos que serán descritos en el presente trabajo.

3.2. Población y Muestras

3.2.1. Población

En la siguiente investigación de población donde se desarrollará el trabajo está comprendida a los profesionales de la salud y personal administrativo que laboran en el Centro de Salud San José de Ancón Tipo A que se encuentra ubicado en la vía principal Ancón – Atahualpa, del cantón Santa Elena de la Provincia de Santa Elena.Ccomo se muestra la distribución en la tabla Nº1

3.2.2. Muestra

La muestra que se obtendrá del **Centro de Salud San José de Ancón Tipo A**, con la guía del distributivo según organigrama se cuenta con 20 personas la cual servirá como tamaño de la muestra para la implementación del proyecto de tesis.

Tabla Nº 1

Cuadro Distributivo de la Población

Distributivo de la Población	
Odontólogos	2
Conserje	2
Asistente de atención al usuario	1
Médico General	5
Auxiliar de Enfermería	1
Auxiliar de Laboratorio	1
Enfermera	2
Auxiliar de Farmacia	1
Obstetras	3
Químico Farmacéutico	1
Promotor Social	1
Total	20

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Departamento de Talento Humano

3.3. Características de la Población

La muestra de la Población está constituido por el Personal Médico y Administrativo del **Centro de Salud San José de Ancón Tipo A** del Cantón Santa Elena de la Provincia de Santa Elena.

3.4. Delimitación de la Población

El Centro de Salud San José de Ancón Tipo A cuenta con la distribución en su infraestructura de la siguiente forma:

Tabla Nº 2

Delimitación de la Población

Delimitación de la Población	
Departamentos	**Funcionarios**
Consultorio Médicos	4
Consultorio Odontológicos	2
Consultorio Obstétricos	3
Enfermería	3
Estadísticas	2
Sala de Reuniones	0
Laboratorio	1
Toma de Muestra	1
Farmacia	1
Dirección	1
Bodega	2
Total	20

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Departamento de Talento Humano

3.5. Tipo de muestra

Dentro de la población establecida en el **Centro de Salud San José de Ancón** forma parte del muestreo, para poder establecer la información verídica con el único fin de mejorar la planeación y control del al momento de la investigación.

Para el Centro de Salud se tomara de una manera aleatoria para asegurar la variedad de criterios por cada una de las áreas elegidas.

3.6. Tamaño de la Muestra

Realizada previamente la explicación de la delimitación de la población, esta se rige a un solo tipo de muestreo la misma que se basa en la cantidad de médicos Profesionales y Personal Administrativo donde aplicaremos la siguiente fórmula para el cálculo del muestreo de la población:

$$n = \frac{m}{e^2 (m-1)+1}$$

Donde:

m = Es el Tamaño de la Población (20)

e = Error máximo permitido para la media muestra, en este caso será un margen de error de 0.06

n = Es el tamaño de la muestra

n = 19

3.7. Técnicas e Instrumentos de Recolección de Datos

La técnica de la recopilación de datos y el análisis de la implementación de un servidor firewall para filtrado web y servidor de archivos fueron la observación directa y la entrevista con la parte responsable del proceso tecnológico y la máxima autoridad de la Dirección Distrital, a quien está sujeta como ente rector del Centro de Salud San José de Ancón Tipo A del cantón Santa Elena.

Cada una de las técnicas a utilizar en el proceso de investigación científica es indispensable, ya que estos ayudarían a integrar una estructura con los que podamos obtener datos cuantitativos y cualitativos.

Esto además nos ayudara a tener la recopilación de información necesaria, con las personas responsables de llevar cada uno de los procesos, además de verificar cada una de las políticas establecida dentro del proceso informático de un Centro de Salud Tipo A, a

continuación se detalla los instrumentos de la investigación que se utilizaran:

Entrevista: Es una de las técnicas de la Investigación para la recopilación de la información mediante la cual se realiza un cuestionario previamente elaborados con las variables de la investigación, lo que se puede a obtener la opinión y valoración de la selección de una muestra.

La ejecución de esta técnica se la realizo con la obtención de la información que se fundamentó con la Responsable Distrital de Tecnología de la Información de la Dirección Distrital e Salud de Santa Elena del Cantón Santa Elena a la Ing. Lorena Villon, la cual manifestó la información ampliamente con la información necesaria acerca del tema de investigación del proceso de filtrado web.

Además de la una entrevista con el Dr. Edgar Rodríguez Tenempaguay, médico responsable del Cetro de Salud San José de Ancón Tipo A, donde manifestó la ampliamente las necesidades en cuanto a la parte tecnológica y de cómo su personal usa los equipo y el tiempo que ellos ocupa en distracciones que llevan a la acumulación de trabajo.

Encuesta: La parte de la encuesta no aplica debido a que es una implementación dentro de un área establecida para funcionarios de un centro de salud.

Observación: Esta técnica consiste en observar atentamente el proceso al cual se maneja actualmente dentro del sistema de red interno y del acceso web, además de la custodia de los archivos internos de la institución.

En el actual proyecto investigativo se utilizó la técnica de la Observación directa para cumplir con la visión de la investigación sobre los hechos relacionados con el problema actual analizado el cual me permito tener una idea clara acerca del acceso web.

- Todas las computadoras tienen acceso web sin restricción.
- La distracción por el acceso a las redes sociales y demás páginas web que causan distracción al funcionario.
- No se tiene un control de descargar y la cantidad de paquetes utilizados por cada usuario
- Los documentos son almacenados en cada una de las computadoras sin un resguardo con protección de la información confidencial

3.8. Instrumentos de la Investigación

Para la precisión del uso de los instrumentos de investigación para la elaboración de tesis son:

Registro de Observación: Durante la visita al Centro de Salud San José de Ancón Tipo A del cantón Santa Elena, se pudo conocer de manera directa de todos los argumentos necesarios para el estudio de la problemática en el Centro de Salud, se pudo observar todo el proceso interno de cada uno de los servicios prestados y cada una de las funciones realizadas por cada uno de los funcionarios y de la cantidad de información que almacenan en cada computador, además de considerar que pondrá en funcionamiento el Sistema Hospitalario SAIS (Sistema de Atención Integral de Salud) que consiste en agendamiento, consulta externa, laboratorio, farmacia, bodega y odontología. Actividades de prestación de servicio en el centro de salud para la atención al usuario de la localidad.

3.8.1. Procedimiento de la Investigación

3.8.1.1. Procedimiento

El procedimiento que se realizó para la investigación fue el siguiente:

- **Primero:** Se envió una carta de permiso al responsable Distrital en Tecnología de la Comunicación para poder realizar la respectiva investigación de cómo se maneja la infraestructura tecnológica y el tráfico de la red.
- **Segundo:** Se procedió a Visitar las instalaciones del Centro de Salud San José de Ancón Tipo A, concedido el permiso necesario patra realizar el análisis respectivo y recopilación de la información necesaria.
- Se definió el objetivo principal para el estudio y la ejecución del proyecto de tesis a realizar en el Centro de Salud.
- Se eligieron diferentes técnicas a emplear para la recopilación de datos como son la observación directa y entrevistas directas con los responsables del área a ejecutar el proyecto.
- Se analizaron los diferentes tipos de información recopilados y luego se procedió a realizar la propuesta en base al problema actual del centro de salud.

Durante este procedimiento de investigación se encontró lo siguiente:

- **Lentitud de acceso al servicio web:** Los funcionarios realizan sus procesos de acceso web del proyecto Sisalud que consiste de consultas online y mientras existan descargas de otros paquetes donde utilizan más recursos, hacen más lentos los servicios de navegación. El personal Administrativo y medico realizan actividades adicionales tales como el registro de información y recopilación de matrices de trabajos diarios necesitan que los servicios web trabajen de manera efectiva y rápida. Debido a la falta de automatización en los procesos de la comunicación, debido al escaso aprovechamiento de los recursos informáticos existentes en el Centro de Salud.

3.9. Análisis de Factibilidad

Institucional Administrativa: Una vez realizada la respectiva recopilación de información se procede a presentar la propuesta de trabajo y a brindar la solución a los inconvenientes que se pueden suscitar durante la apertura del servicio de internet de los diferentes departamentos, por lo que nos enfocaremos básicamente en dos aspectos: Utilización correcta de los recursos y no exponer la información y que siempre este protegida.

Financiera: El esquema económico para la implementación del servidor web y servidor de archivos, cumplen con características comunes considerando costos no muy elevados para mantener una red necesaria cumpliendo normas y políticas.

Mercado: Actualmente en el mercado local e internacional la migración a sistemas operativos libres, se los consideran como un ahorro considerable de los sistemas informáticos y mejor manejo de los recursos. Con la optimización de recursos evitando la compra de licencias de los servidores, en el mercado nacional el uso de software libre es usado para diferentes proyectos como telefonía, sistemas de seguridad, software entre otros que abarcan en su mayoría de las empresas privadas y más aún obligatorias en las públicas.

Tecnología: La forma de Interactuar con cualquier sistema operativo, mucho mejor con software libre deja entendido un alto nivel de protección y libre de amenazas externas. Lo que se propone es la implementación de un servidor que registre todos los procedimientos realizados de un computador desde su ip local, donde los registros quedaran almacenados en un Log de información.

3.10. Resultados de la Entrevista

Una vez realizadas las entrevistas con el Director del Centro de Salud y la Responsable de Tecnología de la Dirección Distrital conlleva a obtener las necesidades del centro de salud en cuanto a los parámetros a seguir para que el centro de salud goce de los requisitos mínimos para el proceso tecnológico en políticas de seguridad en el acceso Web.

3.10.1. Entrevista con la Ing. Lorena Villon

Existen muchas necesidades que se deben implementar dentro del proceso Tic, donde se incluyen políticas de seguridad no solo por un servidor de filtrado de contenido Web o un Servidor de Archivos, pero basándonos en el proceso el cual se prevé implementar en este proyecto son las de servidor Proxy y Servidor de Archivos obtenemos las informaciones necesarias detalladas a continuación:

- Debe existir un servidor proxy el cual deben tener políticas de acceso según la actividad de los departamentos y/o las funciones de cada funcionario.
- Además de un registro de equipo mediante la dirección física del equipo.
- El Servidor debe constar con clave que solo el personal informático tenga el acceso a los mismos.
- Los firewalls deben estar activados, para evitar la filtración de información o ataques exteriores.
- El servidor de archivos debe estar especificado por departamentos para la compartir archivos
- Los equipos informáticos de cada funcionario deberán cambiar de contraseña cada 30 días.

Como Tecnología de la Información existen un sinnúmero de actividades y políticas por aplicar pero, nos basaremos en la implementación de los Servidores Proxy y de Archivos.

3.10.2. Entrevista con el Dr. Edgar Rodríguez

En la entrevista realizada con el Director del centro de salud da a conocer cuáles son las problemáticas que existen actualmente en el centro de salud, tales como llegar a perjudicar al proceso tecnológico y las actividades cotidianas de los funcionarios del centro de salud.

Las claves de la red Wifi son fáciles de obtener, se filtra la información y cualquiera se puede conectar. Lo que provoca que existan muchos jóvenes alrededor del centro de salud conectado al a red, esto provoca que el internet se vuelva lento y pesado recalcando que los funcionarios cumplen carios procesos que deben estar cargados vías online por el ministerio de salud pública.

Las distracciones que provoca a los médicos debido a que tienen libre acceso de información en la Web.

Cuando se habla de los problemas que ocasiona compartir archivos de forma empírica ya sea este por una memoria extraíble, surge el asunto de la contaminación de los pen drivers e incluso la perdida de información provocada por los virus, entro otros asuntos de los cuales solo nos enfocamos a lo que se realiza en este proyecto.

3.11. Resultado Observados

Dentro del proceso de observación, luego del recorrido y las entrevistas necesarias podemos observar cómo se encuentra el centro de salud en la infraestructura tecnológica. Cabe recalcar que el centro de salud es nuevo., motivo por el cual, una vez conocidos los resultados podemos concluir con lo siguiente:

- La infraestructura en cuanto a cableado estructurado, cuenta con cableado categoría 6 y un cableado de VozIp, cumpliendo con las normas establecidas.
- Se cuenta con un rack en el departamento de Tic´s, con 1 switch de 24 Puertos, de los cuales hay disponibilidad de 3 puntos.
- Cuenta con una zona Inalámbrica libre.
- Cuenta con un servidor de VozIp con 5 teléfonos de comunicación interna.
- Cuenta con equipos informáticos completamente nuevos.
- La necesidad de instalar un servidor Proxy.
- La necesidad de instalar un servidor de Archivos en la nube.

3.12. Problemática

En las observaciones realizadas durante la investigación en situ, se encontraron varios problemas de los cuales provocan efectos que repercuten en las actividades de los funcionarios.

Tabla Nº 3

Causas y Efectos

	Causa (Problema)	Efectos
1	Libre Acceso a la Web.	Distracción de los funcionarios al poder ingresar libremente a cualquier contenido en la Web.
2	Libre Acceso a la Red Inalámbrica.	Al no existir un servidor proxy que haga los registros por una dirección Mac, cualquier equipo podrá conectarse sin restricciones.
3	Virus al pasar información por cualquier medio de almacenamiento.	Al pasar alguna información por medio de las unidades extraíbles, provoca daños y la infección de los equipos.
4	Saturación en las aplicaciones web del Ministerio	Los procesos de actualización de información tardan en subir, y funcionarios llevan su trabajo a continuar a casa, debido a que los recursos están siendo ocupado en otro tipo de descargas
5	Vulnerabilidad en los procesos internos.	Los archivos confidenciales que se usan dentro del centro de salud están expuestos a cualquier ataque exterior.

Fuente: Centro de Salud San José de Ancón.

Elaborado por: Luis Agualongo

3.13. Tecnología

3.13.1 Infraestructura Interna del Centro de Salud

El centro de salud San José Ancón Tipo A es un centro de salud que comienza su funcionamiento desde el mes de Febrero del 2016, por tal motivo su infraestructura tecnología es completamente nueva, consta de un cableado estructurado categoría 6, telefonía de VozIp, impresora multifunción de alto rendimiento y computadoras de quinta generación con procesadores Core i5.

Las computadoras todas en su totalidad cuentan con sistema operativo libre (Ubuntu), lo que facilitara el proceso de instalación deservidores bajo esta misma plataforma.

Cuenta con un cableado estructurado para equipos informáticos y junto a este un cableado de telefonía VozIp el cual sirve de comunicación interna.

3.13.2 Equipos Informáticos

En el centro de salud San José de Ancón tipo A, se cuenta con los siguientes equipos de trabajos y con el equipo informático que hará las veces de servidor proxy y de archivos.

Tabla Nº 4

Características de los Equipo/Servidor

Cantidad	Equipo/Marca	Características	Detalle
1	Server HP PROLIANT ML10	Procesador	Core i7
		Memoria	6 Gb
		Disco Duro	3 Tb
		Tarjeta de red integrada	10/100/1000
		Tarjeta de red Adicional PCI	10/100/1000

Fuente: Centro de Salud San José de Ancón.

Elaborado por: Luis Agualongo

Tabla Nº 5

Características de los Equipo/Estaciones

Cantidad	Equipo	Marca/Modelo	CARACTERISTICAS
15	CPU	Ari	Core i5, 2Gb Ram,500 DD
15	Monitor	Ari	20”
15	Mouse	Ari	
15	Teclado	Ari	

Fuente: Centro de Salud San José de Ancón.

Elaborado por: Luis Agualongo

3.13.3 Plataforma

La información que se ha obtenido y que está basada en la necesidad y la obligatoriedad que implica a para el Centro de Salud en base a políticas informáticas de hoy en día. Se trata de enfocarse en los puntos específicos que nos guiaran en ver el panorama del cual buscar la solución integral.

En el mercado actual existen un sinnúmero de servidores bajo la plataforma Linux que nos ayudaran a simplificar estos problemas, recordando el bajo costo que esto implica y de las asistencias técnicas inmediatas, debido a ser un sistema libre y de fácil uso no tanto así de fácil acceso por las seguridades más estrictas que en ellas existen

La distribución Linux que es elegida para la instalación de los servidores de red es Centos 6.5 siendo esta una versión estable, compatible para las infraestructuras i386 y x86_64.

Centos es una distribución de software libre, es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar, además de ser utilizado como entorno administrativo en redes, por diversos motivos como:

- Estabilidad
- Seguridad
- Actualizaciones
- Soporte para varios programas
- Manejo de paquetes
- Operatividad

Cabe recalcar que todo el sistema informático con el cual cuenta el centro de salud está bajo la plataforma Linux, lo que ayudara a una fácil interacción de los equipos al servidor

3.13.4. Programas Internos

Al hablar de un servidor Proxy, filtrado de contenido nos referimos específicamente de un Hardware que intercepta las conexiones de red desde un cliente proveedor hasta el servidor de destino, lo que hace es que intercepte cualquier navegación de páginas web restringidas ya sea por motivos de seguridad, rendimiento, anonimato o vulnerabilidad.

Para esto necesitaremos implementar varias líneas y comandos que permitirán ejecutar programas internos desde el Sistema Operativo centos y los cuales cumplirán funciones específicas que permitan tener un servidor proxy y un servidor de archivos.

Squid. Realizara funciones como servidor Intermediario y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras funciones específicas como filtración de contenido y control de acceso por IP y por usuario. Además de estas funciones hace de un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes.

Servicio DHCP. Este es en lenguaje común que permitirá que una computadora se configure automáticamente para poder conectarse a una red, esto está estableciendo por medio de un protocolo su IP, su máscara, su puerta de enlace, sus DNS entre otros.

Servicio FTP. Consiste en que nuestro Servidor Proxy tenga la posibilidad de que se conecte por FTP para realizar la transferencia de ficheros en nuestra red. Esto nos permite subir y descargar archivos, además de que funciona según el modelo cliente/servidor, cuando se recibe una petición esta la gestiona, establece la conexión y ejecuta las órdenes enviadas por el cliente.

Servicio Samba. Son directorios que obtienen los recursos para compartir a través de nuestra red. Estos recursos aparecen como carpetas normales dentro de nuestra red. Esto lo utilizaríamos en el caso de nuestro servidor Linux para montar archivos en la red como si fueran dispositivos locales.

Shorewall. Es una robusta y extensible herramienta de alto nivel que nos permite la configuración de muros cortafuego. Sólo se necesita definir algunos datos en algunos archivos de texto simple y éste creará las reglas de cortafuegos correspondientes a través de Iptables. Esta herramienta es un programa interno que de ser necesario por el administrador de sistema implementarla para definir reglas más explicitas del cortafuego o firewall.

Squidview. Es una herramienta que se usa en modo de línea de comandos para poder obtener los registros de navegación por dirección IP que pasan por el servidor proxy. De esta manera podemos observar páginas que aún no están en las listas de bloqueo dentro del squid. Esta se obtiene mediante reporte en tiempo real de navegación. Esta herramienta puede ser instalada y usada por el administrador de sistemas para revisar la navegación por IP.

Owncloud.- Es una aplicación de software libre usado para almacenamiento de archivos, conocido como la nube. Con esta aplicación instalada como servidor de archivo y es administrable se puede realizar varios procedimientos tales como: Creación de departamentos, capacidad de almacenamiento por departamentos, permisos para edición, entre otros.

CAPITULO IV
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1. Análisis de Requerimientos

Una vez realizado el respectivo análisis y de acuerdo a las características presentes en el centro de salud enfocaremos los requerimientos determinados.

4.1.1. Requerimiento del entorno

El entorno del servidor firewall y del servidor de archivo, se basa en la necesidad del actual del Centro de Salud. Los procesos que se realiza en el servidor son tales como:

- Filtrado de contenido
- Log de registro de navegación por IP
- Servidor en la nube Onwcloud.

4.1.2. Requerimientos funcionales

Se realizan los procedimientos que el servidor debe usar e implementar:

- El firewall debe cumplir con las políticas para controlar y supervisar el acceso web.
- La persona responsable del monitoreo y quien tenga acceso al servidor será únicamente el personal de tecnología.
- El servidor de archivos cumplirá con las funciones de compartir archivos según las áreas solicitantes con los permisos establecidos.

4.2 Implementación

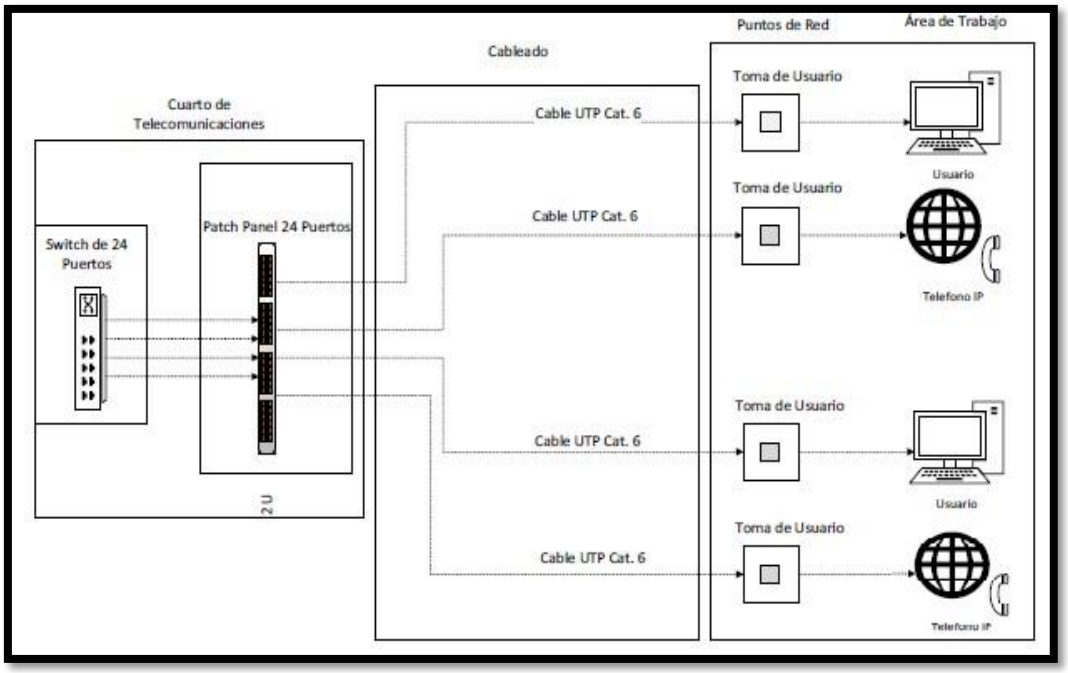
4.2.1. Redes

Para la implementación del Servidor Firewall y el Servidor de Archivos consideramos varios requerimientos que deben ser ubicado en la estructura interna de la red, además de mencionar que todo se encuentra instalada y cumpliendo con las normas establecidas en las políticas ITIL.

La categoría del cable con que cuenta el **Centro de Salud San José de Ancón Tipo A** es de categoría 6, está certificado para permitir velocidades de 1000 megabytes, cada punto de red cuenta con una toma para usuario y otra toma para telefonía IP.

Gráfico Nº 1

Diseño de la Red



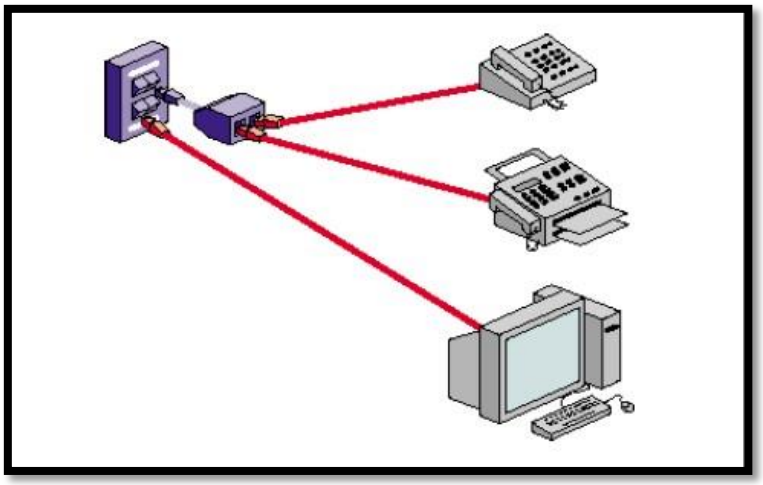
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

El tendido del cableado estructurado se encuentra dentro del centro de salud con cable UTP Cat. 6 siendo este uno de los cables que satisfacen la nueva tecnología y rapidez de la transmisión de datos. Las secciones de la red del centro de salud están formadas de las diferentes secciones ubicadas desde el cuarto de servidores hasta los departamentos en las estaciones de trabajo.

Gráfico Nº 2

Conexión de Voz y Datos

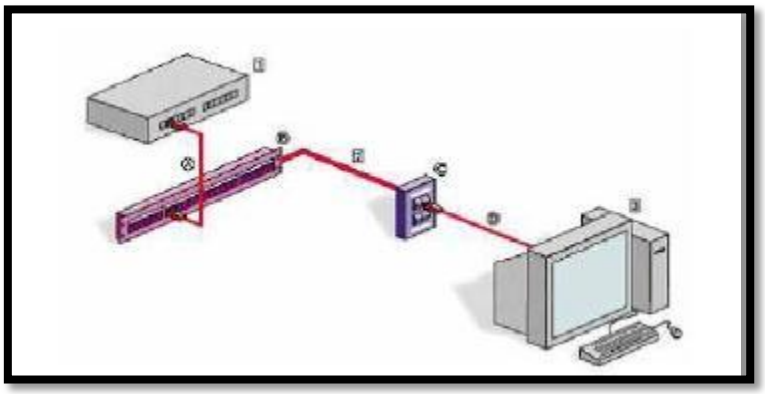


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 3

Conexión de Datos



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Rack de comunicaciones se encuentra actualmente ubicado dentro de la infraestructura de la red actual, con los componentes necesarios para empezar la red interna.

Gráfico Nº 4

Especificaciones del Rack

Descripción	Rack para redes pequeñas
Cantidad	1
Ubicación	Cuarto de servidores – TIC´S
Características	Rack pequeño para una red de 24 puntos
Componentes	Switch – Patch panel – Patch Cord – Servidor de VozIp- 21 puntos de Datos Habilitados

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Switch se encuentra ubicado dentro del rack de comunicaciones, esta conecta a la red desde los puntos de los usuarios en cada departamento con el servidor, de las cuales 21puertos están habilitados entre los puntos de voz y dato. Durante este proceso de implementación del trabajo no es necesario aumentar la cantidad de switch debido a que ya están establecidos en cada una de las estaciones de trabajo. Actualmente ya se encuentran ubicados en la red del centro de salud.

Gráfico Nº 5

Especificaciones del Switch

Descripción	Switch de 24 Puertos
Cantidad	1
Ubicación	Rack de Comunicaciones - Cuarto de servidores – TIC´S
Características	Switch ciscos administrables de 24 puntos
Componentes	Configurado los 21 puntos de red de voz y dato

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Patch panel se encuentra ubicado dentro del rack de comunicaciones, este recibe todos los cables del cableado estructurado además sirve como organizador de las conexiones de la red, este contiene los elementos relacionados de la red de área local (LAN) y de los equipos de conectividad para puedan ser fácilmente incorporados al sistema, y además los puertos de conexión de los equipos activos de la red como los switch y routers. Actualmente ya se encuentran ubicados en la red del centro de salud.

Gráfico Nº 6

Especificaciones del Patch Panel

Descripción	Patch Panel de 24 puertos
Cantidad	1
Ubicación	Rack de Comunicaciones - Cuarto de servidores – TIC´S
Características	Recibe todos los puntos de la red del cableado estructurado
Componentes	Los elementos relacionados a puntos de red, switch y routers

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Patch cord se encuentran ubicado dentro del rack de comunicaciones, es la conexión que se realiza entre el patch panel y el switch. También nos serve para la conexión entre los puntos habilitados en los departamentos y las computadoras para la comunicación de la red. Actualmente ya se encuentran ubicados en la red del centro de salud.

Gráfico Nº 7

Especificaciones de Patch Cord

Descripción	Patch Cord Cat. 6
Cantidad	4
Ubicación	Rack de Comunicaciones – Estaciones de trabajo
Características	Conexión entre los puntos red y las pc – conexión en el patch panel y switch
Componentes	Conectores Categoría 6

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Cajas Dobles y cajas simples se encuentran ubicadas en cada uno de los departamentos habilitando cada punto de red conectados dentro del rack, son cajas dobles por la conexión de voz y datos para cables de categoría 6. Actualmente son 19 puntos habilitados que se encuentran en cada uno de los departamentos del Centro de Salud.

Gráfico Nº 8

Especificaciones de Cajas Dobles

Descripción	Cajas Dobles
Cantidad	9
Ubicación	Estaciones de trabajo – Departamentos
Características	Conexión entre pc y puntos de red – conexión entre patch panel y switch
Componentes	Cajas de conexión de voz y datos

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 9

Especificaciones de Cajas Simples

Descripción	Cajas Simples
Cantidad	3
Ubicación	Estaciones de trabajo – Departamentos
Características	Conexión entre pc y puntos de red – conexión entre patch panel y switch
Componentes	Cajas de conexión de datos

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

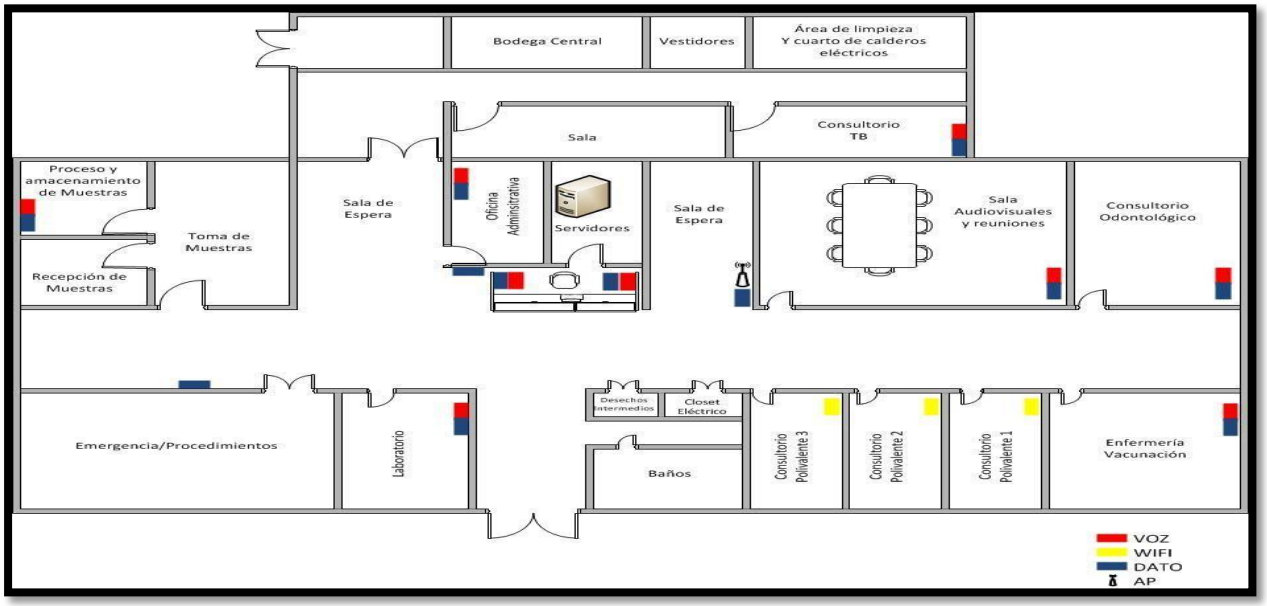
Elaborado por: Luis Agualongo

4.2.1.1. Diseño de la Red Interna

A continuación se muestra el diseño del cableado estructurado del Centro de Salud San José de Ancón Tipo A.

Gráfico Nº 10

Diseño del cableado Estructurado



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Los puntos rojos son los puntos de Voz, donde están conectados los teléfonos a la central IP, conectados para la comunicación interna faltando la instalación de la línea telefónica para su funcionamiento total hacia llamadas externas.

Los puntos Azules es donde se ubican los equipos Informáticos como Impresoras y computadoras, que conectan directamente con los switch que son quienes pasan la información hacia el servidor que se instale en el cuarto de servidores.

Los puntos amarillos son lugar donde no existe un punto físico de red, pero está conectada una computadora con conexión inalámbrica proveída desde un Access Point.

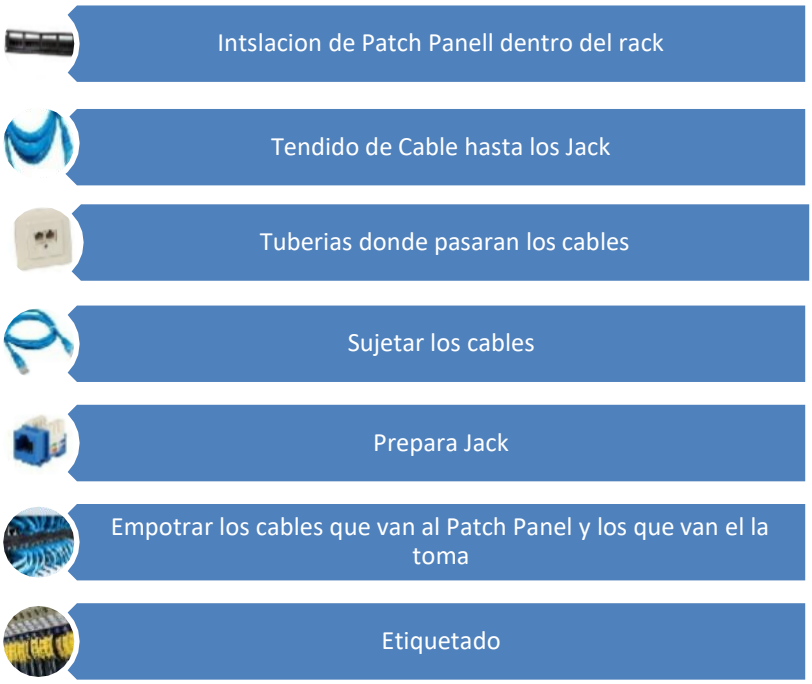
La antena AP (Access Point), indica la instalación de un punto de red Inalámbrico que cubre en su totalidad la parte central del centro de Salud.

4.2.1.2. Infraestructura de la red interna

Ahora presentamos el proceso con el cual se implementó el cableado estructurado desde realizado en el centro de salud.

Gráfico Nº 11

Proceso de implementación de Cableado Estructurado



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

El cableado estructurado tiene la capacidad de transmitir a alta velocidades los datos, el diseño se basa en la tecnología actual considerando la flexibilidad con respecto a los servicios y a la vida útil de la estructura de la red. La visión de esta red provee estandarización, rendimiento, integridad factibilidad y durabilidad.

Con la implementación del cableado estructurado se puede instalar varios servicios en la red tales como VozIp del cual ya cuenta el centro de salud y la instalación del servidor Proxy junto con el servidor de Archivos.

4.2.2. Servidores

Para realizar la implementación de un servidor proxy que nos permitirá filtrar contenido y un servidor de archivos es necesario la implementación del sistema operativo bajo plataforma Unix/Linux:

4.2.2.1. Instalación y configuración de Centos 6.

Se procede a insertar el disco de instalación centos 6 y al esperar unos segundos nos aparece un cuadro de dialogo y presionamos la tecla enter, como se muestra en la Grafica Nº12 que es la primera línea de instalación. Esto hace que la instalación sea de modo gráfica.

Gráfico Nº 12

Modo de Instalación

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

La pantalla que se presenta a continuación, pregunta si quiere verificar el medio de instalación, como se muestra en la Grafica Nº13, si deseamos verificar seleccionamos “OK”, caso contrario “SKIP” para proceder con la instalación.

Gráfico Nº 13

Verificación de los medios de Instalación.

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Hacer clic en el botón “NEXT”, cuando aparezca la pantalla de Centos como se muestra en la Grafica Nº14.

Gráfico Nº 14

Inicio de Instalación

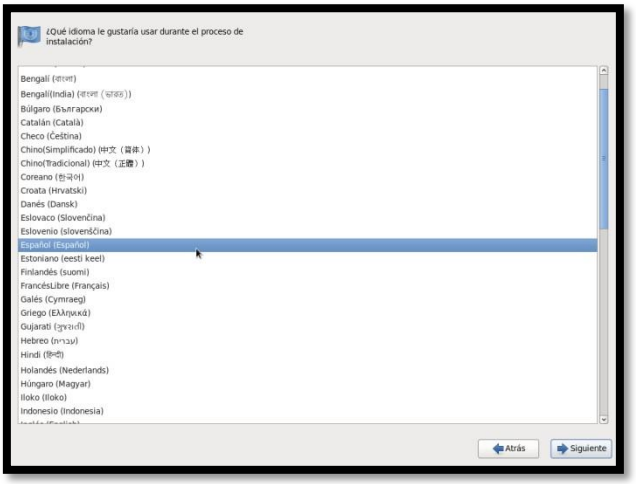
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Seleccionar el idioma que se usara durante la instalación, como se muestra en la Gráfica Nº15,

Gráfico Nº 15

Selección de Idioma



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

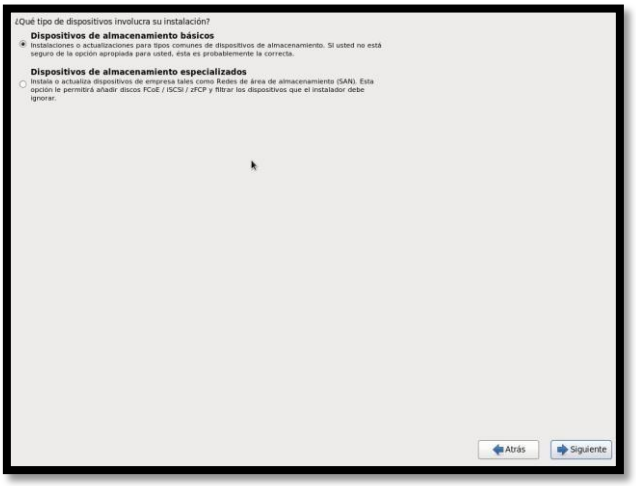
Elaborado por: Luis Agualongo

De la misma forma aparece la configuración del teclado lo que se recomienda es usar en Español.

Esta parte de la instalación nos permite realizar instalación sobre dispositivos especializados, y debido a que se dispone de un disco duro en el equipo se selecciona el almacenamiento básico, como se muestra en la Grafica Nº16.

Gráfico Nº 16

Dispositivo de almacenamiento



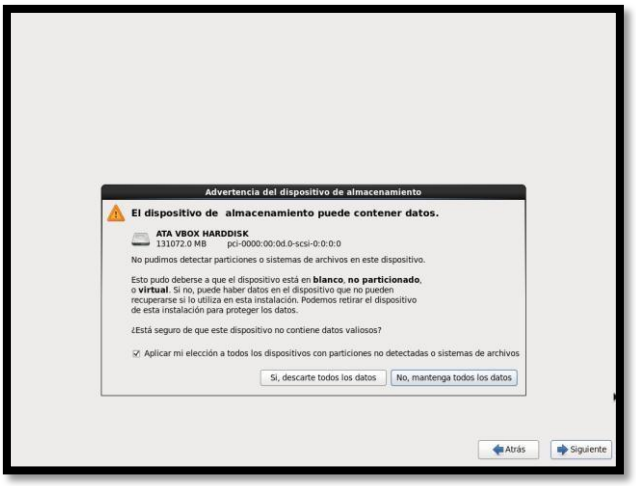
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Como se trata de una instalación completamente nueva sin particiones dentro de la unidad lógica, tendremos la advertencia con respecto a la unidad de almacenamiento que se debe inicializar todo o sobrescribir, como se muestra en la Grafica Nº17.

Gráfico Nº 17

Confirmación de Sobresctritura



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Definir el nombre anfitrión o el nombre de la red local en este caso “localhost.server”, como se muestra en la Grafica Nº18.

Gráfico Nº 18

Nombre del Hosts

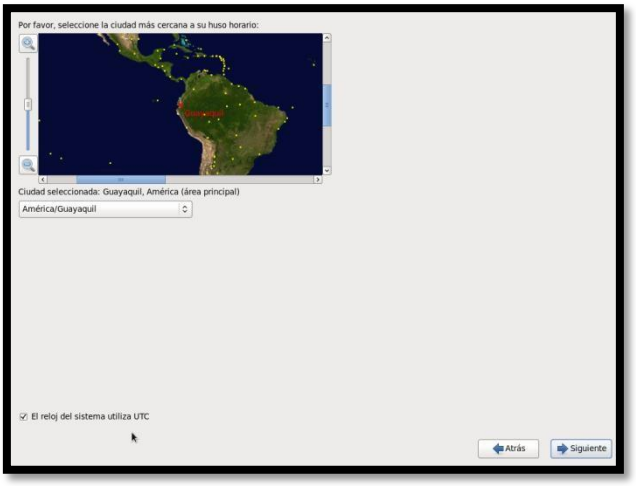
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se define la zona horaria haciendo un clic en el mapa, como se muestra en la Gráfica Nº19, esto sincroniza el tiempo que utiliza el servidor.

Gráfico Nº 19

Zona Horaria



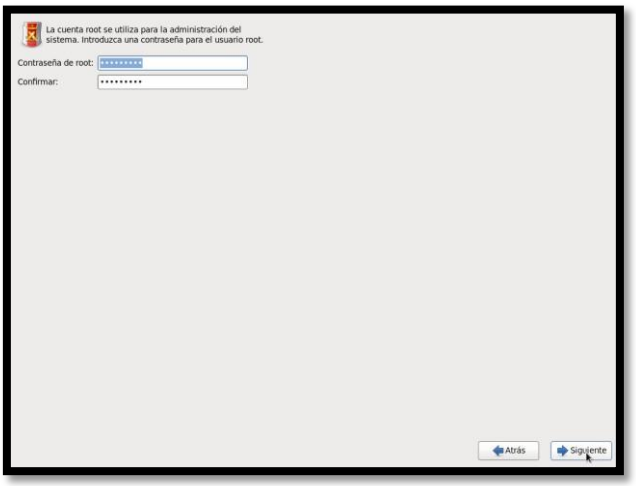
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se define la contraseña Root, la misma cuenta que es usada para la administración del sistema operativo y donde se levantan todos los servicios (como se muestra en la Gráfica Nº20.

Gráfico Nº 20

Contraseña Root



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

A continuación se realiza la creación de las particiones del disco duro, se puede crear un diseño personalizado o predeterminado el cual consiste de los siguientes parámetros:

- Una partición estándar de 200 MB (/boot)
- Un volumen lógico para /, permitirá hacer crecer el sistema añadiendo otro disco duro, con unidades físicas que se añadirán al volumen lógico.
- Un volumen lógico para la partición de memoria de intercambio (swap).

Las opciones de instalación en el disco duro son las siguientes según donde se va a instalar y la disponibilidad del Disco Duro se elige crear un diseño personalizado, como se muestra en la gráfica Nº21.

Gráfico Nº 21

Personalizar particiones

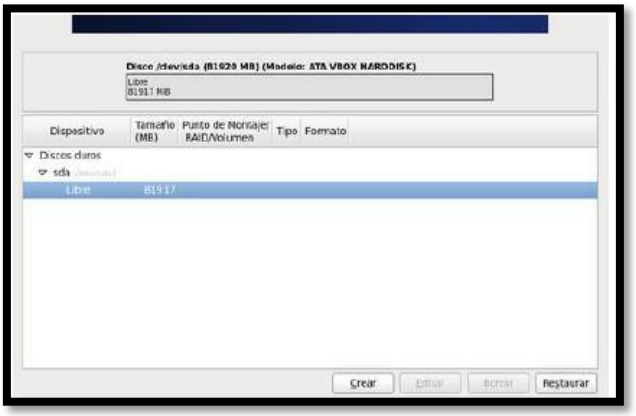
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez seleccionada se muestra las particiones actuales y los espacios libres donde se agregan las nuevas particiones las cuales son creadas a continuación como se muestra en la Grafica Nº22.

Gráfico Nº 22

Partición desde cero



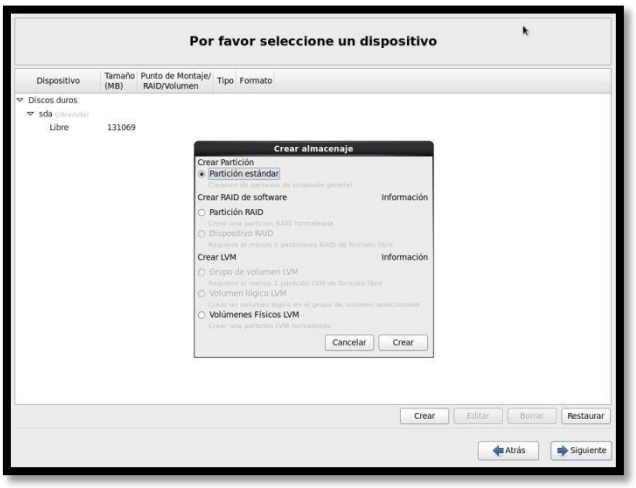
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se comienza a crear las particiones estándar dando clic en el botón “Crear”, creando las particiones antes mencionadas, como se muestran en las Gráficas Nº23.

Gráfico Nº 23

Crear partición



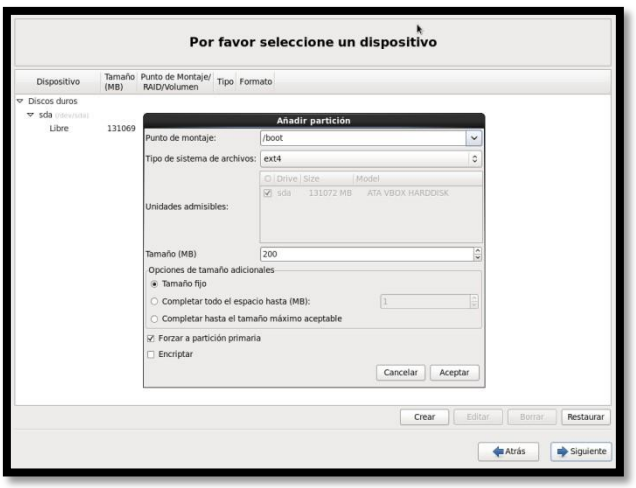
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

En la ventana que está encima de las particiones creamos la primera partición /boot como un punto de montaje con el formato ext4, de tamaño 200 MB y activando el casilla Forzar a Partición primaria.

Gráfico Nº 24

Partición /boot



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Como se muestra en la gráfica #, la creación de la nueva partición, y se vuelve a dar clic sobre el botón crear.

Gráfico Nº 25

Partición Creada /boot

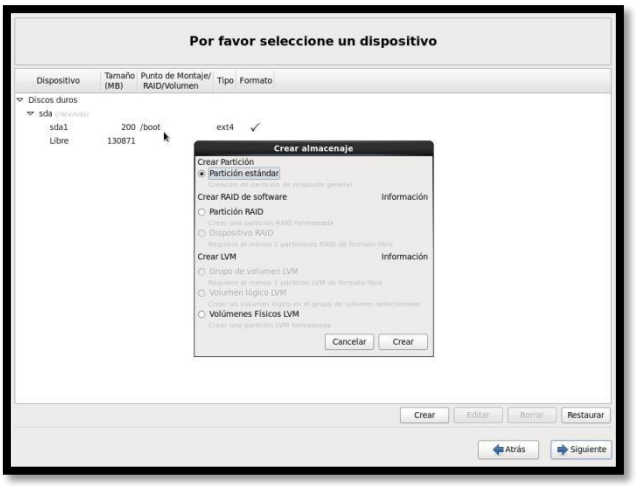
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se abre una nueva ventana para definir la siguiente partición el cual se escoge Partición Estándar como se muestra en la gráfica N26.

Gráfico Nº 26

Crear partición



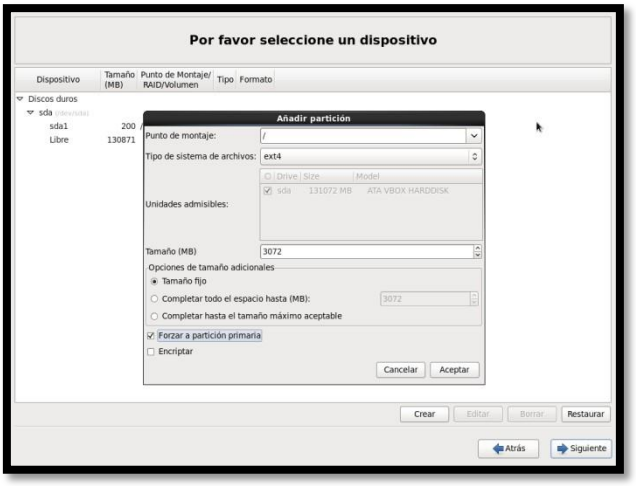
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

En esta ventana la partición que se creara de la define como / siendo este el punto de montaje, manteniendo la ext4 y con el tamaño de 3027 MB. De la misma forma se activa la casilla Forzar a partición primaria. Como se muestra en la gráfica Nº27.

Gráfico Nº 27

Partición /



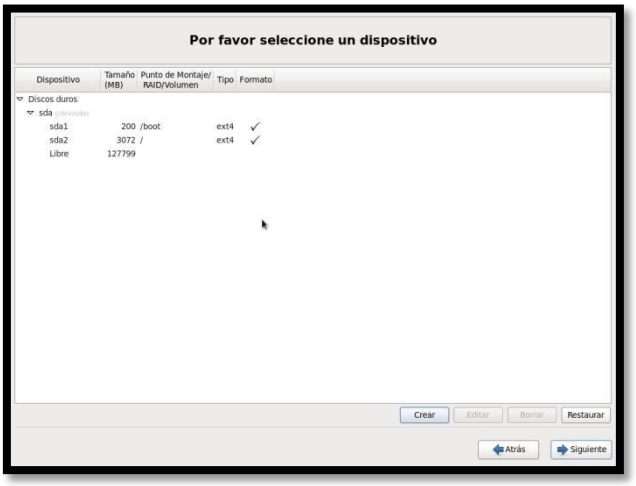
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Por lo que la pantalla como se muestra en la Gráfica Nº28, queda detallada las particiones hasta el momento creadas.

Gráfico Nº 28

Partición creada



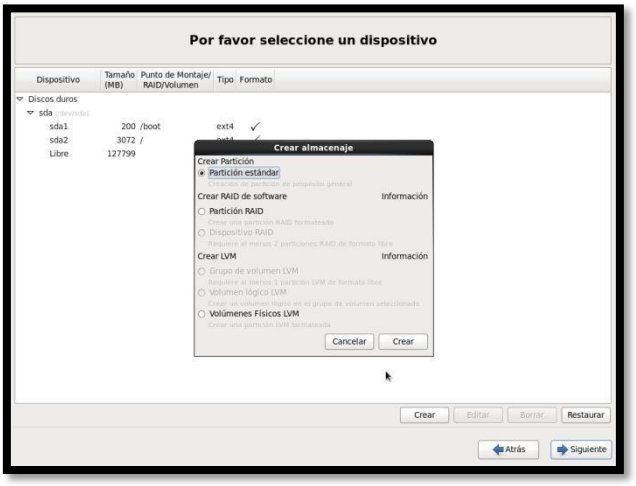
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Nuevamente seleccionamos crear y elegimos Partición Estándar. Como se muestra en la Gráfica N29.

Gráfico Nº 29

Crear partición



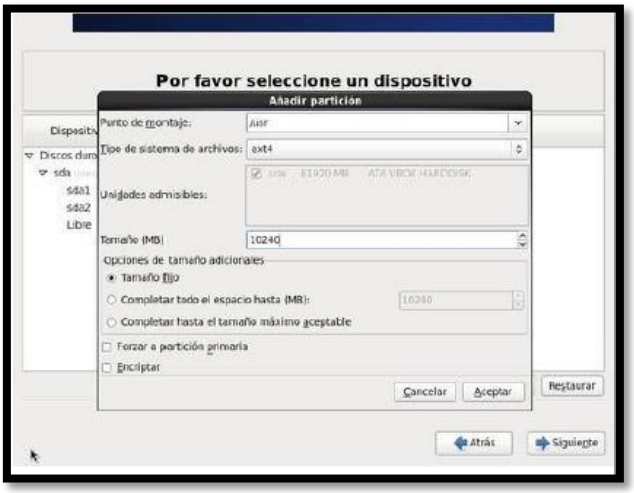
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

En esta nueva ventana se define /usr como punto de montaje que mantenga en formato ext4 y el tamaño de 10240 MB, como se muestra en a gráfica Nº30.

Gráfico Nº 30

Crear Partición /usr



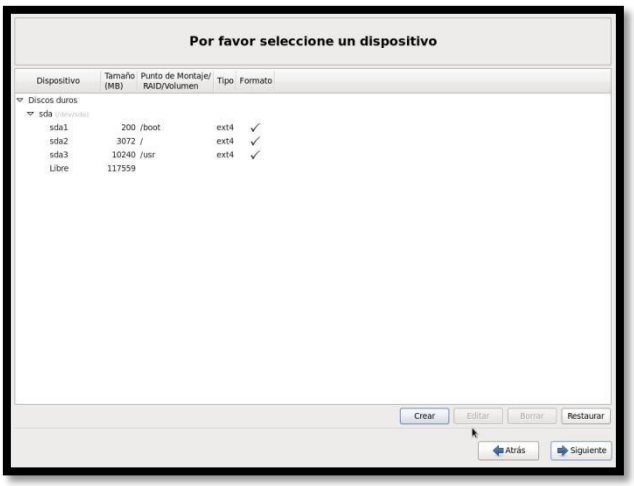
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se debe mostrar la tabla de particiones como se muestra en la Gráfica Nº31, con toda las particiones creadas hasta el momento.

Gráfico Nº 31

Partición creada



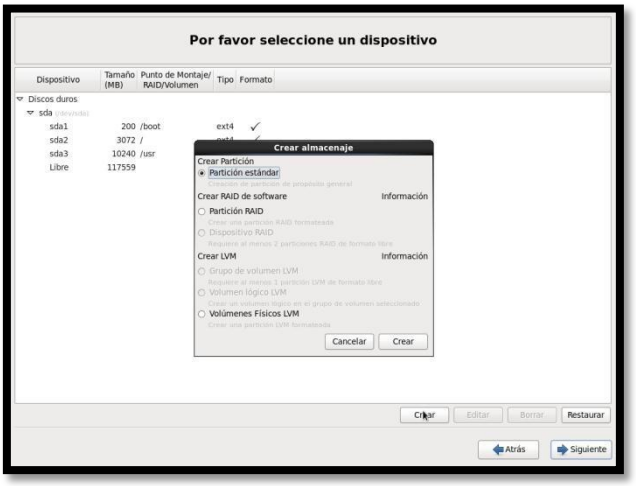
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

De la misma forma se vuelve a crear una nieva partición **estándar y crear,** como se muestra en la gráfica Nº32.

Gráfico Nº 32

Crear Partición



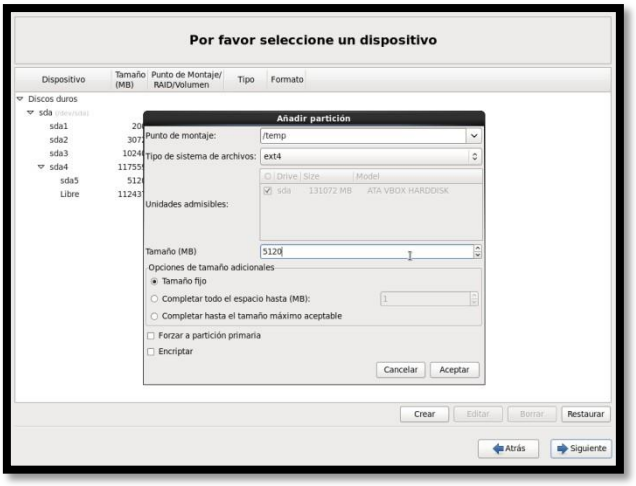
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez realizado el procedimiento anterior obtendremos la siguiente ventana como se muestra en la gráfica Nº33, donde se define la partición /tmp como punto de montaje, manteniendo la ext4 y el tamaño definido en 5120 MB.

Gráfico Nº 33

Crear Partición /tmp



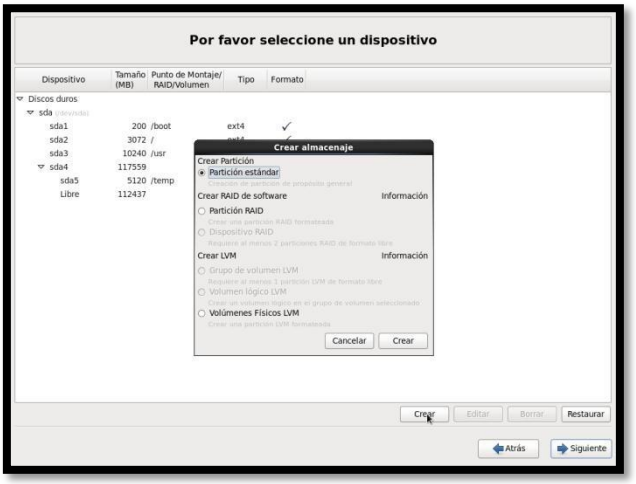
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se crear una nueva partición estándar y crear, como se muestra en la gráfica Nº34.

Gráfico Nº 34

Crear partición



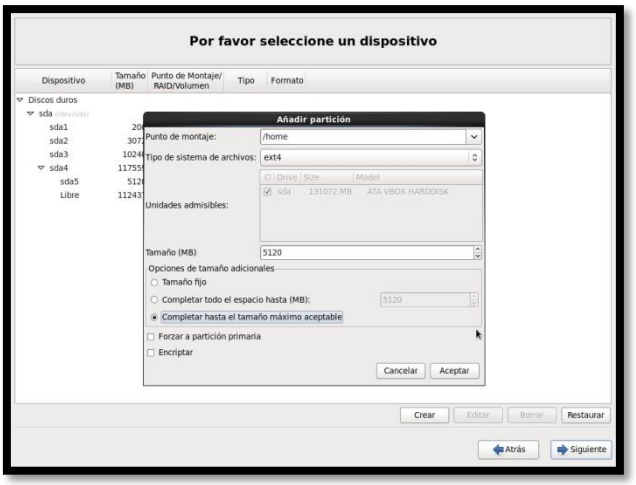
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se define la partición /home como punto de montaje, y activar el casilla **Completar hasta el tamaño máximo aceptable.**

Gráfico Nº 35

Crear partición /home



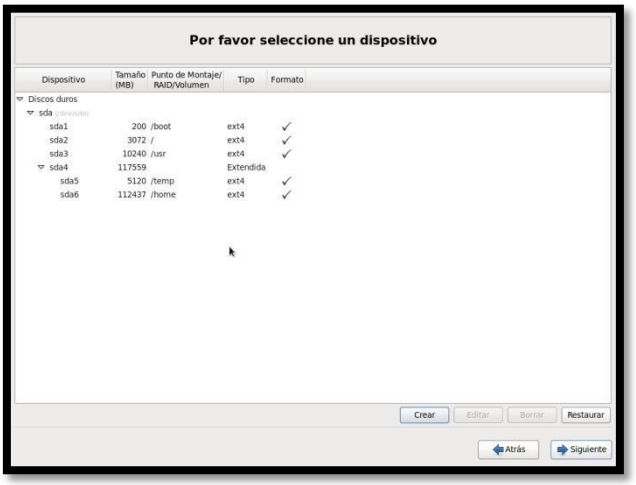
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo.

Tendremos como resultado lo mostrado en la gráfica #, donde aparecen todas las particiones creadas, /home temporalmente tiene todo el espacio asignado que se encuentra libre hasta la creación de la partición /var donde ambas se repartirán el espacio.

Gráfico Nº 36

Particiones creadas



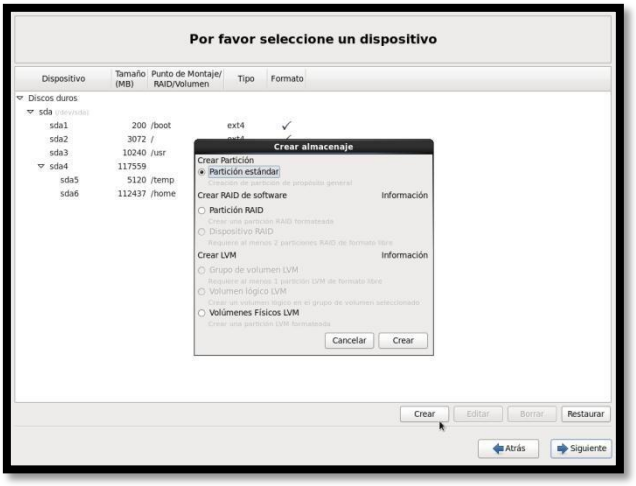
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

De la misma forma se vuelve a crear una nieva partición estándar y crear, como se muestra en la gráfica Nº37.

Gráfico Nº 37

Crear partición



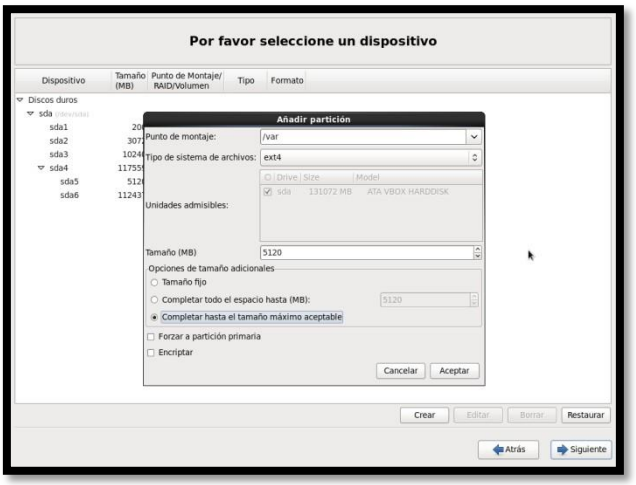
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Esta parte se define /var como punto de montaje, mantiene el formato ext4, además de elegir la casilla Completar hasta el tamaño máximo aceptable tal como se muestra en la gráfica Nº38.

Gráfico Nº 38

Crear partición /var



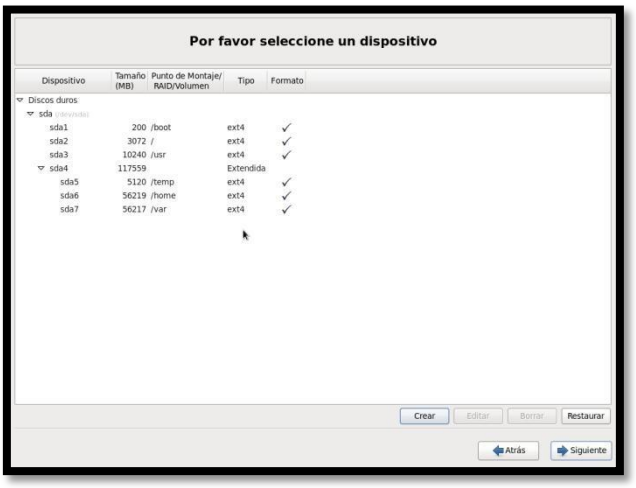
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Ahora se muestra la tabla de las particiones, donde /home y /var tienen los espacios disponibles repartidos como se muestra en la gráfica Nº39.

Gráfico Nº 39

Particiones creadas



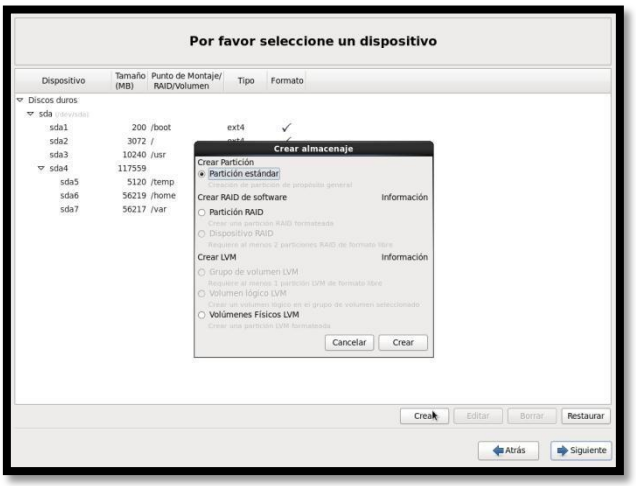
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

De la misma forma se vuelve a crear una nieva partición estándar y crear, como se muestra en la gráfica Nº40.

Gráfico Nº 40

Crear partición



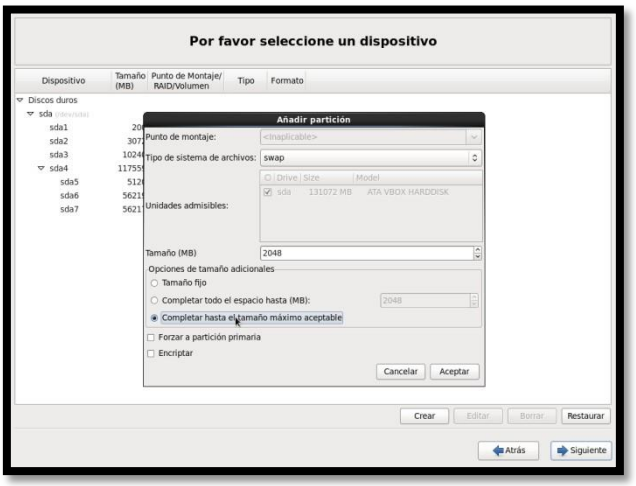
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Ahora se creara la partición Swap y el tamaño de 10240 MB, tal como se muestra en la figura Nº41

Gráfico Nº 41

Crear partición Swap



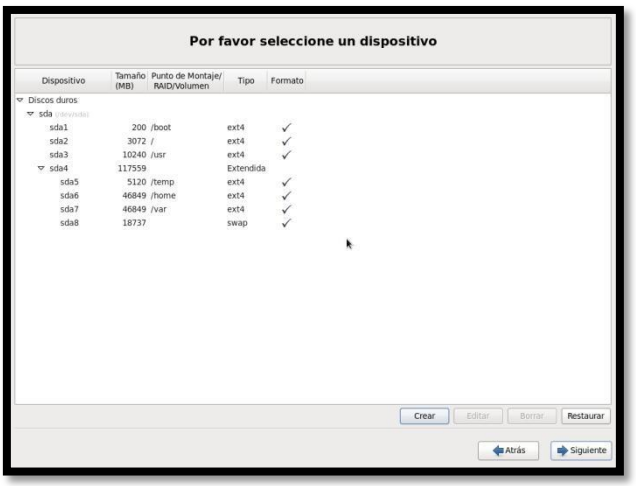
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Ahora se muestra la tabla de particiones asignadas entre /home y /var, y las demás particiones que se crearon en sus taños específicos para la correcta instalación del sistema operativo como se muestra en la gráfica Nº42.

Gráfico Nº 42

Particiones creadas



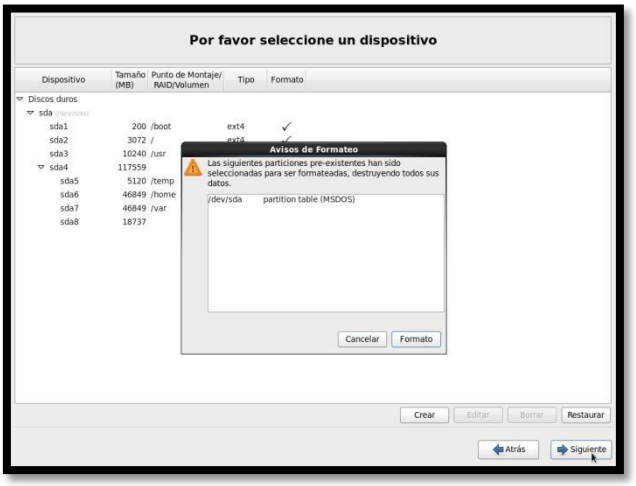
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez creadas las particiones continuamos con el proceso de instalación, en donde aparece un cuadro de aviso de formateo a las particiones existentes dando clic en Formato como se muestra en la gráfica Nº43.

Gráfico Nº 43

Inicio de formateo del Disco



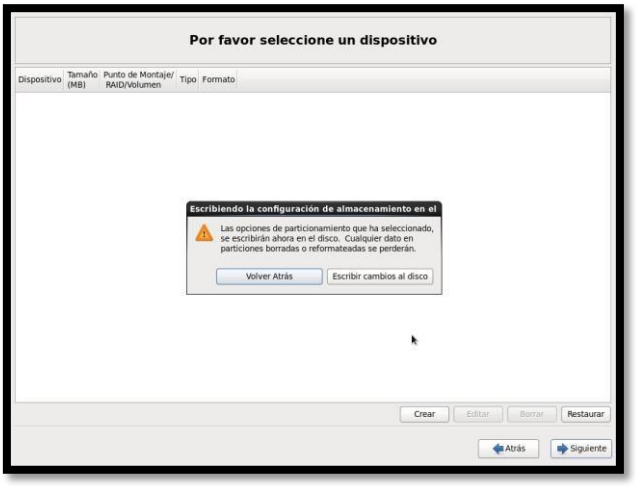
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se solicita la confirmación de los cambios que se está realizando en el Disco Duro, donde damos clic en Escribir cambios al disco duro como se muestra en la gráfica Nº44.

Gráfico Nº 44

Aplicar cambios



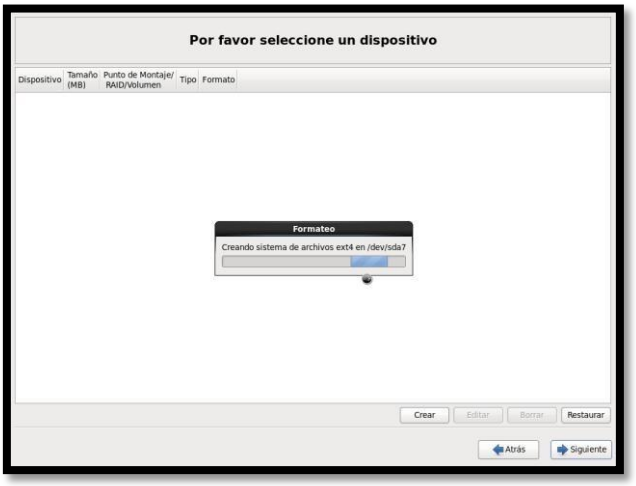
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Esperamos unos minutos mientras se guarda la tabla de las particiones como se muestra en la gráfica Nº45, obteniendo el formato definido anteriormente.

Gráfico Nº 45

Inicio de instalación



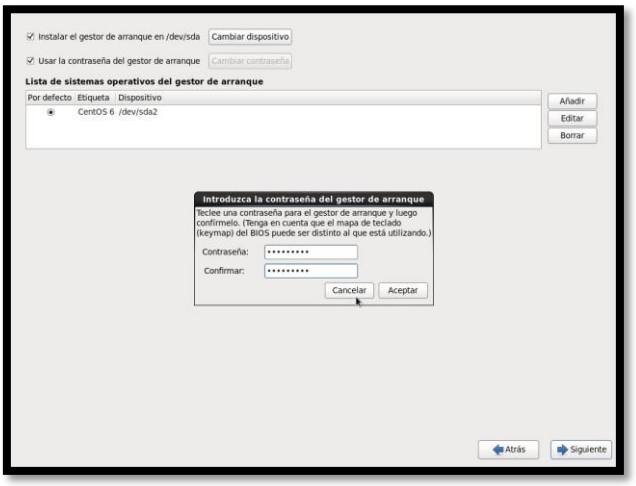
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Por seguridades es necesario asignar una contraseña al gestor de arranque, con la única finalidad de que cualquier acceso físico al sistema, pueda modificar los parámetros de arranque e iniciar en modo de mono-usuario. Por lo que se procede activar la opción Usar la contraseña para gestor de arranque, como se muestra en la gráfica Nº46.

Gráfico Nº 46

Contraseña al gestor de arranque



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Luego de dar siguiente, elegimos el tipo de instalación como se muestra en la gráfica Nº47.

Gráfico Nº 47

Instalación entrono gráfico

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

La configuración de las tarjetas de red se realiza una vez instalada el Sistema Operativo, comenzamos a iniciar el proceso de instalación de paquetes como se muestra en la gráfica Nº48. Es recomendable no realizar la instalación con conexión a internet, ya que esto tardaría bastante el proceso.

Gráfico Nº 48

Instalando centos

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez culminada la instalación la instalación se procede al reinicio del sistema para poder ingresar al entorno de escritorio de centos.

4.2.2.2. Instalación y configuración del Proxy

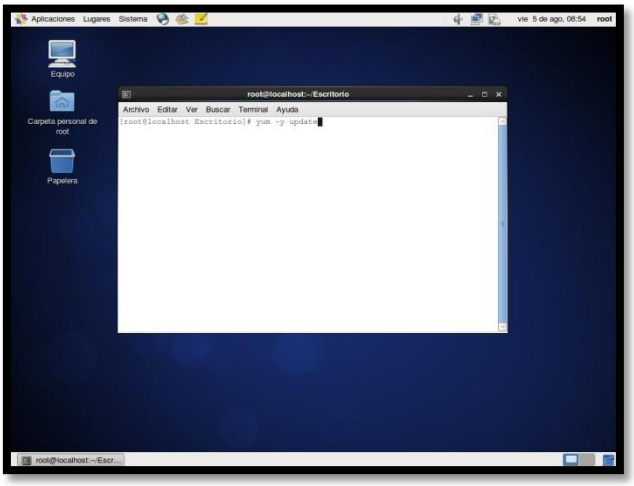
Los paquetes que se proceden a instalar para la implementación de los servicios y la configuración del servidor con los servicios a implementar.

Instalación de SQUID e Iptables. Se procede a realizar la ejecución de las líneas siguientes desde la terminal:

- #yum –y update
- #yum –y install squid httpd
- #yum –y install iptables

Gráfico Nº 49

Comando update

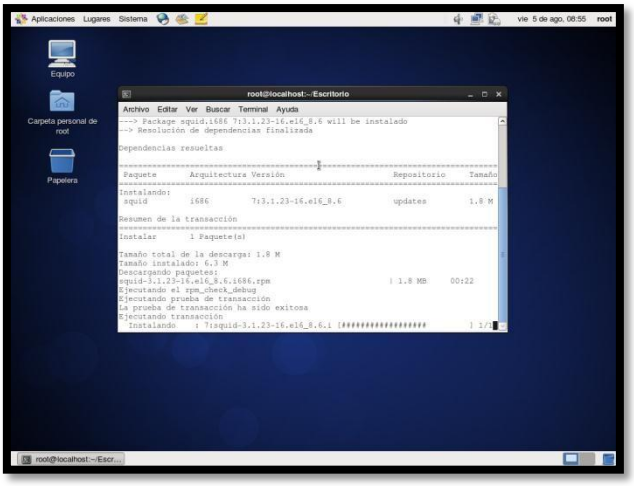


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 50

Descargando actualizaciones

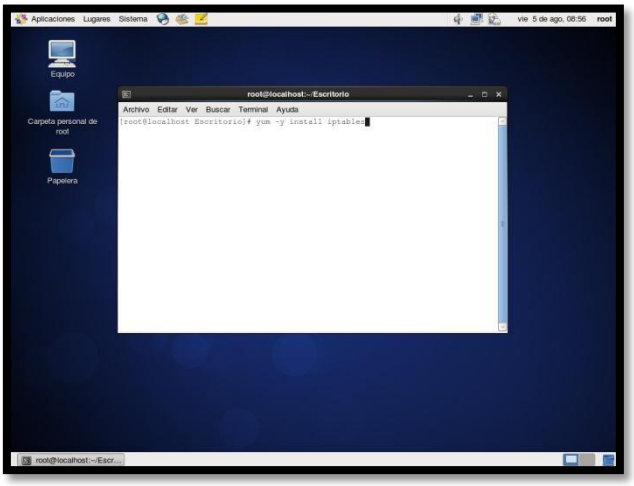


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 51

Instalación de Iptables

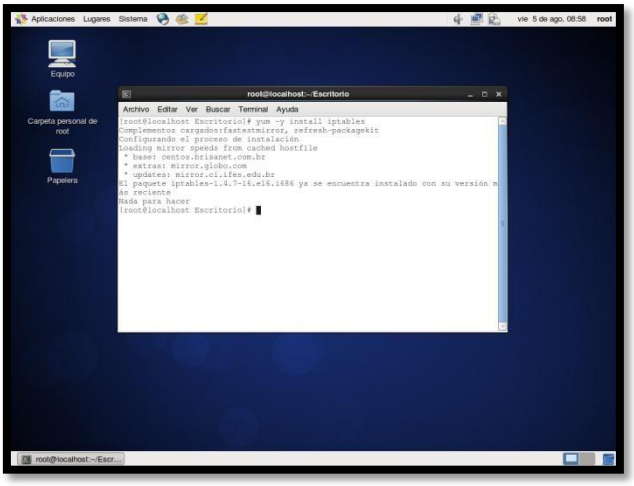


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 52

Aplicación instalada



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

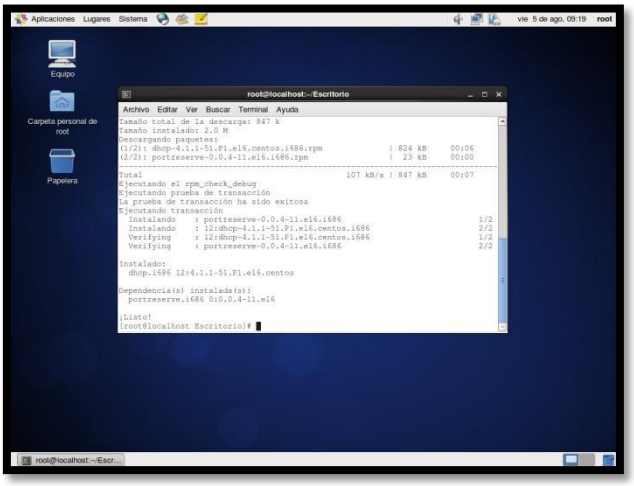
Elaborado por: Luis Agualongo

Instalación deservicio DHCP, al instalar este servicio el equipo servidor designara Ip automáticamente a los equipos conectados en la red, para esto agregamos las siguientes líneas desde la terminal:

- #yum –y install dhcp

Gráfico Nº 53

Instalación Dhcp



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

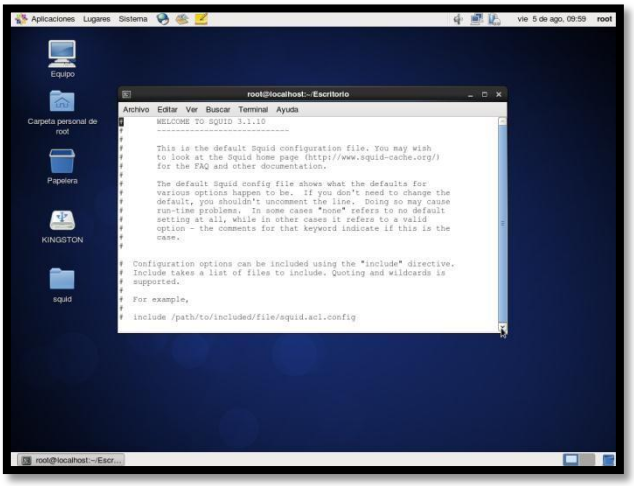
Elaborado por: Luis Agualongo

Configuración del Squid, realizar las configuraciones y asignar las reglas al servidor.

La primera opción es la configuración del archivo principal del Squid como se muestra en la gráfica Nº54.

Gráfico Nº 54

Configuración Squid

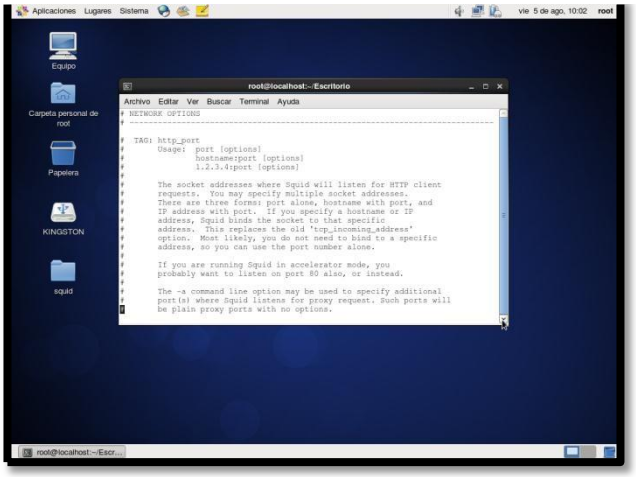


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 55

Configuración Squid



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

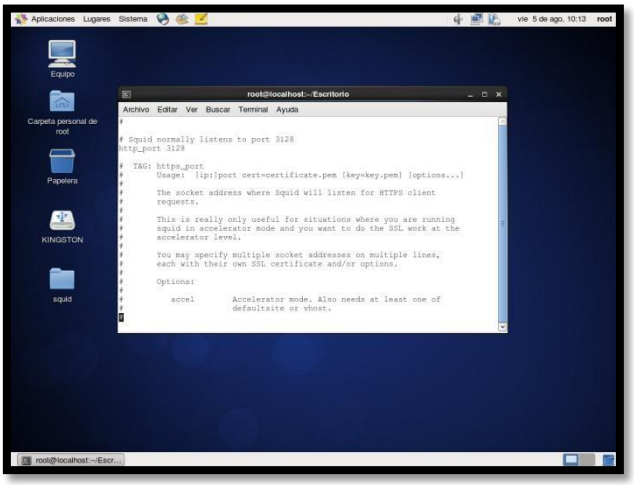
Elaborado por: Luis Agualongo

La configuración principal del Squid es bastante extensa y tiene muchas opciones de configuración según las políticas de las necesidades de la institución, donde se configura los principales parámetros:

- Establecer las direcciones y los puertos por el cual el Squid atenderá las peticiones.
- Establecer cuanto usara en la caché.
- Especificar en qué directorio se guardarán los registros logs del Squid.
- Determinar las líneas de control al acceso acl.
- Identificar los puertos de acceso.

Gráfico Nº 56

Aplicación de Políticas



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

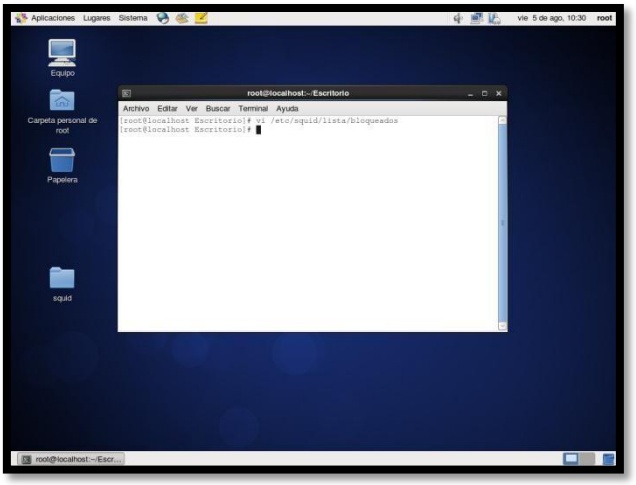
Creación de los archivos a ser denegados, una vez realizada la configuración principal del Squid cumpliendo con las políticas establecidas por el departamento de Tecnología de la Información se procede a crear los archivos para bloquear los sitios web, audios, emuladores, juegos, videos, músicas y televisión.

Creación de archivo para el bloque da páginas.

- #vi /etc/squid/lista/bloqueados

Gráfico Nº 57

Crear Carpeta de listas denegadas

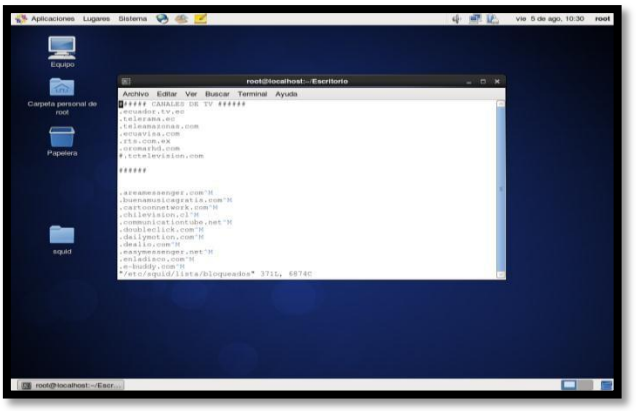


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 58

Lista denegadas



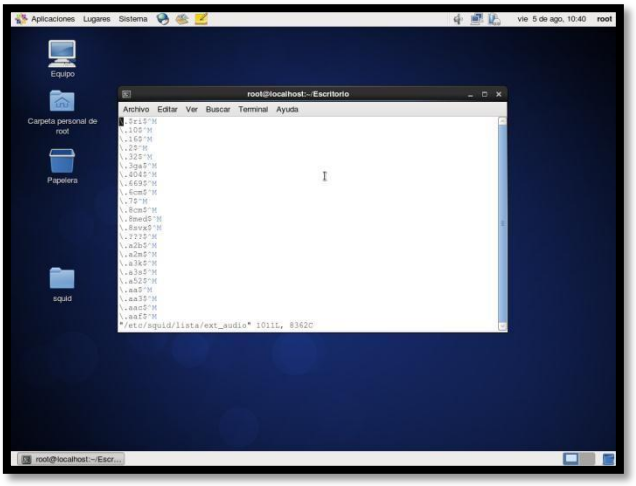
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ #vi /etc/squid/lista/ext_audio

Gráfico Nº 59

Lista de audios



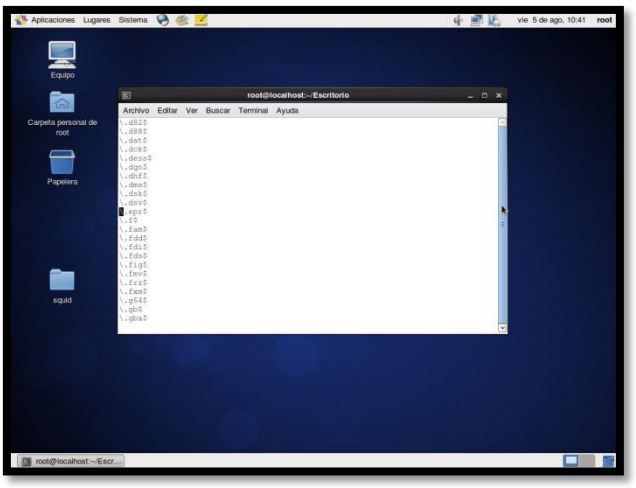
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ #vi /etc/squid/lista/ext_emulador

Gráfico Nº 60

Lista de emuladores



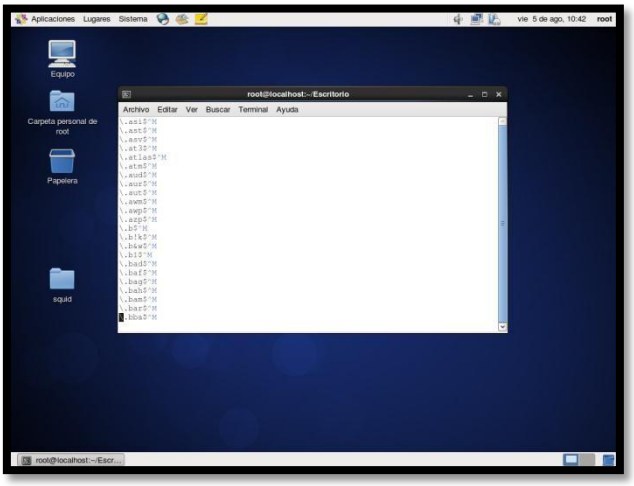
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ #vi /etc/squid/lista/ext_games

Gráfico Nº 61

Lista de juegos juegos



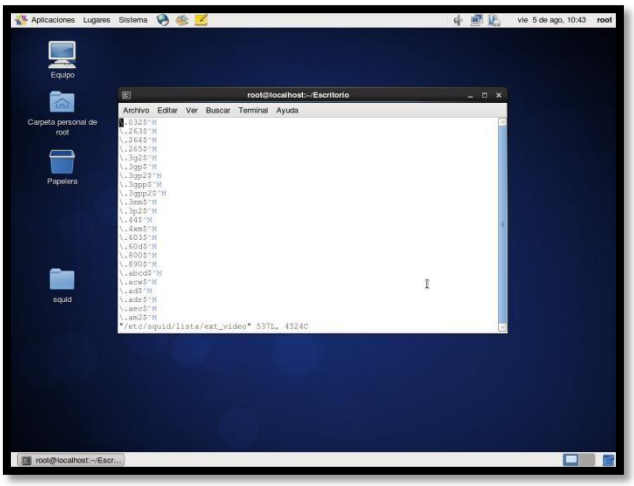
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- #vi /etc/squid/lista/ext_video

Gráfico Nº 62

Lista de formatos de video



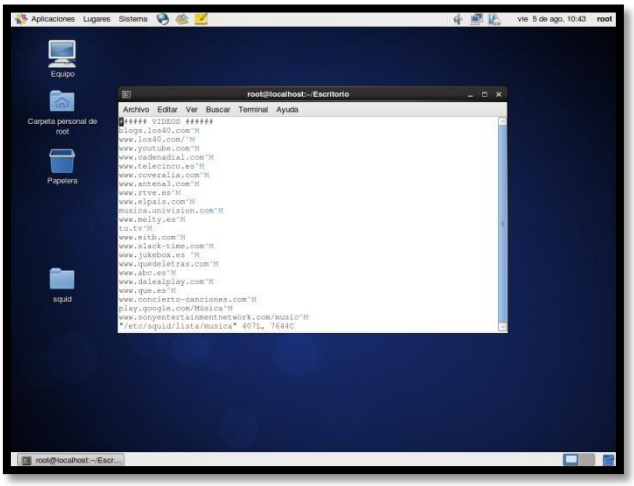
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- #vi /etc/squid/lista/música

Gráfico Nº 63

Lista de formatos de músicas



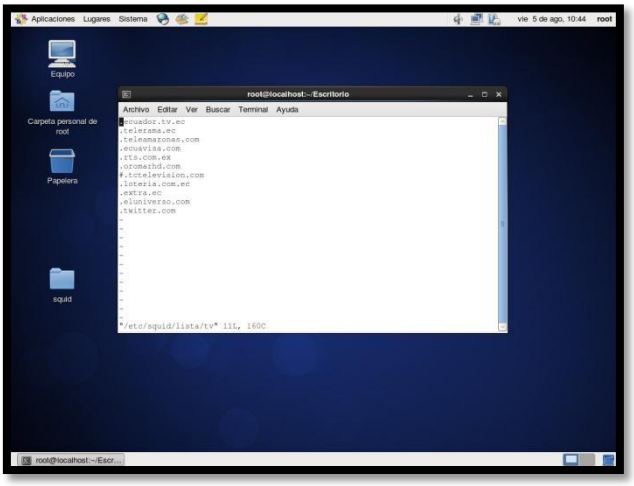
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- #vi /etc/squid/lista/tv

Gráfico Nº 64

Lista de páginas web de Tv



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

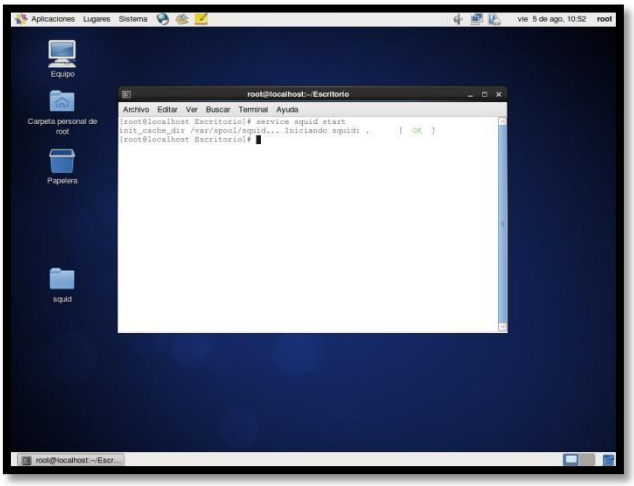
Elaborado por: Luis Agualongo

Ahora levantaremos los servicios para registrar los cambios realizados en el Squid con la línea:

- #service squid start

Gráfico Nº 65

Línea de inicio de squid

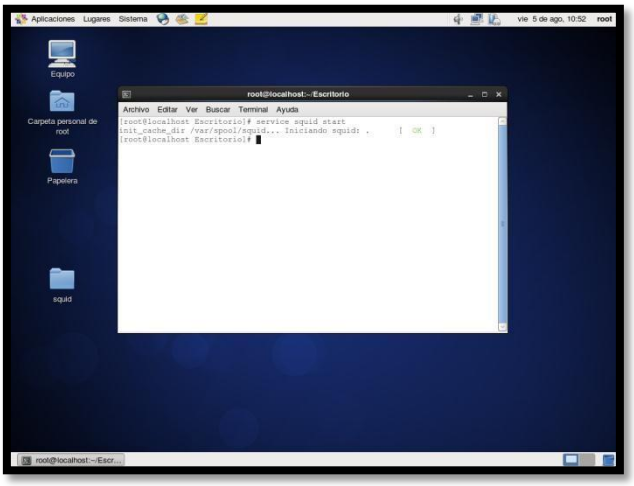


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 66

Squid ejecutado



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

4.2.2.3. Instalación de servidor de archivo en la nube (Owncloud)

Para la implementación de un servidor de archivo utilizamos Owncloud, que es un servidor que almacena la información en la nube. Este nos servirá para administrar y dar los permisos necesarios por cada departamento al que se le crea una cuenta y su administración.

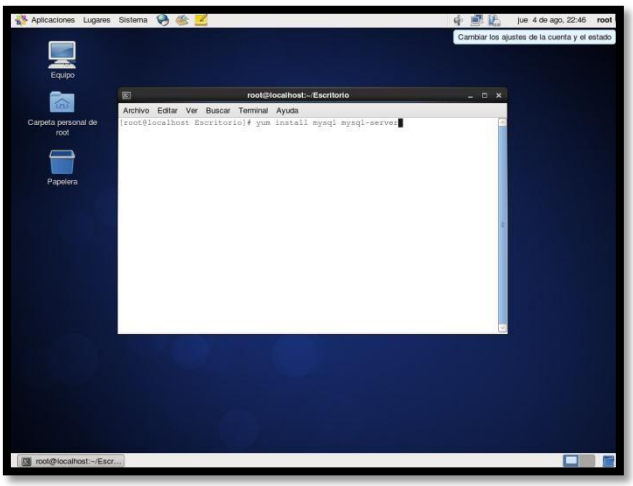
Para proceder con la instalación y configuración del Owncloud procederemos a realizar lo siguiente:

Abrimos la terminal y desde la terminal ejecutamos la instalación del SQL y los gestores de Mysql con la siguiente línea:

- #yum install mysql mysql-server

Gráfico Nº 67

Instalación de Mysql

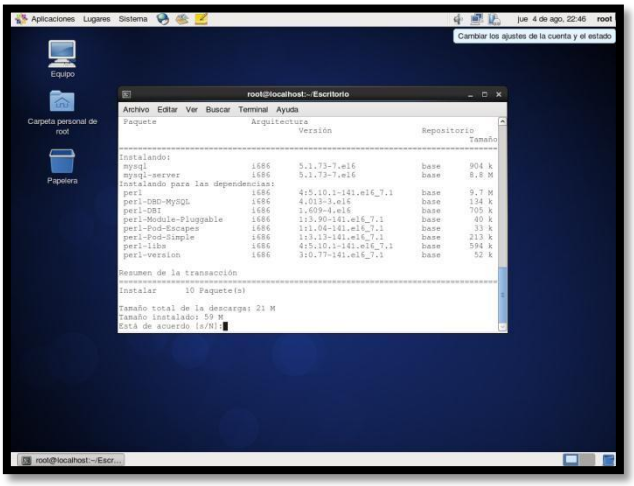


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 68

Descarga de Mysql



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

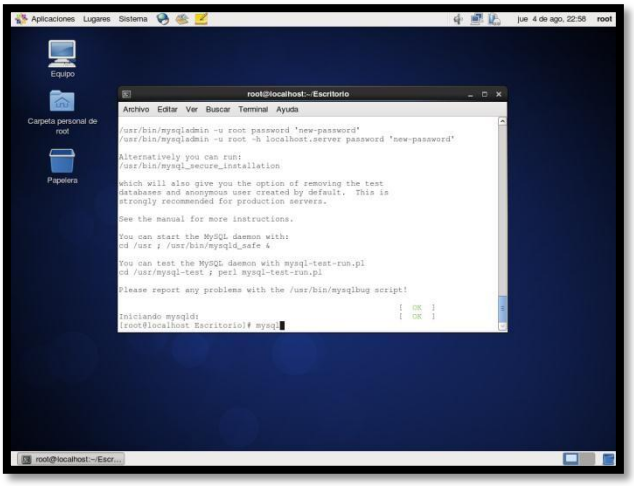
Elaborado por: Luis Agualongo

Levantamos los servicios del mysql con la siguiente línea

- #etc/init.d/mysqld start

Gráfico Nº 69

Inicio de Mysql



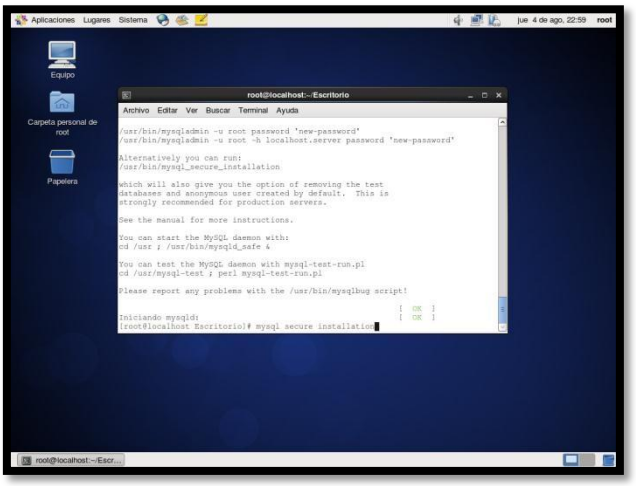
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- #mysql secure installation

Gráfico Nº 70

Instalación de permisos



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

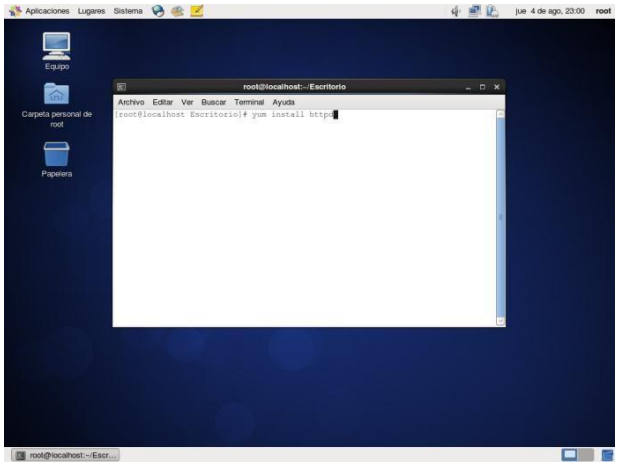
Elaborado por: Luis Agualongo

Ahora se procede a instalar el servicio httpd con la siguiente línea:

- #yum install httpd

Gráfico Nº 71

Instalación de servicio httpd



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

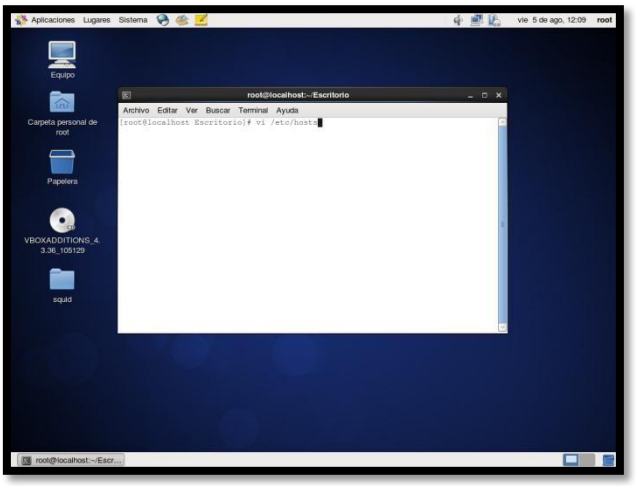
Elaborado por: Luis Agualongo

Para poder continuar debemos de hacer la implementación de una línea en el hosts añadiendo la línea del owncloud y la dirección ip donde tendrá acceso desde las otras computadoras en red.

- #vi /etc/hosts

Gráfico Nº 72

Configuración del hosts

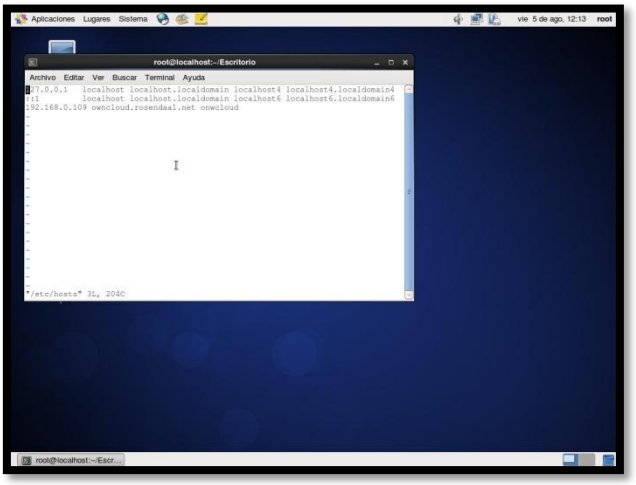


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 73

Aumento de línea para Owncloud



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

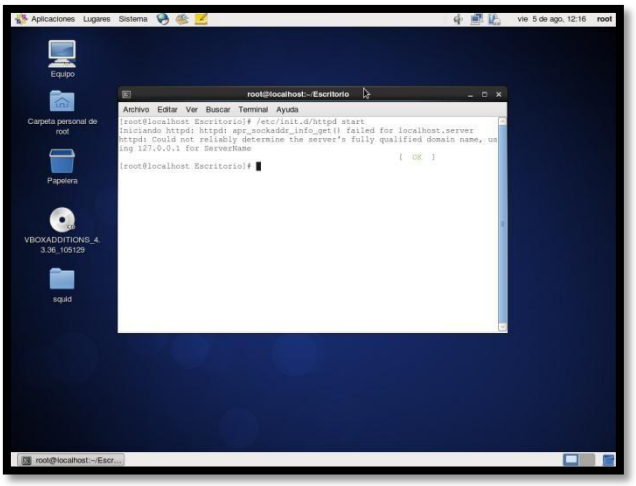
Elaborado por: Luis Agualongo

Levantamos los servicios del httpd con la siguiente línea

- #etc/init.d/httpd start

Gráfico Nº 74

Inicio del servicio httpd



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

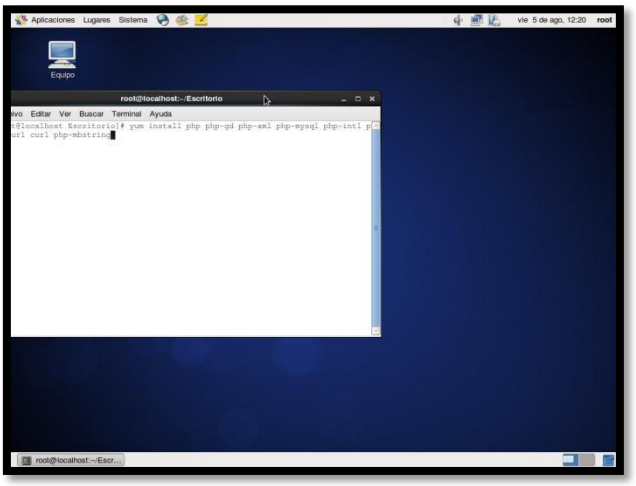
Elaborado por: Luis Agualongo

Se procede a instalar las dependencias del Mysql con la siguiente línea

- #yum install php php-gd php-xml php-mysql php-intl php-curl curl php-mbstring

Gráfico Nº 75

Instalación de dependencias de Mysql

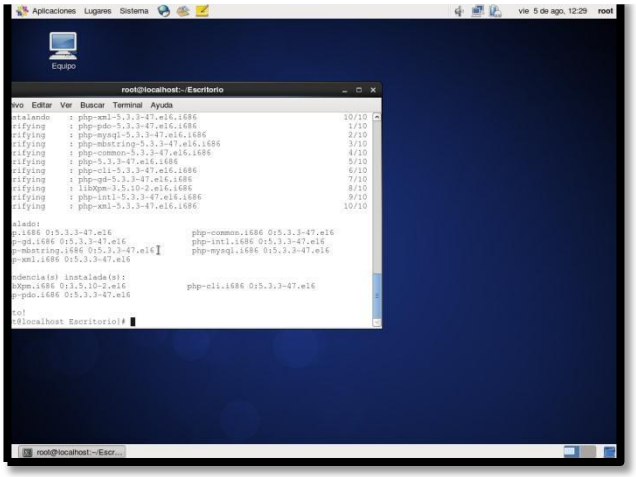


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 76

Descarga de actualizaciones



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

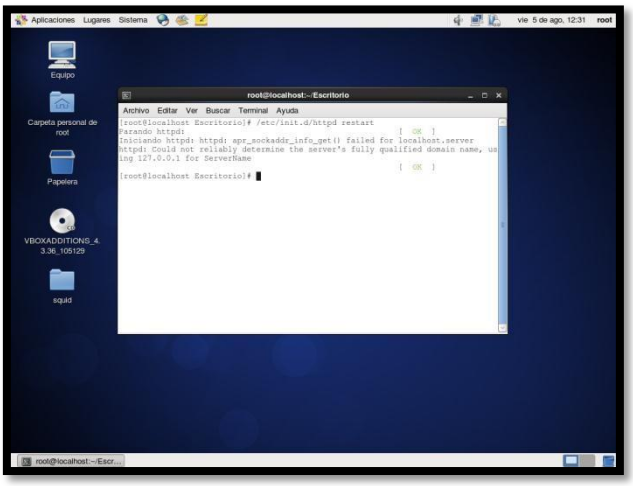
Elaborado por: Luis Agualongo

Ahora reiniciamos los servicios del httpd con la siguiente línea:

- #/etc/init.d/httpd restart

Gráfico Nº 77

Reiniciar servicio httpd



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

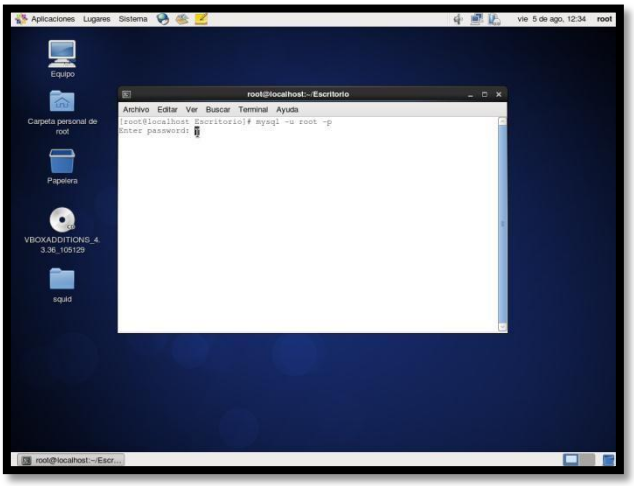
Elaborado por: Luis Agualongo

Se procede a crear la base de datos y el usuario administrador con la ejecución de las siguientes líneas:

Primero accedemos a la administración del entorno mysql ingresando la línea de comando desde la terminal #mysql –u root –p, nos pedirá una contraseña, para este caso es enter debido a que no se colocó contraseña alguna.

Gráfico Nº 78

Ingreso al mysql



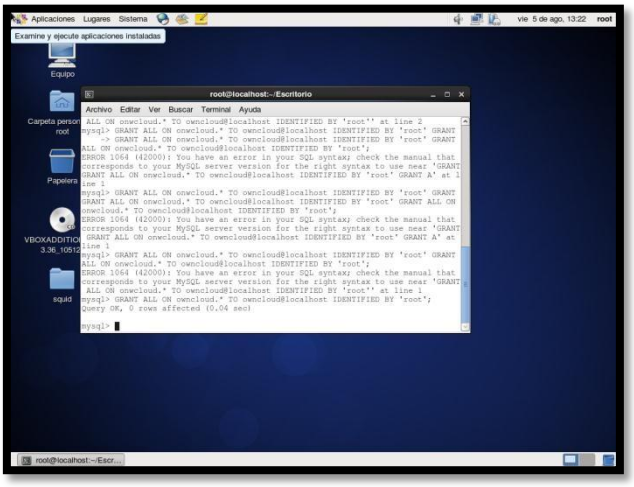
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez dentro de mysql creamos la base y agregamos al usuario administrador con la configuración que se encuentra en la gráfica Nº79#.

Gráfico Nº 79

Crear base de dato mysql



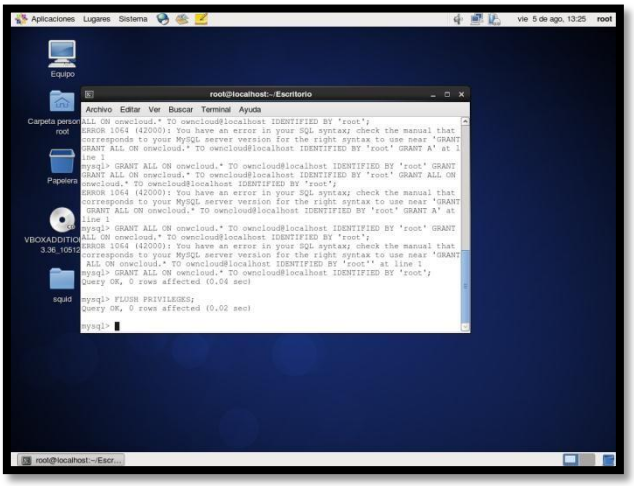
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Ahora le damos los privilegios a full.

Gráfico Nº 80

Privilegios del usuario administrador

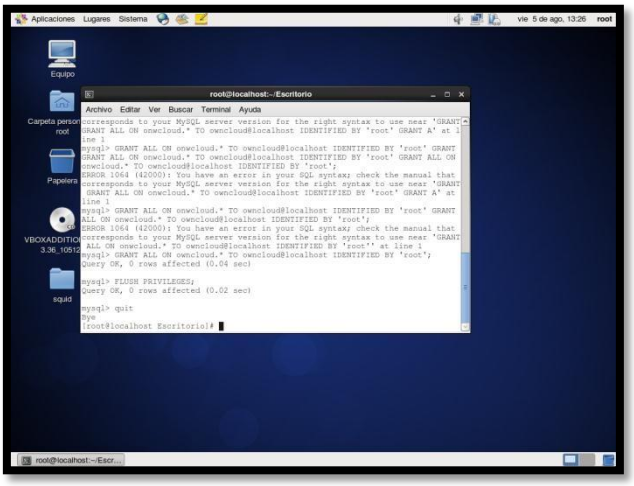


Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Gráfico Nº 81

Confirmación de base creada



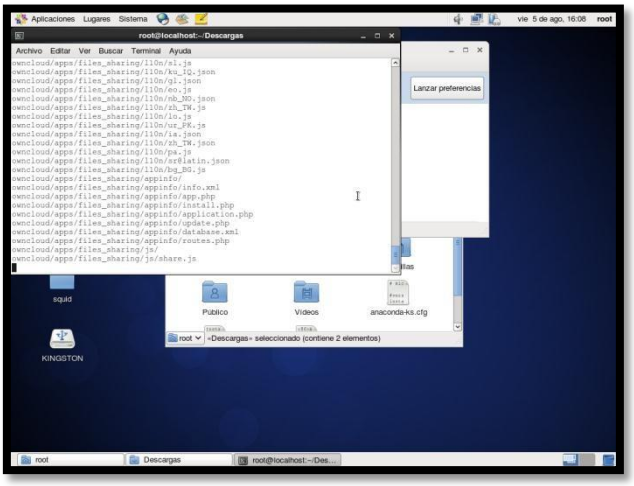
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez realizada la creación de la base de datos, se procede a la descarga del owncloud ultima versión 9.0.4, se descomprime dentro de la siguiente dirección /var/www/html.

Gráfico Nº 82

Descarga de owncloud



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

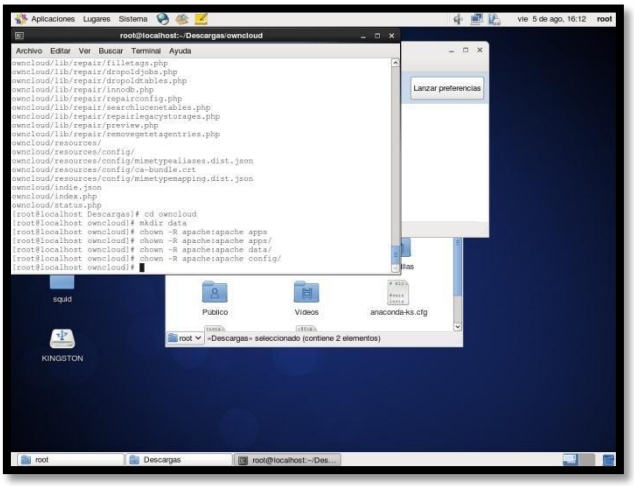
Elaborado por: Luis Agualongo

Una vez descomprimido ejecutamos las siguientes líneas en el orden escrito a continuación para dar los permisos al servicio web del owncloud.

- #mkdir data
- #chown –R apache:apache apps
- #chown –R apache:apache data
- #chown –R apache:apache config

Gráfico Nº 83

Permiso del owncloud



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

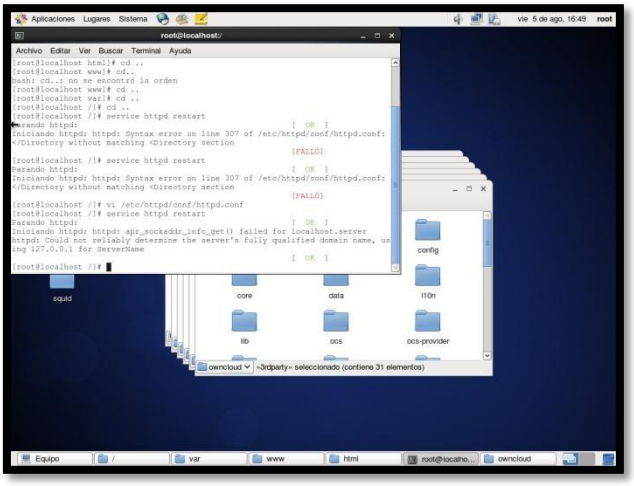
Elaborado por: Luis Agualongo

Reiniciamos los servicios del httpd con la siguiente línea de comando:

- #service httpd restart

Gráfico Nº 84

Reinicio del servicio httpd



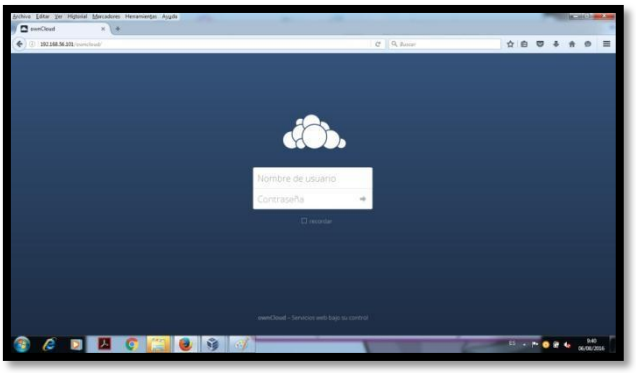
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Ahora si una vez reiniciado los servicios e instalado el Owncloud, podemos acceder desde el servidor Centos con la dirección localhosts/owncloud o desde cualquier pc que este dentro de la red en nuestro caso 192.168.56.101/owncloud desde cualquier navegador.

Gráfico Nº 85

Acceso web



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

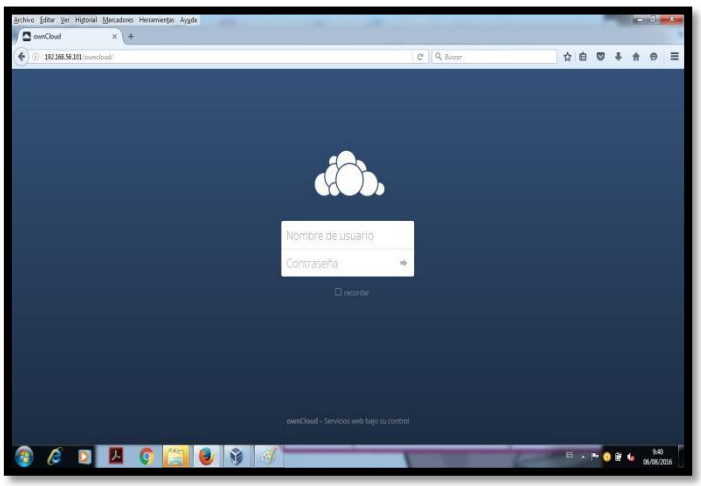
Elaborado por: Luis Agualongo

4.2.2.4. Configuración de Usuarios Y grupos en servidor de Archivos en la nube (Owncloud)

Una vez realizada la instalación del servidor de archivo Owncloud en nuestro servidor proxy, procedemos a ingresar desde cualquier equipo que este en nuestra red mediante un navegador web, en este caso es el 192.168.56.101/owncloud o desde el servidor con localhosts/owncloud.

Gráfico Nº 86

Pantalla inicial de Owncloud



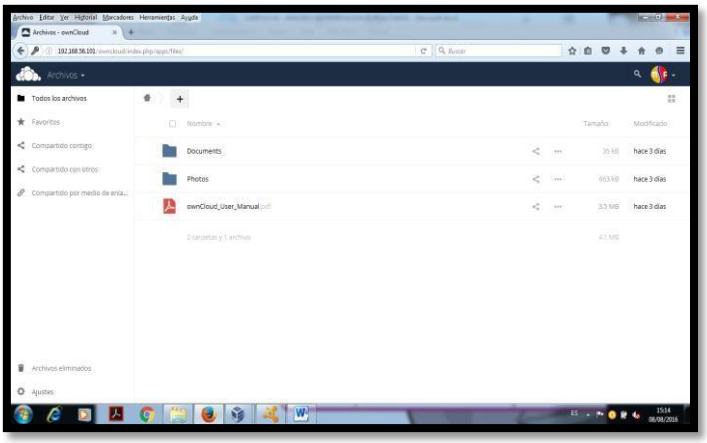
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Una vez realizado el procedimiento antes mencionado nos pedirá un nombre de usuario y contraseña, el usuario es aquel que se creó en la base de datos, en este caso root, y la contraseña por primera vez será enter para poder ingresar al entorno administrativo de Owncloud.

Gráfico Nº 87

Pantalla Owncloud



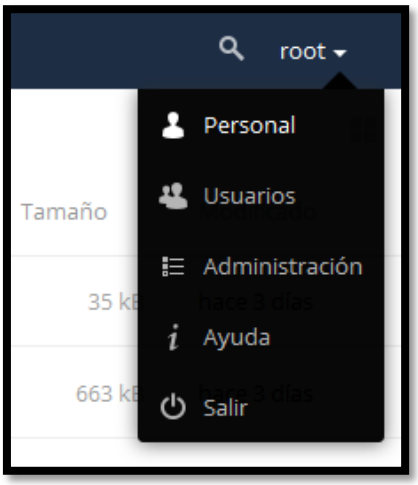
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Lo primero es ingresar a configurar la contraseña administradora, desde la parte superior izquierda del menú donde se encuentra el logotipo de la inicial del nombre de nuestro usuario administrador.

Gráfico Nº 88

Menu Administrador



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Persona y colocamos la nueva contraseña, claramente esta que la contraseña actual quedara completamente vacía, al no existir contraseña alguna durante la instalación y creación de la cuenta en la base de datos

Gráfico Nº 89

Cambio de Contraseña

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

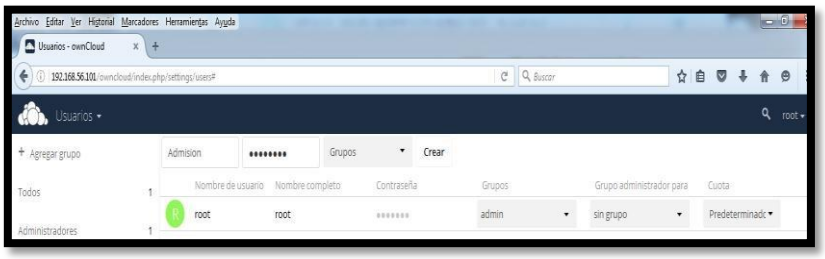
Se procede a la creación de los grupos o departamentos con los privilegios y tamaño máximo de almacenamiento.

Para esto en el menú de root, se despliega una lista y escogemos Usuarios e ingresamos los siguientes datos:

- Nombre de usuario: Admisión
- Contraseña:********

Gráfico Nº 90

Creación de Grupos



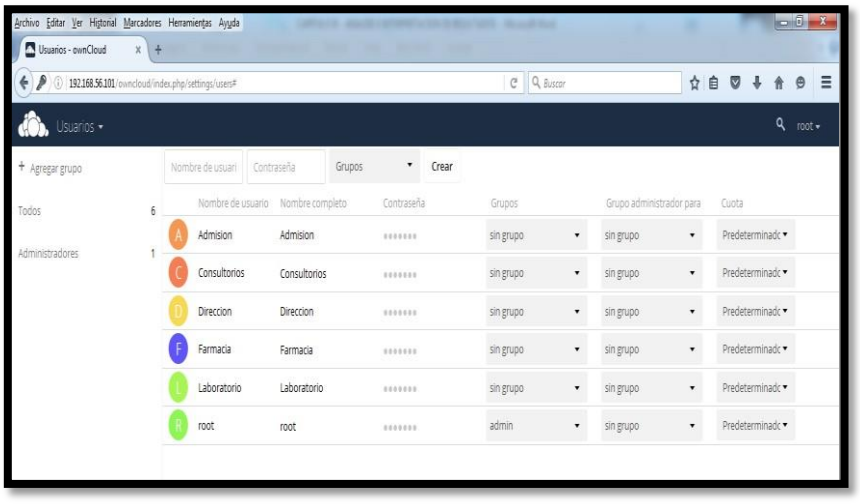
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se crea el primer grupo o departamentos

Gráfico Nº 91

Grupos creados



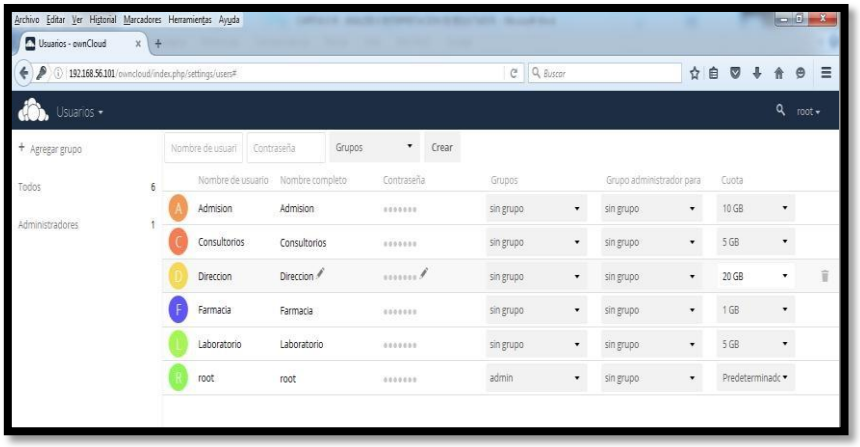
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Se procede a dar las cuotas de almacenamiento, esto para evitar saturar al servidor.

Gráfico Nº 92

Cuotas de almacenamiento



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

4.2.3. Estaciones de trabajo

Los equipos informáticos que se encuentran en cada uno de los departamentos cumpliendo funciones específicas, son aquellas que tendrán los permisos correspondiente a cada acción que ejecuten, que va desde abrir una página web hasta la compartición de archivos.

Cuando hablamos de una restricción web la distribuiremos con los siguientes permisos:

Tabla Nº 6

Privilegios por departamentos

Departamento	Privilegios			
	Total	Interno	Redes	Cursos
Dirección	X			
Admisión		X		X
Administración	X			
Farmacia		X		X
Tic´s	X			
Sala de Reuniones	X			
Odontología		X		X
Consultorio de TB		X		X
Consultorio Medicina General		X		X
Enfermería		X		X

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

Total. Acceso permitido a todo sitio web.

Interno. Acceso restringido, solo tendrá acceso web a sitios seguros e incluso a correos electrónico.

Redes. Acceso a redes sociales, siempre y cuando exista una razón necesaria y justificada se puede dar los permisos. Actualmente en

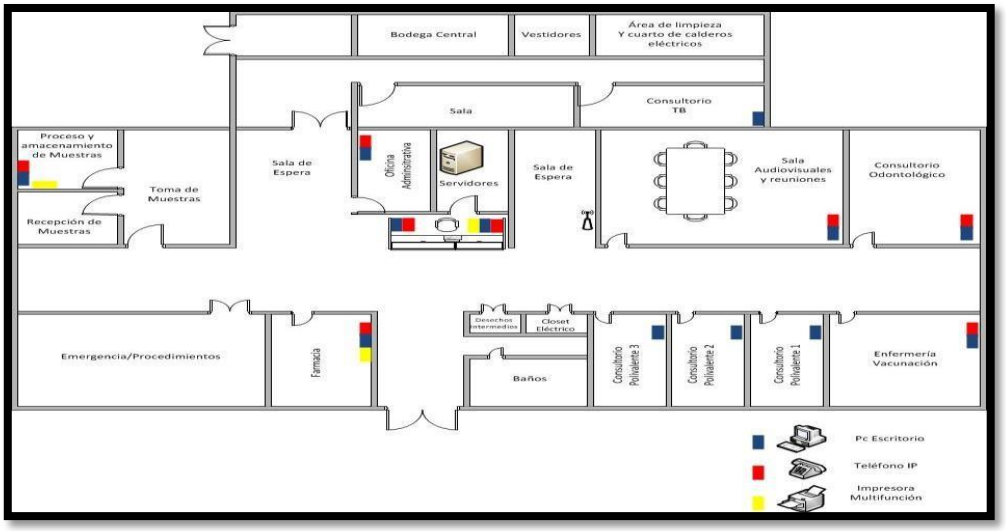
único que tiene acceso a redes es el departamento de Comunicación Social.

Cursos. Acceso que se solicita por un periodo de tiempo, esto permisos incluyen cursos online, videos en YouTube y otros acceso restringidos que son permitidos durante el tiempo que tarde el curso.

La distribución realizada de los equipos informáticos se detalla a continuación:

Gráfico Nº 93

Distribución de equipos informáticos



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

4.2.3.1. Configuración de las estaciones de trabajo (Proxy)

Desde que se levantan los servicios para que inicie el Squid, y el servidor este trabajando dentro de la red como filtrado de contenido las estaciones de trabajo no tendrán acceso al servicio web.

Las direcciones IP las designa automáticamente nuestro servidor ya que tenemos levantado el servicio DHCP.

Por tal razón se procede a realizar las configuraciones y obtener las pruebas de funcionalidad.

4.2.3.2. Para equipos en sistema operativo Ubuntu 14.04, se realiza lo siguiente:

- Clic en el botón de apagado del sistema.

Gráfico Nº 94

Apagado del sistema

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- Configuración del sistema.

Gráfico Nº 95

Configuraciones

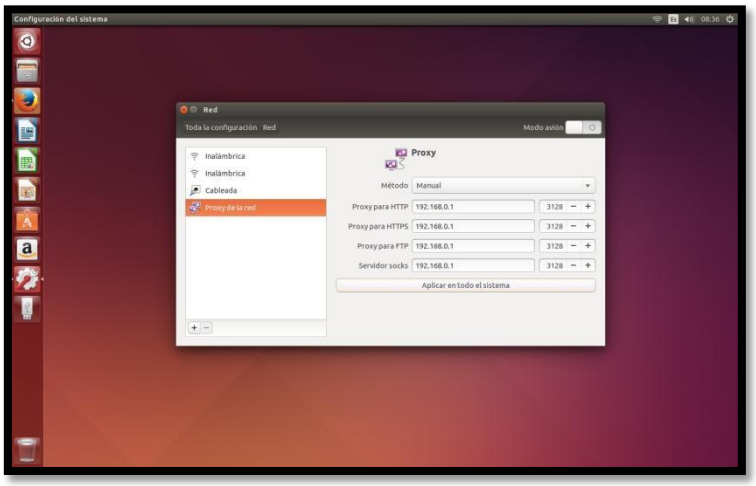
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- Red
- Proxy de red
- Método manual

Gráfico Nº 96

Configuraciones proxy



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- Agregamos la configuración del proxy

- ❖ Aplicar a todo el sistema

4.2.3.3. Para equipos en sistema operativo Windows, se realiza lo siguiente:

- ❖ Inicio
- ❖ Panel de control
- ❖ Redes e internet
- ❖ Opciones de internet

Gráfico Nº 97

Panel de Control

Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- ❖ Conexiones
- ❖ Configuración Lan

Gráfico Nº 98

Conexiones

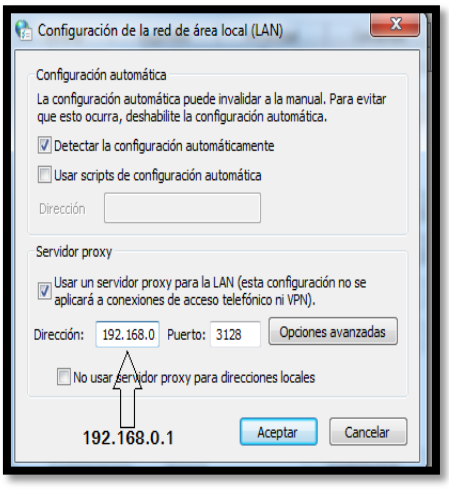
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- Activar la casilla de activar proxy para la Lan
- Ingresamos la dirección y el puerto

Gráfico Nº 99

Configuraciones de Red



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

- Aceptar
- Aceptar

4.2.3.4. Pruebas de Acceso Web

Una vez realizadas las configuraciones se realiza los enlaces a las siguientes direcciones web.

- **www.google.com**

Gráfico Nº 100

Pruebas de navegación

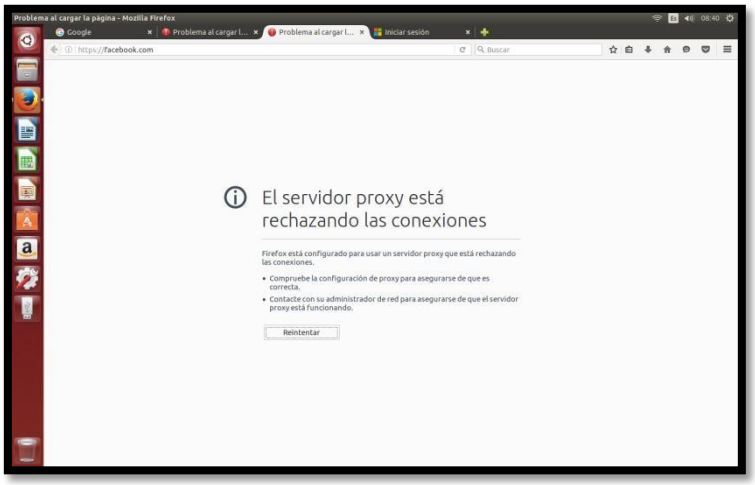
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ **www.facebook.com**

Gráfico Nº 101

Pruebas de navegación



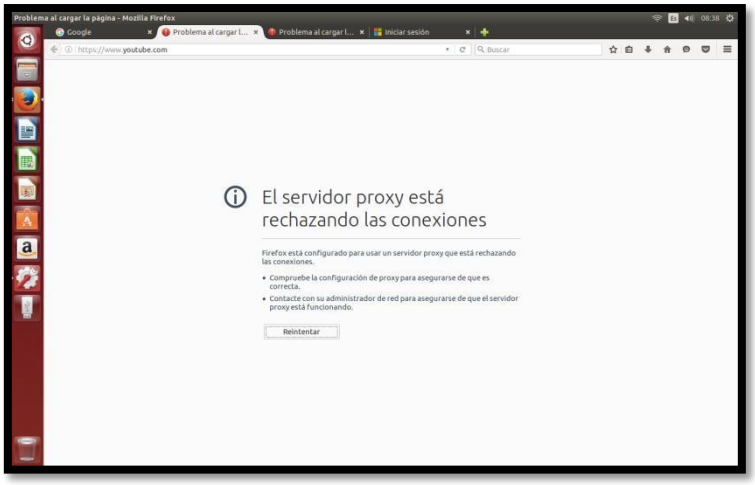
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ **www.youtube.com**

Gráfico Nº 102

Pruebas de navegación



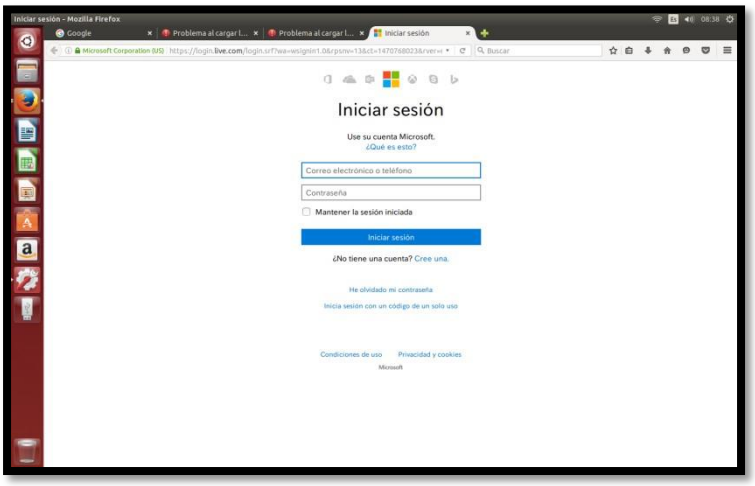
Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

❖ **www.hotmail.com**

Gráfico Nº 103

Pruebas de navegación



Fuente: Dirección Distrital 24D01 Santa Elena Salud.

Elaborado por: Luis Agualongo

4.2.4. Recomendaciones y conclusiones

4.2.4.1. Conclusiones

Con el aumento de los servicios en la red y la presencia cada vez mayor en la web, esto lleva a las instituciones públicas o privadas por medio de su personal de Tecnología a usar herramientas informáticas que garanticen el buen uso de los recursos web para cada uno de los usuarios.

La Instalación del sistema Operativo bajo la plataforma Linux, permite tener un sistema confiable y seguro para las amenazas externas como virus y ataques informáticos.

Linux es un excelente sistema para la implementación de servicios de red, por su potencia, estabilidad, seguridad y bajo costo.

El servidor Proxy permite la administración adecuada para la navegación en sitios de internet a los usuarios. Se tienen que establecer políticas de acuerdo al uso de cada usuario para impedir la mala utilización de los recursos web.

El proxy permite bloquear o habilitar el uso del internet a uno a varios equipos dependiendo de las necesidades de cada uno de los usuarios.

La implementación de los servicios en el servidor proxy es de suma importancia para que el centro de salud cuente con un filtro de información que asegure bien el funcionamiento del recurso web.

La implementación de un servidor de archivos en la nube asegura la confidencialidad de los archivos y el resguardo de los mismos. La compartición se realizara en base a los permisos que se efectúen a cada usuario según su necesidad.

4.2.4.2. Recomendaciones

Se recomienda que el personal de Tecnología sea el único que administre el servidor, tener acceso a él y realice las actualizaciones necesarias.

Se recomienda que el administrador del servidor mantenga actualizada las listas de accesos denegados para que los funcionarios no puedan acceder a los sitios web no permitidos.

Se recomienda que el administrador genere respaldos periódicos de la base, en una actualización o registro de los accesos pueda existir fallas en el sistema y tenga que restaurar la última configuración.

Se recomienda realizar mantenimientos preventivos de hardware/software del servidor proxy y de archivos en la nube, además de la instalación de equipos que mantenga un respaldo de energía en caso de apagones.

Esto nos ayudara a mantener la vida útil del equipo y evitar caídas del servicio, de esta manera será ininterrumpido los servicio proxy y de archivos.

Se recomienda realizar los log de cada uno de los servicios, esto dependerá del administrador de sistema cual desea utilizar, la implementación de esto ayudara a mantener las páginas de bloqueos actualizadas y al monitoreo constante.

Se recomienda capacitar a los usuarios para el uso adecuado de los equipos de trabajo y del uso de los servicios en la web para evitar pérdidas de información y saturación del servicio que puedan afectar a la producción de los profesionales de la salud.

BIBLIOGRAFÍA

Ávila, A. (2007). Instalación a la red Internet

Barrios J. (2016), Implementación de Servidores con GNU/Linux

Barrios, J. (28 de Septiembre del 2015). *Alcance Libre*. 28 de Septiembre del 2015, de http://www.alcancelibre.org/staticpages/index.php/manuales-indice

Barrios, J. (20 de Junio del 2014). *Alcance Libre*. 28 de Septiembre del 2015, de http://www.alcancelibre.org/staticpages/index.php/procedimiento-instalar-centos6-lvm

Delgado, J. A. (2014, noviembre). Nube informática en *Gobernanza de Internet en Ecuador: Infraestructura y acceso*. Artículo presentado en el Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador. Obtenido de http://delgado.ec/research/es/Gobernanza_Internet_Ecuador_2014.pdf.

Barrios, J. (28 de Septiembre del 2015). *Alcance Libre*. 28 de Septiembre del 2015, de http://www.alcancelibre.org/staticpages/index.php/ajustes-posteriores-centos6-instalar

Barrios, J. (21 de Julio del 2016). *Alcance Libre*. 21 de Julio del 2016, de http://www.alcancelibre.org/staticpages/index.php/como-dhcp-lan

Barrios, J. (12 de Septiembre del 2016). *Alcance Libre*. 12 de Septiembre del 2016, de http://www.alcancelibre.org/staticpages/index.php/19-0-como- squid-general

Barrios, J. (2016). *Alcance Libre*, de http://www.alcancelibre.org/staticpages/index.php/20-como-squid-reglas

Barrios, J. (15 de Abril del 2011). *Alcance Libre*. 15 de Abril del 2015, de http://www.alcancelibre.org/staticpages/index.php/como-squid-arp

Cardenas, A. (02 de Noviembre de 2006). Métodos de investigación. Obtenido de Métodos de investigación: http://alexcardenas.blogspot.com/2006/11/las-clases-de-metodos-de investigacion.html

Dr. J. Arranz, (2007). El internet. España: Ideaspropias Editorial, S.L.

Esparza J. (2013). Implementación de un Firewall sobre plataforma Linux en la Empresa de Contabilidad Armas & Asociados. Para obtención de título de tecnólogo en análisis de sistemas informáticos, escuela de formación de tecnólogo, Universidad Politécnica Nacional, Quito.

Kishore S. (Version 1.0), Instalación de Owncloud en Centos 6.5 desde: https://www.howtoforge.com/how-to-install-owncloud_7-on-centos_6.5

Manuel Sierra García, (2006). ¿Qué es un servidor y cuáles son los principales tipos de servidores?

Navarro J. (2009). Implementación de un Proxy en plataforma Linux para control de transferencia de archivos con FTP, E-mail y firewall para el laboratorio de software. Para obtención de título de tecnólogo, escuela de formación de tecnólogo, Universidad Politécnica Nacional, Quito.

Santaella J. (2014). Manual de Instalación de una Nube Owncloud en un servidor

Vasquez A. (2016), Centos Linux y Servicio de Red, desde http://leanpub.com/centosserviciosdered

Ziegler R. (2010), Firewalls Linux, Guía avanzada

ANEXOS

Anexo Nº 1

Ubicación del Centro de Salud San José de Ancón Tipo A.

Anexo Nº2

Comandos y servicios de Linux.

Comandos LINUX		
1	ac	Imprime estadísticas acerca del tiempo que han estado conectado los usuarios.
2	adduser	Ver useradd.
3	alias	Crea atajos de comandos, lista los alias actuales.
4	apt-get	Herramienta de actualizacón/instalación remota de paquetes en sistemas basados en debian.
5	arp	Permite obtener/manipular la lista de direcciones MAC/Ip que el sistema ve.
6	arping	Envía ARP REQUEST a otros equipos en la red.
7	arptables	Firewall similar en funciones a iptables pero para control de tráfico de protocolo arp.
8	at	Programa trabajos, comandos, scripts para su ejecución posterior.
9	atq	Lista los trabajos programados pendientes de ejecutar por el comando at.
10	awk	Análisis y procesamiento de patrones en archivos y listados.
11	basename	Permite eliminar la ruta del nombre de un archivo.
12	bc	Calculadora y lenguaje matemático, muy potente.
13	biosdecode	Información sobre el BIOS.
14	blkid	Muestra atributos de dispositivos de bloque (discos, usb, etc.) tales como LABEL y UUID, entre otros.
15	bzcat	Descomprime archivos comprimidos o empaquetados mediante bzip2.
16	bzip2	Compresor / descompresor de archivos.
17	bzmore	Permite ver el contenido de archivos comprimidos o empaquetados mediante bzip2.
18	cal	Despliega un calendario.

19	cat	Muestra el contenido de archivos y concatena archivos.
20	cd	Cambiar de directorio.
21	cfdisk	Herramienta de particionamiento de discos, usada en sistemas debian principalmente.
22	chage	Permite cambiar la información (expiración, caducidad, etc) de la contraseña de un usuario.
23	chattr	Cambia atributos extendidos de archivos y directorios
24	chfn	Cambia la información usada en finger.
25	chgrp	Cambia el grupo de un archivo(s) o carpetas(s).
26	chkconfig	Controla/consulta el modo en que los servicios se ejecutan o no al inicio del sistema.
27	chmod	Cambia los permisos de un archivo(s) o carpetas(s).
28	chown	Cambia el propietario de un archivo(s) o carpetas(s).
29	chpasswd	Actualiza passwords o contraseñas en modo batch. Puede actualizar contraseñas de grupos de usuarios.
30	chroot	Ejecuta comandos de root en un shell restringido a un directorio y sus subdirectorios.
31	chsh	Cambia tu shell por defecto o shell de login.
32	cleanlinks	Limpia enlaces simbólicos que no tengan relación y también remueve directorios vacios.
33	clear	Limpia la terminal.
34	cmp	Compara dos archivos byte por byte.
35	convertquota	Convierte de los viejos formatos quota.user y quota.group a los nuevos formatos de aquota.user y aquota.group.
36	cpio	Copia, crea, comprime y extrae archivos en distintos formatos y entre equipos o localmente.
37	crontab	Administra archivos cron para los usuarios y root.
38	curl	Permite descargar o transferir url's.
39	cut	Remueve secciones (columnas principalmente) de

		cada línea de un archivo o archivos.
40	date	Muestra/establece la fecha y hora actual.
41	dc	Calculadora interactiva.
42	dd	Convierte y copia archivos y sistemas de archivos.
43	ddate	Muestra la fecha en formato del calendario Discordante.
44	df	Muestra el uso de espacio de discos duros o particiones.
45	diff	Busca y muestra diferencias entre archivos.
46	dig	Utilería para consultas a servidores DNS.
47	dircolors	Configuración de colores para el comando ls.
48	dirs	Permite mostrar, manipular la lista de directorios utilizados en la pila. (ver popd y pushd)
49	dmesg	Muestra los mensajes del arranque del sistema (boot).
50	dmidecode	Lista hardware del equipo directamente del BIOS. (también: lshw)
51	dos2unix	Convierte archivos de formato MS-DOS a formato Unix/Linux.
52	du	Muestra el uso de espacio de archivos y directorios.
53	dump	Permite la creación de respaldos para los sistemas de archivos ext2 y ext3.
54	echo	Imprime una línea de texto, variables, o contenido a un archivo.
55	edquota	Administra el control de cuotas de disco de usuario y grupos.
56	egrep	Es igual que el comando 'grep -E', para uso de expresiones regulares.
57	eject	Desmonta y expulsa un medio removible, como cdroms.
58	env	Ejecuta un programa en un entorno modificado.

59	ethtool	Permite desplegar o cambiar valores de una tarjeta de red.
60	exit	Sale del shell o terminal actual.
61	expect	Permite crear secuencias de diálogos y programar sesiones interactivas con otros comandos o scripts.
62	export	Exporta el valor de una variable.
63	exportfs	Mantiene una lista de sistemas de archivos del tipo NFS que han sido exportados.
64	expr	Evaluador de expresiones matemáticas.
65	factor	Encuentra los números primos de un número dado.
66	fc	Lista, edita y reejecuta comandos previamente ejecutados.
67	fdisk	Herramienta para particionar discos, común a casi todas las distros.
68	fgrep	Es igual que 'grep -F' para uso de expresiones regulares en búsquedas de archivos y listados.
69	file	Determina el tipo de archivo.
70	find	Búsqueda de archivos, multitud de opciones de búsqueda.
71	findfs	Busca un sistema de archivos por UUID o LABEL (etiqueta).
72	findsmb	Lista información sobre equipos que respondan a paquetes SMB. Lista una red Windows. (Parte del paquete Samba)
73	finger	Muestra información sobre los usuarios del sistema.
74	fortune	Imprime un adagio al azar.
75	fping	Permite mandar paquetes ICMP (pings) a múltiples equipos en una red y determinar si están vivos o no.
76	free	Muestra el espacio usado y libre de memoria RAM y Swap.
77	fsck	Herramienta para verificar/reparar sistemas de

		archivos.
78	fuser	Identifica procesos utilizando archivos o conexiones (sockets).
79	gawk	Análisis y procesamiento de patrones en archivos y listados. (versión gnu)
80	gcc	Compilador de C y de C++ de GNU.
81	gedit	Editor de textos de gnome.
82	gpasswd	Permite la administración del archivo /etc/group
83	gpg	Herramienta de encriptación y de generación de certificados de seguridad (opengpg).
84	grep	Busca patrones de cadenas dentro de archivos.
85	groupadd	Crea un nuevo grupo en el sistema.
86	groupdel	Elimina un grupo en el sistema.
87	groupmod	Modifica un grupo en el sistema.
88	groups	Imprime los grupos a los que pertenece un usuario.
89	gzip	Comprime/expande archivos.
90	halt	Apaga el equipo.
91	hdparm	Establece y muestra características sobre los discos duros.
92	head	Despliega las primera líneas de un archivo.
93	help	Ayuda sobre los comandos internos de bash.
94	history	Muestra el historial de comandos del usuario.
95	host	Utileria de consulta a sevidores DNS.
96	hostname	Despliega el nombre del equipo.
97	htpasswd	Administra archivos de usuario/contraseña para autentificación básica de Apache.
98	hwclock	Muestra/Establece la fecha/hora del bios o hardware. (Fecha/Hora del sistema con date)
99	id	Muestra el UID (User ID) y GID (Group ID) del usuario
100	ifconfig	Muestra/Configura las interfaces de red del sistema.

101	ifstat	Pequeña utileria que permite observar estadísticas de las interfaces de red en tiempo real.
102	init	Control de inicialización de un nivel de ejecucción.
103	insmod	Inserta módulos en el kernel.
104	ipcalc	Realiza cálculos simples sobre direcciones IP.
105	ipcount	Identificación de rangos de red, cálculo de IP's.
106	iptab	Muestra una tabla de direcciones IP de acuerdo al prefijo CIDR
107	iptables	Herramienta de configuración del firewall de Linux.
108	iptraf	Analizador de tráfico de red en modo de texto.
109	iwconfig	Configura una tarjeta de red inalámbrica.
110	iwlist	Obtiene información detallada de una tarjeta inalámbrica.
111	jobs	Muestra los trabajos del usuario en suspensión o en background.
112	kate	Editor de textos de KDE.
113	kill	Termina procesos, mas correctamente envía señales a procesos.
114	killall	Termina procesos del mismo nombre o conjunto.
115	last	Muestra información de los últimos usuarios logueados.
116	lastb	Muestra información de los últimos intentos fallidos de loguearse.
117	less	Muestra el contenido de un archivo, permite búsquedas y movimento hacía atrás y adelante.
118	ln	Crea enlaces (accesos directos) suaves y duros de archivos y directorios.
119	locale	Información específica sobre las variables de entorno locales.
120	locate	Indexa y busca archivos. Mas seguro utilizar slocate.
121	losetup	Define y controla dispositivos del tipo 'loop'.

122	lpq	Muestra los documentos para imprimir en la cola de impresión.
123	lpr	Añade un documento a la cola de impresión.
124	ls	Lista archivos y directorios.
125	lshw	Lista hardware del equipo directamente del BIOS. (también: dmidecode)
126	lsmod	Muestra el estatus de los módulos en el kernel.
127	lsof	Muestra archivos abiertos de un programa en ejecucción, o de un usuario, proceso, etc.
128	lspci	Lista los dispositivos pci del sistema.
129	lsusb	Lista los dispositivos usb del sistema.
130	mail	Envía y recibe correos.
131	man	Muestra el manual del comando indicado.
132	mc	Manejador de archvivos con soporte de mouse en modo de texto, no todas las distro lo tienen.
133	mcedit	Editor de textos de mc.
134	md5sum	Comprueba (y genera) archivos con firma de certificación md5.
135	mkdir	Crea directorios.
136	mkfs	Construye un sistema de archivos de Linux.
137	mkpasswd	Generador de contraseñas. (Paquete del programa 'expect').
138	modinfo	Muestra información acerca de los módulos del kernel.
139	modprobe	Herramienta que añade/remueve módulos del kernel.
140	more	Paginador similar a less pero menos funcioanal, ya que sale avanza y no retocede.
141	mount	Monta dispositvos de almacenamiento en particiones indicadas.
142	mtools	Conjunto de utilidades para acceder a discos DOS desde Linux.

143	mv	Mueve archivos y directorios.
144	netstat	Herramienta de red que muestra conexiones, tablas de ruteo, estadísticas de interfaces, etc.
145	nice	Ejecuta un programa con una prioridad de ejecucción distinta a la normal.
146	nohup	Ejecuta un programa inmune a los hangups y sin salida a una terminal.
147	openssl	Control, administración, generación de certificados de seguridad.
148	partprobe	Indica al sistema operativo de los cambios indicados en /etc/fstab
149	passwd	Cambia la contraseña del usuario indicado.
150	ping	Manda un echo_request (solicitud de eco) a un equipo en al red.
151	pkill	Manda señales a procesos basado en sus atributos.
152	popd	Remueve entradas (directorios utilizados) de la lista de directorios utilizados en la pila. (ver dirs y pushd)
153	pr	Formatea o convierte archivos de texto para imprimirlos.
154	ps	Muestra los procesos del sistema o del usuario o ambos.
155	pstree	Muestra los procesos en forma de árbol.
156	pushd	Agrega entradas (directorios utilizados) en la lista de directorios (pila o stack). (ver dirs y popd)
157	pwck	Verifica la integridad del archivo /etc/passwd
158	pwconv	Agrega o establece la protección shadow el archivo /etc/passwd.
159	quota	Permite ver el uso de cuotas por usuario.
160	quotacheck	Crea, verifica, administra sistemas de cuotas de disco
161	quotaoff	Desactiva el control de cuotas de discos.

162	quotaon	Activa el control de cuotas de discos para usuarios y grupos.
163	rdesktop	Abre terminales gráficas ha?ia equipos Windows.
164	reboot	Reinicia el equipo.
165	renice	Cambia la prioridad de un proceso o programa en ejecucción.
166	repquota	Reporte de uso de cuotas de disco.
167	resolveip	Resuelve la ip del dominio o host que se indique.
168	rev	Invierte las líneas de un archivo.
169	rm	Borra o elimina archivos.
170	route	Muestra/altera la tabla de ruteo IP.
171	rpm	Programa para la instalación/actualización/eliminación de paquetes, distros basadas en redhat.
172	runlevel	Muestra el nivel de ejecución actual y anterior del sistema.
173	scp	Copia archivos entre equipos, parte del paquete openssh (protocolo de comunicación encriptado).
174	screen	Administrador de terminales virtuales.
175	sed	Editor en línea que filtra y transforma archivos.
176	service	Ejecuta/detiene servicios en modo manual.
177	set	Muestra o establece el entorno de variables para el usuario actuual.
178	sha1sum	Comprueba (y genera) archivos con firma de certificación sha1.
179	shopt	Habilita o deshabilita variables opcionales del comportamiento del shell.
180	shred	Elimina archivos de manera segura e irrecuperable.
181	shutdown	Apaga o reinicia el equipo.
182	sort	Ordena líneas de archivos y listas
183	ss	Utileria similar a netstat pero más básica, listados

		rápidos de sockets establecidos.
184	ssh	Programa de login remoto seguro, programa del paquete openssh (protocolo de comunicación encriptado).
185	startx	Inicia una sesión X.
186	su	Cambia del usuario actual al indicado.
187	sudo	Permite indicar que usuario ejecuta que comandos de root.
188	sync	Forza bloques en memoria a discos, actualiza el superbloque.
189	tac	Igual que cat, muestra y/o concatena archivos pero al revés.
190	tail	Muestra la parte final de un archivo.
191	tailf	Sinónimo del comando tail -f, permite ver en tiempo real la parte final de un archivo, es decir, conforme se va escribiendo, útil para monitorear bitácoras.
192	tar	Herramienta empaquetadora/compresora de archivos.
193	testparm	Revisa archivos smb.conf de samba por errores o correciones.
194	time	Devuelve el tiempo en que se ejecutó el comando o programa indicado.
195	top	Muestra los procesos del sistema de manera interactiva y continua.
196	touch	Crea archivos vacios, cambia fechas de acceso y/o modificación de archivos.
197	tput	Cambia valores o capacidades de la terminal, en base a terminfo.
198	traceroute	Imprime la ruta de los paquetes de red hasta el destino indicado.
199	tty	Imprime el nombre de la terminal en la que se esta.

200	tzselect	Permite establecer una zona o huso horario.
201	umask	Establece una máscara de permisos para cuando se crean directorios y archivos.
202	umount	Desmonta sistemas de archivos.
203	unalias	Elimina alias de comandos, creados con el comando alias.
204	uname	Despliega información del sistema.
205	uniq	Omite o reporta sobre líneas repetidas en un archivo o listado.
206	units	Convertidor de unidades de un sistema a otro, soporta decenas de sistemas de medición.
207	up2date	Herramienta de actualización/instalación remota de paquetes, (usada en redhat, centos).
208	uptime	Muestra que tanto tiempo lleva prendido el equipo.
209	urpme	Programa del paquete urpmi para desinstalar o eliminar paquetes.
210	urpmi	Herramienta de actualización/instalación remota de paquetes, distros basadas en rpm (usada en mandriva).
211	useradd	Añade usuarios.
212	userdel	Elimina usuarios.
213	usermod	Modifica información de usuarios.
214	users	Muestra los nombres de usuario de todos los usuarios conectados actualmente al sistema.
215	vi	Editor visual de pantalla, editor de textos, que encuentras en todas las distros Linux.
216	vim	Igual que el vi pero mejorado.
217	visudo	Editor para el archivo de configuración /etc/sudoers de sudo.
218	vmstat	Proporciona información sobre la memoria virtual.
219	w	Muestra quien esta conectado al sistema y que esta

		haciendo.
220	wall	Manda un mensaje a todas las terminales.
221	warnquota	Configura /etc/warnquota.conf como complemento de mensajes para cuotas de disco.
222	wc	Cuenta palabras, líneas, caracteres de un archivo o listado.
223	wget	Descargador de archivos desde Internet, no interactivo.
224	whatis	Descripción corta, en una línea de un comando o programa.
225	whereis	Localiza el binario, fuentes y/o librerias, y documentación de un comado.
226	which	Muestra la ruta completa de un comando.
227	who	Muestra quien esta conectado al sistema.
228	whoami	Muestra el usuario actual.
229	xhost	Control de acceso para sesiones X.
230	xkill	Mata o termina a un cliente X, es decir, a un programa gráfico.
231	yes	Imprime una cadena repetidamente hasta que sea terminado o matado el comando.
232	yum	Herramienta de actualización/instalación remota de paquetes, distros basadas en rpm (usada en fedora, redhat y derivados).
233	zcat	Descomprime / muestra archivos comprimidos con gunzip (es idéntico a utilizar gunzip -c)
234	zenity	Despliega varios tipos de diálogos en X desde una terminal.
235	zless	Permite mostrar el contenido de archivos comprimidos.
236	zmore	Permite mostrar el contenido de archivos comprimidos.

Anexo Nº3

Carta de autorización la empresa

Instituto Superior Tecnológico Bolivariano de Tecnología

Guayaquil, Miércoles 1 de Junio del 2016

Srta.
Mgs. Lorena Villon Moreno
Responsable de Tecnología de la Información
Dirección Distrital de Salud 24D01 Santa Elena

De mis consideraciones:

Por medio del presente me dirijo a usted Mgs. Lorena Villon Moreno, responsable de Tecnología de la Dirección Distrital 24D01 Santa Elena Salud de la manera más respetuosa solicitarle la respectiva autorización para la creación del **Diseño de un servidor Firewall y servidor de Archivo (Owncloud),** en el centro de salud San José de Ancón Tipo A que usted dirige, y así poder ayudar en el proceso de filtrado de contenido y la compartir archivos con el personal de la institución, creando un sistema más ágil, seguro y brindando la confianza necesaria en los procesos y recursos web.

La Información que estoy solicitando es el soporte para mi **PROYECTO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNOLOGÍA EN ANÁLISIS DE SISTEMAS.**

Agradezco de antemano por su ayuda y comprensión, deseando que mi proyecto sirva a la institución.

DIRECCION DISTRITAL 24D01 SANTA ELENA-SALUD
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN SOPORTE TÉCNICO Y REDES 3

Recibido por: LORENA VILLON
Fecha: 2/JUN/2016 Hora: 08:00

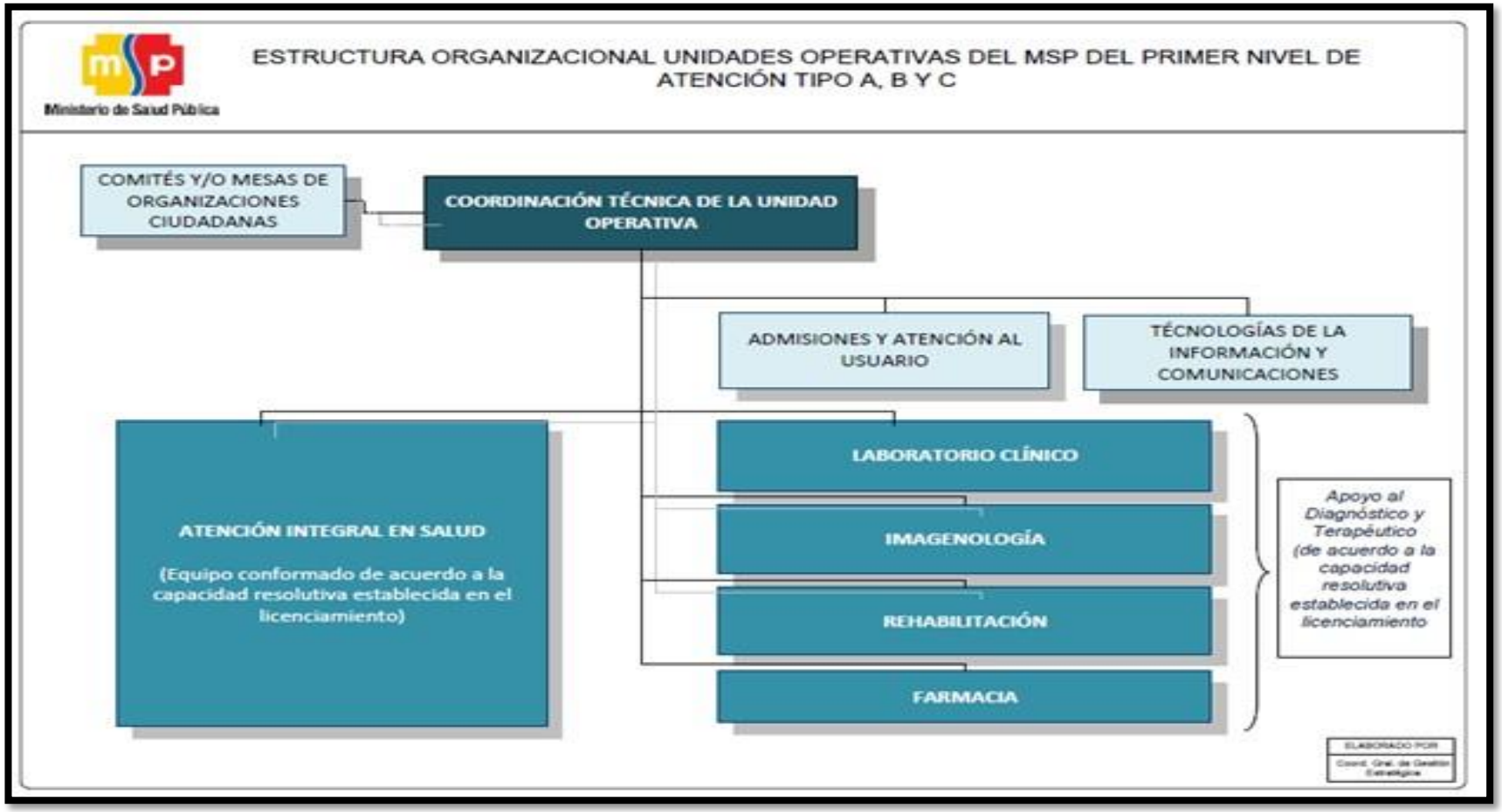
Atentamente

Luis Antonio Agualongo Domínguez
C.I: 091965096-0

AUTORIZADO
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACION SOPORTE TECNICO Y REDES 3
Ing. Lorena Villon Moreno
DIRECCIÓN DISTRITAL 24D01 SANTA ELENA-SALUD

Anexo Nº4

Organigrama de la empresa



Anexo Nº5

Políticas uso de servicios de Red y Servicios informáticos del Ministerio de Salud Pública del Ecuador

Políticas Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública

Revisiones y Versiones

Modificaciones	Nombre	Cargo
Realizado por	Aldo Cárdenas	Director de la Dirección Nacional de Tecnologías de la Información y Comunicaciones
Revisado por	Wilfrido Almache	Coordinador de Desarrollo de Software
	Javier Jaramillo	Coordinador de Redes e Infraestructura.
	Danilo López	Coordinador de Proyectos de Tecnología
	Lenin Robalino	Analista de Proyectos de Tecnología
Realizado por	Eduardo Véliz	Asesor - Coordinación General de Gestión Estratégica
Aprobado por	David Mejía	Coordinador General de Gestión Estratégica
Autorizado por	Carina Vance	Ministra de Salud Pública

Versiones y Modificaciones

Versión	Nombre	Descripción	Fecha
1.0	Aldo Cárdenas	Creación del Documento	07-Sep-2012
1.0	Lenin Robalino	Cambio de Formato al documento	26-Sep-2012
1.0	Danilo López	Revisión del Documento	03-Oct-2012
1.0	Javier Jaramillo	Revisión del Documento	03-Oct-2012
1.0	Wilfrido Almache	Revisión del Documento	03-Oct-2012
1.0	Lenin Robalino	Revisión del Documento	03-Oct-2012
1.1	Eduardo Véliz	Revisión del Documento	30-Oct-2012
1.2	Mónica Uyana	Revisión del Documento	12-Dic-2012

Contenido

1. Introducción

El Ministerio de Salud Pública proporciona a sus funcionarios recursos informáticos y servicios de red para su utilización en actividades laborales, de investigación, desarrollo e innovación y de proyección social, incluyendo las tareas administrativas asociadas.

Dado que estos recursos y servicios son ampliamente utilizados y considerando que la red de datos sobre la que están soportados está integrada a su vez en otras de índole más amplia, se evidencia la necesidad de implementar una normativa que partiendo de la ineludible adecuación a la legislación vigente, clarifique la forma correcta de uso de los mismos, delimite las responsabilidades y proporcione un marco para la regulación del uso de cada uno de ellos.

2. Objetivo

Establecer la regulación para el uso de los recursos informáticos y servicios de red que el Ministerio de Salud Pública, proporciona a los funcionarios para su utilización en temas exclusivamente laborales según sus funciones.

3. Alcance

La presente Política, es aplicable para todos los funcionarios del Ministerio de Salud Pública que utilicen los servicios de Tecnologías de la Información.

La Dirección de Tecnologías de la Información y Comunicaciones, será la encargada de administrar la presente Política, actualizarla y velar por su cumplimiento y aplicabilidad, así como modificarla en el caso de ser necesario.

Esta Política, será aplicable a todos los equipos de computación que pertenezcan al Ministerio de Salud Pública a nivel nacional y que formen parte de los activos fijos de la Institución, así como también al personal interno y externo de la Institución, quienes hagan uso de los recursos de la infraestructura de red del Ministerio de Salud Pública, incluyendo a visitantes de otras instituciones o ciudadanía en general.

4. Cómo usar este documento

Este documento es una ***Guía*** sobre las políticas implementadas, que garantizarán una operación y ejecución adecuadas dentro de la Dirección Nacional de Tecnologías de la Información y Comunicaciones y sus Coordinaciones.

5. Principios Generales

Los principios generales en que se inspira esta regulación son los siguientes:

- Absoluto respeto a los derechos y libertades constitucionales, así como a las disposiciones establecidas en el Ministerio de Salud Pública.
- Proteger el buen nombre y el prestigio de la Institución, así como de los Centros, Departamentos, Direcciones, Servicios y demás Unidades Administrativas que la constituyen.
- Evitar cualquier situación que pueda derivar en algún tipo de responsabilidad civil, administrativa o penal para el Ministerio de Salud Pública.
- Facilitar el máximo aprovechamiento de los recursos informáticos, propiciando una gestión eficiente de los procesos incluidos en sus sistemas de información y redes de comunicaciones con las que opera.
- Prevenir los riesgos o daños sobre los sistemas de información y los datos en ellos incorporados, que puedan deberse a la acción humana, referente a conductas incorrectas o inadecuadas.

6. Ámbito de aplicación

La presente regulación será aplicable a todos los miembros de la Institución, a nivel individual y colectivo, incluyendo direcciones, subsecretarías, coordinaciones, servicios, entre otros, así como terceras personas tales como consultores y contratistas con o sin relación de dependencia a la Institución, quienes al momento de utilizar los recursos informáticos y/o servicios de red pertenecientes a la Institución, aceptarán el uso y aplicabilidad del presente.

Con objeto de dar la mayor publicidad a la presente Política, la Dirección de Tecnologías de la Información y Comunicaciones dispondrá de los medios necesarios para mantener al alcance de los involucrados el presente documento, así como para responder a consultas e inquietudes de manera inmediata, considerando en primera instancia que su desconocimiento no exime de su cumplimiento.

7. Marco Legal

Con Acuerdo Ministerial 00001034 de 01 de noviembre de 2011, publicado en el Registro Oficial No. 279 de 30 de marzo 2012, se emite el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública, mismo que dispone como misión de la Dirección Nacional de Tecnologías de la Información y Comunicaciones: "Proponer, implementar y administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TIC's), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional.

8. Consideraciones Generales

Las Políticas relacionadas a las Tecnologías de la Información, están enfocadas a los equipos de computación que son asignados a cada funcionario, así como al centro de datos, y a la propiedad de la información que es creada y usada por los usuarios del Ministerio de Salud Pública, con el fin de evitar la inadecuada utilización de los recursos informáticos que se pone a disposición de los funcionarios, para que desarrollen sus actividades.

La presente Política constituye el marco de referencia de las Tecnologías de la Información del Ministerio de Salud Pública y serán cumplidas por todos sus funcionarios y personal externo que hacen uso de recursos de la infraestructura de red institucional.

- Se determina el uso de las contraseñas que son utilizadas con el fin de garantizar que la información solo sea accedida por el personal autorizado y que cuente con un control de accesos.

- Se regulariza el uso del correo electrónico, e Internet, los cuales se han convertido en herramientas de trabajo y uso diario, por lo cual es importante cumplir con las políticas relacionadas a ellos, con el fin de evitar cortes e interrupciones que podrían afectar la productividad e imagen de la Institución.
- El software utilizado por el Ministerio de Salud Pública, que haya sido desarrollado o adquirido, estará regulado por las normas y reglamentos vigentes, dando cumplimiento a lo dispuesto por el Decreto Ejecutivo No. 1014 de 10 de abril de 2008, publicado en el Registro Oficial No. 322 de 23 de abril del mismo año sobre el uso del software libre en las Entidades de la Administración Pública Central.

9. Declaración de políticas

9.1 Políticas Generales

Es responsabilidad de la Dirección Nacional de Tecnologías de la Información y Comunicaciones y de otras Unidades Administrativas del Ministerio de Salud Pública:

- Velar por los recursos informáticos y de servicios de red del Ministerio de Salud Pública.
- La Dirección Nacional Administrativa es la responsable de la entrega de equipos y activos fijos a los funcionarios, así como de la custodia de los equipos informáticos de la Institución.
- Los Subsecretarios, Coordinadores Generales, Directores de cada área o Gerentes de Proyectos, son los responsables del pedido de los recursos informáticos y del uso de los servicios de red de los miembros de su departamento o grupo, destinados a las actividades propias de cada estructura.
- Bajo ninguna circunstancia los funcionarios de la Institución, utilizarán los recursos informáticos para realizar actividades prohibidas por las normas establecidas o por normas jurídicas nacionales o internacionales.
- Para los equipos informáticos propiedad del Ministerio de Salud Pública, la Coordinación de Soporte a usuario y mesa de ayuda perteneciente a la Dirección

Nacional de Tecnologías de la Información y Comunicaciones, será la única coordinación autorizada a realizar actividades de soporte técnico y cambios de configuración en los equipos informáticos de los funcionarios de la Institución.

- En el caso de contratación para labores de mantenimiento, la Dirección Nacional de Tecnologías de la Información y Comunicaciones, aprobará previamente los mantenimientos solicitados. En caso de arriendo de computadoras la empresa contratada es la única autorizada para realizar labores de soporte y mantenimiento.

9.2 Políticas Para Equipos Informáticos

Como responsabilidades de la Dirección Nacional de Tecnologías de la Información y Comunicaciones están:

- Los equipos informáticos propiedad del Ministerio de Salud Pública, se utilizarán únicamente para actividades laborales que permitan alcanzar las metas y objetivos planteados por la Institución.
- Para el buen funcionamiento de los equipos informáticos, se realizarán los mantenimientos necesarios tanto preventivos como correctivos una vez al año, los términos de contratación serán elaborados y considerados en el POA de la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- La Dirección Nacional Administrativa es la responsable de la asignación y distribución de equipos informáticos a los funcionarios internos de la Institución,
- La configuración y asignación de usuarios a cada equipo.
- La compra de equipos informáticos será responsabilidad de la Dirección Nacional Administrativa, previa aprobación de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, enmarcadas en la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento.
- La compra de accesorios y reparaciones será solicitada por la Dirección Nacional de Tecnologías de la Información y Comunicaciones a la Dirección Nacional Administrativa, si un área requiere algún tipo de accesorio, deberá contar con la

aprobación de la Dirección Nacional de Tecnologías de la Información y Comunicaciones.

- Para poder conectar un equipo informático que no sea propiedad del Ministerio de Salud Pública a la red institucional, se solicitará el permiso correspondiente a la Dirección Nacional de Tecnologías de la Información y Comunicaciones, para que inspeccione el equipo, con el fin de comprobar que dicho activo no constituye un riesgo para la seguridad de los servicios, red y recursos informáticos de la Institución, se evalué la necesidad de conexión a la red del Ministerio de Salud Pública y se conceda la autorización correspondiente si es el caso.
- En caso de robo, hurto o extravío del equipo informático del Ministerio de Salud Pública, se notificará inmediatamente a la Dirección Nacional Administrativa, para empezar los trámites correspondientes.
- En caso de daño de cualquier equipo informático, se informará inmediatamente a la Dirección Nacional de Tecnologías de la Información y Comunicaciones, para realizar las correcciones necesarias.
- Solo el personal autorizado por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, será el encargado de abrir los equipos informáticos propiedad del Ministerio de Salud Pública, para el caso de los equipos arrendados la empresa contratada dueña de dichos activos será la única autorizada para abrir los equipos, o en su caso autorizar la apertura de los mismos.
- Todos los equipos informáticos pertenecientes al Ministerio de Salud Pública, contarán con un software antivirus así como también un firewall personal, los cuales serán administrados por la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Todos los equipos informáticos bajo la supervisión del Ministerio de Salud Pública, serán actualizados de manera periódica con los últimos parches de seguridad del sistema operativo y aplicaciones instaladas en el equipo.
- Todas las computadoras conectadas a la red del Ministerio de Salud Pública, contarán obligatoriamente con un fondo definido por la Dirección Nacional de Comunicación, Imagen y Prensa e implementado por la Dirección Nacional de Tecnologías de la Información y Comunicaciones.

9.3 Acceso a servidores y Centro de Datos

Es responsabilidad de la Coordinación de Redes, Comunicaciones y Seguridad Informática de la Dirección Nacional de Tecnologías de la Información y Comunicaciones:

- El acceso al centro de datos del Ministerio de Salud Pública, es exclusivo e intransferible para los Funcionarios del Área de Redes, Comunicaciones y Seguridad Informática de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, o quien dicha Dirección designe.
- Las claves de acceso a los servidores estarán bajo la custodia y son de responsabilidad exclusiva del Área de Redes, Comunicaciones y Seguridad Informática y solo se entregarán previa autorización por escrito del Director Nacional de Tecnologías de la Información y Comunicaciones.
- La configuración de los servicios tecnológicos en los ambientes de pruebas y producción, así como el paso a producción de las aplicaciones desarrolladas o adquiridas, son de responsabilidad del Área de Redes, Comunicaciones y Seguridad Informática de la Dirección Nacional de Tecnologías de la Información y Comunicaciones .
- Es responsabilidad del Área de Redes, Comunicaciones y Seguridad informática, monitorear los enlaces de comunicaciones, los servicios tecnológicos de esta Cartera de Estado, además de garantizar la continuidad de los servicios y comunicaciones del Ministerio de Salud Pública.

9.4 Propiedad de la Información

- Todos los funcionarios del Ministerio de Salud Pública que tengan asignado un equipo informático, estarán conscientes que los datos que se crean y/o modifican en todos los sistemas, aplicaciones y cualquier otro medio de procesamiento electrónico sea disco duro interno o externo, memoria flash, etc., durante el desarrollo normal de sus actividades laborales, son propiedad de la Institución.

- Todos los derechos de autor de un software, hojas de cálculo, archivos PDF o tipo de documentos, macros, base de datos, etc., y su respectiva documentación, creados por los funcionarios en ejercicio de sus actividades laborales, son de absoluta exclusividad del Ministerio de Salud Pública.
- La Dirección Nacional de Tecnologías de la Información y Comunicaciones será la encargada de resguardar los respaldos que tengan información de actividades laborales del Ministerio de Salud Pública y que fueron realizados o solicitados por los funcionarios, información que podrá ser entregada al momento de finalización de la dependencia laboral bajo pedido expreso a la citada Dirección.

9.5 Usos Inadecuados

Las actividades descritas a continuación quedan completamente prohibidas:

- Violar los derechos de autor, patentes o propiedad intelectual e industrial, en cualquiera de sus modalidades.
- La difusión de información confidencial.
- Instalar software malware (virus, gusanos, troyanos, rootkits, scareware, spyware, adware intrusivo, crimeware, entre otros) dentro de la red, computadoras o en los servidores del MSP.
- En ningún caso, se podrán utilizar los recursos informáticos de la Institución para actividades y/o difusión de contenidos que sean contrarias al ordenamiento jurídico.
- Utilizar la infraestructura tecnológica del Ministerio de Salud Pública, con ánimos de lucro.
- Igualmente se prohíbe el uso de los sistemas de comunicaciones del Ministerio de Salud Pública, con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
- Realizar cualquier tipo de actividad en la infraestructura tecnológica y de comunicaciones, que contravengan la seguridad del software o sistemas implementados o que generen interrupción o duplicación en los servicios.

- Realizar monitoreo de puertos o análisis de tráfico en la red del Ministerio de Salud Pública, con el motivo de evaluar seguridades y vulnerabilidades, la Dirección Nacional de Tecnologías de la Información y Comunicaciones es la responsable de la seguridad informática y puede realizar estas actividades o dar la respectiva autorización siempre y cuando tenga conocimiento su Director.
- Violación a los mecanismos de seguridad de información para evadir accesos por autenticación, y auditorias de red, software, internet o ingresos a cuentas de usuarios no autorizados.
- Interferir o negar el servicio de redes y comunicaciones tecnológicas del Ministerio de Salud Pública, con el propósito de lesionar el servicio con el uso de programas de envío de mensajes de cualquier tipo, vía intranet o internet.
- Instalar cualquier tipo de software en los equipos del Ministerio de Salud Pública, sin autorización previa de la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Compartir carpetas con derechos a todos los usuarios, la Dirección Nacional de Tecnologías de la Información y Comunicaciones, podrá cambiar los permisos de recursos compartidos de la red.
- Descarga de archivos de música o videos desde Internet.

9.6 Excepciones

El Despacho Ministerial, Subsecretarios, Coordinadores Generales, Directores de Áreas, Gerentes de Proyecto, y otros funcionarios internos que desempeñen funciones especiales dentro de la Institución, pueden solicitar accesos especiales a los equipos, red, sistemas y aplicaciones de la Institución sin que estas inciten a realizar violaciones a los accesos y Políticas, los cuales pondrían en riesgos la integridad de los funcionarios e Institución en general. El consenso de excepciones es debido a la responsabilidad atada a los cargos Directivos, dichas solicitudes deberán ser solicitadas mediante memorando en el cual se detallarán las características del usuario y las funciones que necesite que le sean habilitadas.

9.7 Políticas de Contraseñas

Todo funcionario del Ministerio de Salud Pública, es responsable de velar por la seguridad de las contraseñas a su cargo que utiliza para el acceso a los distintos servicios y recursos ofrecidos.

Toda contraseña es de uso exclusivo, y por lo tanto personal e intransferible.

- Todas las contraseñas del sistema (cuentas de administrador, cuentas de administración de aplicaciones, etc.), se cambiarán con una periodicidad de al menos una vez cada tres meses.
- Todas las contraseñas de usuario (cuentas de correo, cuentas de servicios web, etc.), se cambiarán al menos una vez cada seis meses.
- Ante la sospecha de que una contraseña haya sido revelada a terceros, se cambiará la misma de forma inmediata, y se procederá a notificar del incidente de seguridad, a la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Las cuentas de usuario que tengan privilegios de sistema, a través de su pertenencia a grupos o por cualquier otro medio, tendrán contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.
- Las contraseñas de los funcionarios que ingresan al Ministerio de Salud Pública, serán proporcionadas por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, luego de recibir el listado respectivo por parte de la Dirección Nacional de Talento Humano.
- Las contraseñas de los funcionarios que se desvinculan del Ministerio de Salud Pública, se desactivarán una vez que la Dirección Nacional de Tecnologías de la Información y Comunicaciones, reciba el listado respectivo por parte de la Dirección Nacional de Talento Humano.

9.8 Selección de Contraseñas

Se pondrá especial atención en la selección de contraseñas fuertes para la autentificación.

Una contraseña fuerte tiene las siguientes características:

- Más de ocho caracteres.
- Mezcla de caracteres alfabéticos, no alfabéticos y numéricos.
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal del usuario o de algún pariente cercano tal como número de teléfono, número de identificación, Cédula de Ciudadanía, fecha de nacimiento, etc.

9.9 Prohibición

- Revelar o compartir su contraseña de cualquier forma.
- Escribir la contraseña o almacenarla en archivos sin que sean encriptadas, comunicarla en el texto de mensajes de correo electrónico, o en cualquier otro medio de comunicación electrónica.
- Comunicar las contraseñas en conversaciones telefónicas.

9.10 Políticas de Internet y Correo Electrónico

- Los servicios de correo electrónico e internet, son administrados por la Dirección Nacional de Tecnologías de la Información y Comunicaciones. Para el enlace de Internet el proveedor es el responsable de garantizar su disponibilidad, de un mínimo de 99.6%.
- La Dirección Nacional de Tecnologías de la Información y Comunicaciones, monitoreará las actividades de la red, tanto para correo electrónico, internet y uso de red de datos con el fin de vigilar el cumplimiento de las políticas establecidas para el uso de tecnologías de información.

9.11 Correo Electrónico

- El correo electrónico es proporcionado con el objeto de apoyar las funciones de comunicación, de los Funcionarios del Ministerio de Salud Pública.
- El acceso a estos recursos, estará condicionado a la aceptación de la Política de Uso.
- El acceso a este servicio, se lo realiza por medio de la página web institucional (www.salud.gob.ec), link Webmail, o directamente desde la URL https://mail.msp.gob.ec.
- Las comunicaciones institucionales efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas institucionales creadas en la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Los buzones de correo electrónico, creados para los funcionarios del Ministerio de Salud Pública, son propiedad de éste, por tanto, también toda información contenida en ellos, su uso será para temas exclusivamente laborales.

9.12 Tipos de Cuentas

9.12.1 Cuentas Personales

El personal del Ministerio de Salud Pública, contará con una cuenta de correo, en el servidor de la Institución con capacidad de bandeja por defecto de 1GB, cuya dirección electrónica estará formada por el nombre y el apellido del usuario, separados por un punto (.) Salvo sus debidas excepciones (nombre.apellido@msp.gob.ec).

9.12.2 Cuentas Temporales

Estas cuentas se crearán bajo propósitos específicos, que serán detallados en el campo de texto "Notas" al momento de crearla. Además se especificará el tiempo de validez, para que sea borrada una vez que ya no se la necesite. El formato para este tipo de cuenta será el siguiente: proposito@msp.gob.ec.

9.12.3 Cuentas Departamentales

Estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada dirección o lista de usuarios específica, el formato para este tipo de cuentas será el siguiente: nombredirecciónolista@msp.gob.ec.

9.13 Responsabilidad de los Usuarios

- Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.
- La cuenta de correo es intransferible, por lo que no debe proporcionarse a otras personas.
- Los correos deberán ser marcados como urgentes únicamente cuando realmente lo sean.
- La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona, sin la autorización del remitente.
- En forma general un correo electrónico, deberá ser impreso únicamente cuando sea necesario, ya que esta herramienta fue creada para tener un archivo electrónico, agilizar las comunicaciones, descartar en la medida de lo posible el archivo tradicional y lograr un ahorro de papel.

9.14 Prohibiciones

- Utilizar el correo electrónico para actividades comerciales ajenas a la institución.
- Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo institucional.
- Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.
- Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico.
- Distribuir mensajes con contenidos inapropiados.

- Ofrecer su cuenta de correo electrónico a personas no autorizadas.
- Atentar contra la seguridad del servidor de correo de la institución.

9.15 Seguridad

- El usuario se compromete a crear una contraseña de características fuertes, que impidan el acceso a la cuenta por métodos de fuerza bruta o ingeniería social. Se considera fuerte a una contraseña que sea formada por letras mayúsculas, minúsculas, números, símbolos y con una extensión mínima de siete caracteres. Ej.: Passw0rd&
- El usuario se compromete en dar aviso al departamento de soporte a usuario, en el caso de cualquier fallo de seguridad con su cuenta, incluyendo accesos no autorizados, pérdida de contraseña, etc.
- El usuario se compromete en notificar al área de redes, en el caso de recibir correos sospechosos o de origen desconocido, así se evitarán las infecciones con virus, gusanos, phishing y malware en general. Bajo ningún aspecto abrirá o ejecutará archivos adjuntos a correos dudosos.

9.16 Internet

- Para equipos de cómputo personales, que necesiten permisos de internet, los funcionarios solicitarán a la Dirección Nacional de Tecnologías de la Información y Comunicaciones, el ingreso del equipo a la red del Ministerio de Salud Pública, para desempeñar sus actividades.
- La conexión a internet, solo podrá realizarse por los medios dispuestos por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, a cada uno de los diferentes funcionarios.
- No se podrá utilizar el internet del Ministerio de Salud Pública, como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley.
- La Dirección Nacional de Tecnologías de la Información y Comunicaciones, asignará a cada usuario, permisos y perfiles de navegación dependiendo de las actividades que realice. Si se necesita habilitar cualquier contenido de internet a los usuarios, los

Directores de cada área enviarán el listado de personal, a que páginas de internet y con qué objetivo, a la antedicha Dirección.

- Si la conexión a internet se encuentra habilitada por USB móvil, se deberá desconectar el equipo de cómputo de la red del Ministerio de Salud Pública, sea ésta por medio cableado o inalámbrico, y solo podrán utilizar este medio los funcionarios que tienen permiso de conexión recibido por la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- La Dirección Nacional de Tecnologías de la Información y Comunicaciones, en coordinación con la Dirección Nacional Administrativa, es la única encargada de solicitar enlaces de datos e internet, aumento de ancho de banda, o suspensión de servicio a proveedores.

9.17 Políticas de Software

9.17.1 Políticas de administración e Instalación de Software

La Dirección Nacional de Tecnologías de la Información y Comunicaciones, será la única área encargada de la administración, instalación, soporte y funcionamiento del software instalado en el Ministerio de Salud Pública, sea web o de escritorio. Dentro de las responsabilidades de la administración e instalación de software se describe las siguientes:

- Mantener bajo resguardo las licencias de uso de software de la institución, además de llevar un control de las licencias que se encuentran en operación y uso.
- Mantener actualizado el catalogo de software (libre o propietario) de la Institución, desinstalar el software de las computadoras que no posean licencias o que no estén aprobadas por la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Previa la instalación de software libre en los equipos, se deberá verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software, de conformidad a lo dispuesto por el Decreto Ejecutivo No. 1014.
- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en

riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno, según las disposiciones del Decreto Ejecutivo No. 1014.

- Generación de estándares de software institucional (software instalado en las computadoras del Ministerio de Salud Pública, antes de ser entregados al usuario final)
- Generación de estándares de software adicional, que será de uso exclusivo de la Dirección Nacional de Tecnologías de la Información y Comunicaciones, entre los cuales se pueden encontrar los siguientes:

    - Software preinstalado en el equipo de cómputo.
    - Software de actualización remota.
    - Software de acceso a componentes en los servidores de la institución.
    - Software de uso emergente (previo análisis de licencia y seguridad).
    - Generación de estándares de software de soporte (sistema informático que viene junto a la adquisición de un artículo como cámaras, IPAD, periféricos, etc.)

En la administración de software no se podrá instalar lo siguiente:

- Copias ilegales de cualquier sistema informático, software o programa.
- Software descargado desde internet.
- Software que no haya sido aprobado por la Dirección Nacional de Tecnologías de la Información y Comunicaciones.
- Software adquirido para uso personal sin fines institucionales.
- Software de entretenimiento.

Para el requerimiento de instalación de software en las computadoras del Ministerio de Salud Pública, que no se encuentren definidos por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, se enviará una solicitud de instalación vía memorando, para que se realice el análisis correspondiente del software y su posterior implementación, en el caso que el pedido sea autorizado.

10. Vigencia de las Políticas

Las Políticas descritas en el documento entrarán en vigencia, desde su aprobación por la máxima autoridad del Ministerio de Salud Pública y serán revisadas y actualizadas por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, de acuerdo a los cambios en la infraestructura y servicios de tecnologías de la Institución.

11. Incumplimientos a la Política

El desconocimiento de la presente Política no exime a los funcionarios de las sanciones correspondientes por incumplimientos.

12. Actuaciones en caso de incumplimiento

En caso de incumplimiento de la presente regulación, se advertirá del hecho al infractor, pudiéndose generar la suspensión temporal con carácter cautelar del acceso a los recursos informáticos y servicios de red con la aprobación de la Autoridad Máxima de la Institución. En caso de que el usuario no responda o ignore la advertencia, se procederá con la suspensión total de los accesos a todos los recursos y servicios.

Para casos de reincidencia (por tercera vez) en el incumplimiento de una de las políticas citadas, se comunicará a la Dirección Nacional de Talento Humano sobre el particular, para que dicha Dirección proceda de acuerdo a lo señalado en las normas vigentes.

Todo lo anterior se entiende sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan.

13. Glosario.

- **Recursos informáticos**: Todos los medios de cualquier naturaleza, físicos o lógicos que intervienen en los sistemas de información y en las redes de comunicaciones.
- **Red de Comunicación Institucional**: Infraestructura de comunicaciones de propiedad o bajo la supervisión del Ministerio de Salud Pública, accesible por los Funcionarios mediante la cual se transmiten los mensajes de voz, datos, imágenes y señales de control. Esta red para permitir la comunicación completa está conectada con redes externas que constituyen lo que se denomina extranet.
- **Servicio de red**: Cualquier servicio o aplicación que utilizando la red ministerial permite a los funcionarios, comunicarse entre sí o con terceros y acceder o compartir información, bien accediendo a la intranet o a la extranet. Son ejemplos de servicios de red: el correo electrónico, servidores de páginas web, el teléfono, etc.
- **Responsable y usuario**: Para cualquier recurso informático y servicio de red, ya sea central, de Centro, Departamental, de Direcciones o Subsecretarias, existirá un responsable y dos categorías de usuarios denominadas Administrador de los recursos y Usuario.
- **Responsable de los recursos informáticos**: Es la persona que ha de velar por el buen uso de los recursos bajo su tutela.
- **Administrador de los recursos informáticos**: Es la persona encargada de gestionar los recursos informáticos conectados directa o indirectamente a la Red de la Institución pertenecientes a la Dirección Nacional de Tecnologías de la Información y Comunicaciones. Los Responsables nombrarán a los Administradores de los recursos informáticos y estos a su vez comunicaran al Responsable todas las incidencias que detecte y que puedan afectar al buen funcionamiento de los recursos.
- **Usuario**: Es la persona que tiene alguna vinculación con el Ministerio de Salud Pública y utiliza los recursos o servicios informáticos ofrecidos por esta Secretaria de Estado.
- **Identificador**: Información, frecuentemente constituida por una cadena de caracteres, que identifica a un usuario en los sistemas informáticos.
- **Contraseña**: Información, frecuentemente constituida por una cadena de caracteres, que se utiliza en el proceso de autenticación de un usuario.

- **Identificación y autenticación**: Procedimientos de reconocimiento y comprobación, respectivamente, de la identidad de un usuario.
- **Control de acceso**: Mecanismo que en función a la identificación y autenticación permite acceder a los servicios Institucionales.
- **Cuenta de usuario**: Se denomina así la personalización de un servicio de red para su uso por un usuario. Normalmente la utilización personalizada de un servicio de red conlleva la asignación de un identificador y una contraseña que permiten al usuario la utilización personal de dicho servicio y el acceso al espacio virtual restringido del mismo. Por ejemplo la cuenta de usuario del correo electrónico.
- **Servidor**: Equipo informático que proporciona a los usuarios uno o varios servicios de red. (por ejemplo un servidor de archivos o un servidor de correo electrónico)
- **Lista de distribución**: Servicio de red que agrupa a un conjunto de direcciones electrónicas bajo un solo nombre "lista" y permite enviar mensajes de correo electrónico a todas las direcciones incluidas en la lista.

Anexo Nº6

Formulación de preguntas para la entrevista con responsable de Tecnología y dirección del centro de salud.

1.- ¿Nombres, apellidos y cargo en la unidad de salud?

2.- ¿Qué tal es el servicio de internet en el centro de salud?

3.- ¿Cuáles son los principales problemas que usted puede observar en el uso de la web?

4.- ¿Quienes acceden al servicio Wifi del Centro de Salud?

5.- A parte del servicio web, ¿existen otros inconvenientes?

6.- ¿Cómo contralan el acceso web?

7.- ¿Qué políticas se debe implementar?

8.- ¿Existen Normativas Internas? ¿Cuáles son?

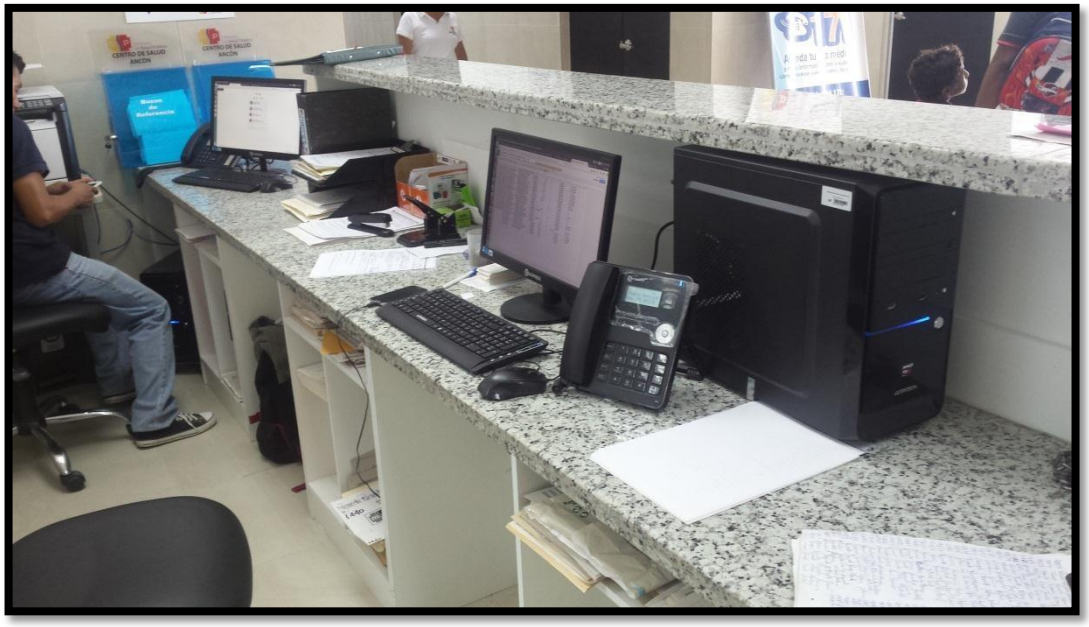
10.- ¿La implementación de este proyecto será de gran utilidad para la filtración de contenido y mejorar los recursos web?

Anexo Nº7

Fotos del Centro de Salud San José de Ancón

Entrada Principal

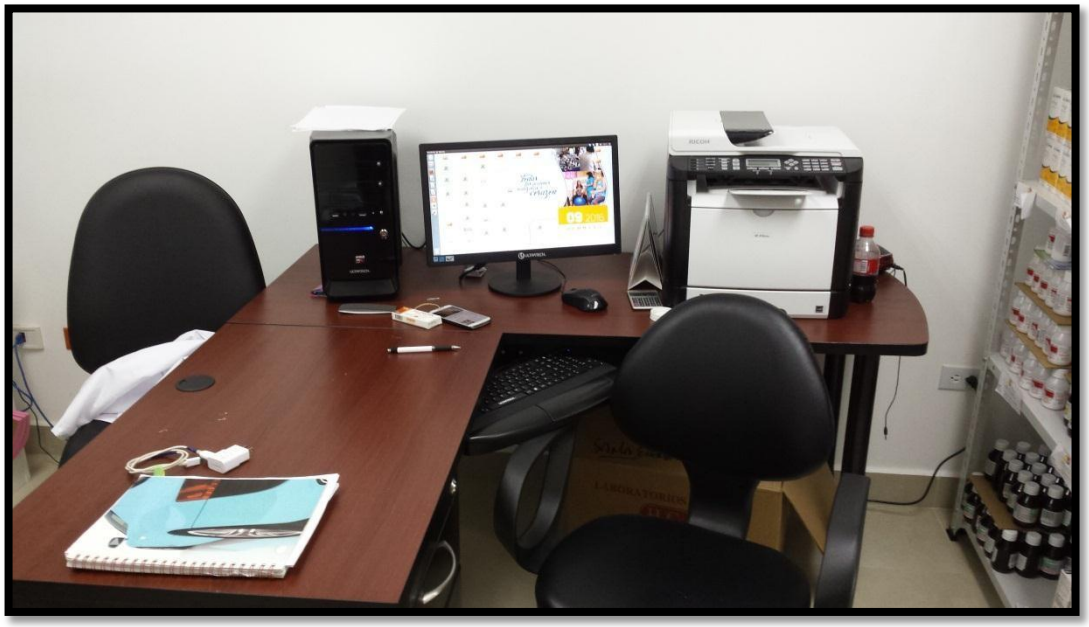
Rack de Servidor



Estaciones de Trabajos

Sala Múltiple Audio-Visual

Consultorio Médico



Departamento Administrativo

Sala de Espera

Televisores Informativos