IMPLEMENTACION DE UN SERVIDOR RADIUS PARA MITIGAR LOS RIESGOS DE ACCESO NO AUTORIZADO A LA RED INALÁMBRICA DEL HOSPITAL UNIVERSITARIO DE SANTANDER

GONZALO CARRILLO ARIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2015

IMPLEMENTACION DE UN SERVIDOR RADIUS PARA MITIGAR LOS RIESGOS DE ACCESO NO AUTORIZADO A LA RED INALÁMBRICA DEL HOSPITAL UNIVERSITARIO DE SANTANDER

GONZALO CARRILLO ARIAS

Trabajo de grado para optar el Título de:

Especialista en Seguridad Informática

Director de Proyecto:

Ing. John Freddy Quintero Tamayo. MS (c)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2015

Nota de aceptación

_____

_____

_____

Presidente Jurado

_____

Jurado

_____

Jurado

_____

Bucaramanga, Octubre de 2015

AGRADECIMIENTOS

El autor:

Quiero expresar mi agradecimiento a la Empresa Social del Estado Hospital Universitario de Santander, quien con su ayuda ha contribuido a que pudiera realizar y culminar este trabajo.

En especial agradezco al ing. John Freddy Quintero Tamayo, su desinteresada y eficaz colaboración en la realización del presente trabajo, por su intensa labor en la orientación, dirección y supervisión realizada.

CONTENIDO

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pag.

INTRODUCCION

Con el avance de las tecnologías la demanda de los usuarios en las empresas y con las constantes modificaciones estructurales, así como el uso de material movible en las infraestructuras físicas de las empresas nos obliga cada vez más a implementar soluciones de conectividad vía *WiFi*, al igual que los múltiples equipos recientes con distintas tecnologías con características como alcance para una mejor cobertura y cifrado para una mejor seguridad en redes de datos tenga una gran importancia en la aplicación de las diferentes alternativas de solución.

Como encargados de la seguridad informática es nuestro deber garantizar que los usuarios naveguen de manera segura en cada infraestructura que implementemos, y que de igual forma puedan transportar sus datos seguros sin que se pierda o altere información alguna, otra de nuestras obligaciones es que los usuarios que se conecten realicen sólo las tareas que están estrictamente autorizadas en los protocolos de seguridad de las empresas, de manera que se garantice y minimice un posible acto de vandalismo o de infiltración de los ciberdelincuentes.

A continuación podemos encontrar la definición del entorno, que describe cada una de las fases investigadas, y detalla claramente la situación actual que hay en la red inalámbrica de la ESE Hospital Universitario de Santander.

Para el caso en concreto se plantea la configuración y puesta en funcionamiento de un Servidor RADIUS que servirá para minimizar el riesgo encontrado en el acceso a la red inalámbrica de la ESE Hospital Universitario de Santander.

1. SITUACION ACTUAL DE LA INALAMBRICA DE LA ESE HUS

1.1 DESCRIPCION

Actualmente, el Hospital Universitario de Santander ofrece el servicio de acceso al sistema integrado “Dinamica.net” que maneja por módulos tanto lo General, lo Financiero y lo Medico – Asistencial además de internet ya que se hace necesario para consultas de tipo investigativo, no sólo mediante una infraestructura de red cableada, sino también de forma inalámbrica.

Aunque Dinamica.net cuenta con manejadores de Bases de Datos que garantizan la seguridad de la información y también cuenta con un sistema de seguridad por usuario con su correspondiente clave de acceso que autoriza o restringe sus actividades, no se puede desconocer que existe vulnerabilidad en el acceso a la red inalámbrica ya que se puede presentar que las dos claves de configurar la inalámbrica sean usadas por personas con conocimientos básicos en sistemas y empleadas para configurar equipos sin el respectivo licenciamiento del sistema operativo y que no cuenten con un antivirus actualizado lo cual sería blanco fácil para generar un ataque desde el exterior de la institución, con sus respectivas consecuencias teniendo en cuenta que la razón de ser del Hospital son sus pacientes y por ende la privacidad y confidencialidad de la historia clínica ya que es un derecho tan así que ni siquiera un familiar sin la respectiva autorización puede tener acceso a la misma.

Cada semestre académico se le configura el acceso al sistema a gran cantidad de estudiantes de las diferentes universidades que hacen sus prácticas en la institución y por lo general cuando terminan su ciclo se van y en sus equipos personales continua la configuración de acceso a la red de datos lo que causa un numero de máquinas fuera de la institución que potencialmente podrían facilitar las claves de acceso a la inalámbrica a personal externo con malas intenciones.

De permanecer este riesgo sin controlar se pondría en peligro la confidencialidad de los datos de la institución, especialmente las historias clínicas de los pacientes.

1.2 FORMULACIÓN

¿Se mitigará el riesgo de acceso no autorizado a la red inalámbrica con la implementación de un Servidor RADIUS?

2. JUSTIFICACIÓN

A la par como van creciendo la cantidad de nuevas conexiones a bajos costos y mayor velocidad también va creciendo la inseguridad en las redes inalámbricas, este es un dolor de cabeza que no ha recibido la solución adecuada por la mayor parte de administradores de redes y los responsables de la información, aunque sabemos que no hay una red que no pueda ser accedida ilegalmente, podemos reducir las vulnerabilidades para tener unos riesgos controlados.

Lo preocupante de esta situación es que la mayoría de los administradores de redes tal vez no visualizan los alcances negativos de usar estas conexiones en la red de una empresa sin la debida seguridad.

Al navegar equipos posiblemente infectados de virus informáticos pueden generar fallas a la red y también se está generando un problema de orden legal con Microsoft ya que el Hospital legalmente responde por todo equipo que se conecte a la red aunque no sean de la entidad.

Es usual encontrar redes en las cuales el acceso a Internet está protegido apropiadamente con cortafuegos configurado, pero dentro de la red hay *access point* con alcance de señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal, tendrá acceso a la red del Hospital en este caso, con la posibilidad de conectarse a la red de la empresa y desde esta conectarse hacia otras estructuras para luego desconectarse y no ser detectado, robar *software* y/o información, introducir *software* maligno entre muchas otras cosas. Es por este motivo que se toma la decisión de implementar el servidor RADIUS con el fin de mantener un control sobre los usuarios que se conectan a la red inalámbrica de la ESE HUS.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar un servidor RADIUS para mejorar el nivel de seguridad en la red inalámbrica del Hospital Universitario de Santander.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar amenazas y vulnerabilidades en la seguridad inalámbrica.
- Recopilar información de las características técnicas de los dispositivos inalámbricos que se encuentran instalados en el edificio del hospital.
- Adecuar la máquina que va a servir de Servidor RADIUS, en lo referente a sistema operativo y actualizaciones.
- Configuración y puesta en funcionamiento de un Servidor Radius.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

El hombre desde hace muchos siglos se la ha ingeniado para transmitir mensajes cifrados, veamos cuales han sido sus principales inconvenientes presentados con el desarrollo de estos, en especial con el tratamiento de la seguridad de la información y protección de datos.

La seguridad de la información es todo lo que conlleve a proteger y salvaguardar la información de todos y cada uno de los peligros que esta tenga al asecho con el fin de que la misma cumpla con ciertos requisitos, tales como: confidencialidad, disponibilidad e integridad, no diferente a la seguridad informática ya que lo que esta última busca es la misma seguridad pero en medios informáticos, desde principios de la historia del hombre podemos encontrar que este ha tratado de esconder cierto tipo de información respecto a los demás hombres utilizando este aspecto en ventajas que serían usadas en un tiempo determinado, es así como en la antigüedad surgen las bibliotecas, lugares donde se podían resguardar la información para transmitirla y así evitar que otros la obtuvieran.

Entre las primeras muestras de protección de la información la encontramos en el *Sun Tzue* en el arte de la guerra y se vuelve a señalar con Nicolás Maquiavelo con su obra el príncipe, donde señalan la importancia de la información sobre sus adversarios, en la Antigua Grecia con la creación de los primeros intentos criptográficos tales como la *escítala* quien usa el cifrado de transposición, luego para la época de los Romanos, Julio Cesar utilizaba un lenguaje de cifrado para referirse a sus comandantes.

Llegado el auge de las computadoras hacía finales de los años 80, *James P Anderson* integrante de las fuerzas armadas norteamericanas publica uno de los primeros textos que habla sobre la seguridad en los computadores.

Algunos estudios se realizan durante los años siguientes hasta que en 1980 *James P. Anderson* escribe "*Computer Security Threat Monitoring and Surveillance*", es dónde se da comienzo para detección de intrusos en sistemas de computadores principalmente mediante la consultas de ficheros log.

Entre 1984 y 1996, *Dening y Neumann* desarrollan el primer modelo denominado IDES (*Intrusion Detection Expert System*) basado en reglas. Desde este momento,

se han ido proponiendo y creando nuevos sistemas de detección de intrusos hasta obtener una separación clara entre los sistemas que efectúan la detección dentro de los ordenadores y aquellos que la efectúan en el tráfico que circula por la red.

Las redes inalámbricas (WLAN) son un tema que ha generado controversia en el terreno empresarial; en la mayoría de las empresas se cuenta con una WLAN de algún tipo o al menos, se han sopesado las ventajas y los inconvenientes de la tecnología inalámbrica. En cualquier caso, a las empresas que han implementado redes inalámbricas les suele preocupar la seguridad de la solución utilizada, en tanto que a las que han rehuido de la tecnología inalámbrica tienen la duda de haber podido perder una evidente productividad y un considerable ahorro en infraestructura por su simplicidad y rápida instalación.

Por lo general los responsables de tomar decisiones tecnológicas han sentido en el pasado un miedo justificado acerca de la seguridad de la tecnología inalámbrica e, incluso en la actualidad, dicha tecnología lleva el estigma de no haber sido nunca segura, debido a la detección y divulgación de brechas de seguridad. A pesar de que se han desarrollado muchas soluciones alternativas a lo largo de los años, las soluciones comunes que se han diseñado para abordar los problemas de la seguridad inalámbrica han tenido fallas que representan un valor monetario elevado ya que hablamos de la pérdida del activo más importante de las empresas que es la información.

En las últimas etapas de las redes inalámbricas se han producido numerosos avances de igual manera la tecnología ha mejorado para admitir velocidades superiores y hay más confiabilidad, también los estándares garantizan la seguridad de las transmisiones inalámbricas. Estos estándares, si se configuran correctamente, son mucho más seguros y se pueden utilizar con un elevado nivel de confianza pero por lo general cuando se instala un *router* o un AP cometemos el error de dejar la configuración que trae por defecto y es esto lo que la hace tan vulnerable.

Debido a que su medio de transporte es el aire, las redes inalámbricas son inseguras, es por ello que se debe tener en cuenta en este tipo de redes la encriptación. Lo que más se debe utilizar es WPA y WPA2, que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso.

4.2 MARCO NORMATIVO

4.2.1 "Normas 802.x para la especificación de redes inalámbricas. El grupo de normas 802 describe las recomendaciones para las redes. La sección de las redes inalámbricas comienza con el código 802.11, el cual es seguido por una letra, la cual asigna a cada norma un único identificador a pesar de que todas ellas comparten el código 802.11.

4.2.2 Normas globales. Todas las normas 802 se originaron en el Instituto de Ingenieros Eléctricos y Electrónicos. La IEEE (siglas en inglés) tiene varios grupos de trabajo relacionados con la parte de redes. Cada uno de estos grupos de trabajo se especializa en la generación de normas para un aspecto particular relacionado con éstas. Cada grupo de trabajo lleva un código y asigna ese código en todas sus normas. Los dos grupos más conocidos son los asignados con las normas 802.3, los cuales se especializan en las normas *Ethernet* y 802.11, que cubren las redes *Wi-Fi*"[1].

4.2.4 "*Wi-Fi CERTIFIED*. Es el logotipo que se otorga a los equipos de *WLAN* que pasan las pruebas de funcionalidad e interoperabilidad de la Alianza *Wi-Fi*. Un equipo certificado con este logotipo, funciona con cualquier otra pieza de red inalámbrica que también cuente con el mismo logotipo.

4.2.3 Alianza *Wi-Fi* ó *Wi-Fi Alliance (Wi-Fi).* La Alianza ***Wi-Fi (Wireless Fidelity)*** es una asociación internacional sin fines de lucro que fue formada en 1999. Se formó para certificar la interoperabilidad de productos *WLAN* basados en la especificación IEEE 802.11. El objetivo de la alianza *Wi-FI* es mejorar la experiencia del usuario mediante la interoperabilidad de los productos.

4.2.5 *Wireless LAN Association (WLANA).* Es una asociación comercial educativa sin ánimo de lucro, cuyo objetivo es brindar información al público en general, usuarios e industrias sobre temas relacionados con *WLAN*, como por ejemplo, aplicaciones, tendencias, problemas, disponibilidad, etc. También cuenta con programas de certificación como por ejemplo la *CWNA (Certified Wireless Network Administrator)*"[2].

---

[1] Texto recuperado de la página web http://www.ehowenespanol.com/normas-802x-especificacion-redes-inalambricas-info_295325/

[2] Texto recuperado de la página web http://es.wikipedia.org/wiki/Organizaciones_Certificadoras_y_Reguladoras_Inal%C3%A1mbricas

4.2.6 "*Federal Communications Commission (FCC)*. Es la agencia gubernamental de Estados Unidos. Es responsable de regular las comunicaciones interestatales e internacionales por radio, televisión, satélite y cable. Casi todos los países tienen una agencia reguladora que vigila el uso del espectro de radio o espectro de frecuencias en ese país. En otros países lo hacen los ministerios de correos y telecomunicaciones, por ejemplo, en Perú el encargado es el Ministerio de Transportes y Comunicaciones.

4.2.7 *Underwriters Laboratories Inc. (UL)*. Es una organización sin fines de lucro de certificación y prueba de la seguridad de los productos o equipos, tiene una reputación de ser líder en la prueba y certificación de productos en cuanto a su seguridad. UL es uno de los asesores más reconocidos y acreditados del mundo. El logotipo de UL significa que el producto ha sido aprobado en cuanto a requisitos de seguridad para su normal operación.

También significa que las comprobaciones periódicas de las instalaciones de fabricación certificadas por UL han reafirmado este estado de seguridad.

En el año 2001, 64482 fabricantes diferentes fabricaron productos certificados por UL y alcanzó 190 millones de clientes con mensajes de seguridad en Estados Unidos y Canadá.

4.2.8 *European Telecommunications Standards Institute (ETSI)*. Es una organización sin ánimos de lucro cuya misión es producir los estándares de telecomunicaciones que se utilizaran en Europa y otros lugares. El ETSI tiene miembros de 52 países que se extienden más allá de Europa. El ETSI representa a operadores, fabricantes, proveedores de servicios, investigadores y usuarios. Las actividades del ETSI están determinadas por las necesidades del mercado expresadas por sus miembros. El ETSI juega un papel importante en el desarrollo de estándares y documentación técnica"[3].

4.3 MARCO CONTEXTUAL

4.3.1 Nombre de la empresa. Empresa Social del Estado Hospital Universitario de Santander.

[3] Texto recuperado de la página web http://es.wikipedia.org/wiki/Organizaciones_Certificadoras_y_Reguladoras_Inal%C3%A1mbricas

4.3.2 Reseña histórica. La E.S.E Hospital Universitario de Santander, creado mediante decreto 0025 de 2005, es una Institución Pública de orden Departamental, prestadora de servicios de salud de mediana y alta complejidad con estándares de Calidad, que en cumplimiento de su Misión busca mejorar continuamente sus procesos de atención en búsqueda de la implementación de los estándares superiores de calidad establecidos en el Sistema Único de Acreditación.

La ESE Hospital Universitario de Santander es una institución dedicada a contribuir al mejoramiento de la calidad de vida de la comunidad del nororiente colombiano, mediante el trabajo de un equipo humano calificado, con apoyo tecnológico, a través de un proceso administrativo transparente y el compromiso con la academia, apoyado en la investigación y generación de conocimiento.

Su compromiso con la academia, apoyado en la investigación y generación de conocimiento, la ha posicionado como una de las instituciones más representativas en prestación de servicios de salud en el Departamento.

Actualmente la ESE Hospital Universitario de Santander presta 7 servicios de salud de mediana y alta complejidad, su estructura la constituye un edificio de 11 pisos con una capacidad de 384 camas, distribuidas entre hospitalización, observación, consulta externa, servicio de urgencias, quirófanos y partos, en donde se internan usuarios que requieren diagnóstico y tratamiento en las diferentes especialidades médicas y médico quirúrgicas.

La unidad de cuidados intensivos para adultos cuenta con 12 camas y la neonatal y pediátrica con 8 camas, también cuenta con una moderna unidad de cuidados en quemados con capacidad para albergar 13 adultos y 8 pediátricos, cada una con la mejor tecnología en equipos de monitoreo, en donde los usuarios permanecen al cuidado del mejor equipo médico científico con el ánimo de garantizar la mejor atención personalizada.

Cuenta con 7 salas de cirugía, 2 salas de partos y 1 servicio de imagenología y laboratorio clínico donde se realizan diversos procedimientos e intervenciones con el apoyo de tecnología adecuada, y dos sedes ambulatorias con 13 consultorios debidamente dotados para consulta médica general y especializada.

Así mismo cuenta con el Hemocentro de Santander, antes Banco Metropolitano de Sangre, el único centro de acopio de unidades de sangre público del

departamento de Santander, que proyecta suplir las necesidades de sangre de toda la comunidad santandereana.

Finalmente su unidad de Oncología Y Radioterapia cuenta con la más adelantada tecnología disponible en el área de Radioterapia y las mejores instalaciones para la aplicación de Quimioterapia, con lo que se asegura una óptima atención desde el punto de vista profesional y físico.

4.3.3 "Misión. Somos la E.S.E. Hospital Universitario de Santander, institución que presta servicios de salud de mediana y alta complejidad, con énfasis en docencia e investigación, basados en criterios éticos, técnicos, científicos y de gestión integral, que nos constituye como centro de referencia de la red pública del nororiente colombiano y el resto del país, involucrando la participación de talento humano competente que realiza sus actividades con sentido humano y alineado con los valores y principios organizacionales. Para lograr lo anterior la organización está comprometida con el trato digno y humanizado, y la provisión de entornos de atención seguros y con tecnología de avanzada.

4.3.4 Visión. Para el año 2020 la E.S.E Hospital Universitario de Santander se consolidará como una institución prestadora de servicios de salud de alta complejidad, acreditada, competitiva y líder en la generación de conocimiento humano, con enfoque de seguridad, humanización y responsabilidad social.

La E.S.E. Hospital Universitario de Santander será líder en el uso eficiente y transparente de los recursos para la ejecución de sus procesos, que aseguren sostenibilidad financiera, mejoramiento continuo de las condiciones laborales y evidentes márgenes de rentabilidad económica y social.

4.3.5 Políticas institucionales. El Hospital Universitario de Santander desarrolla cada una de las Políticas Institucionales como se observa en la figura 1, identificando el compromiso de la Gerencia con la prestación de servicios de salud con óptima calidad éstas serán las responsables de motivar al equipo de colaboradores en la implementación de los estándares del Sistema Único de Acreditación en la E.S.E. HUS"[4].

[4] **Fuente:** Tomado de los documentos privados de la ESE HUS.

Figura 1. Políticas institucionales

Fuente: http://hus.gov.co/index.asp?id=2&ide=105&id_seccion=75&elado=

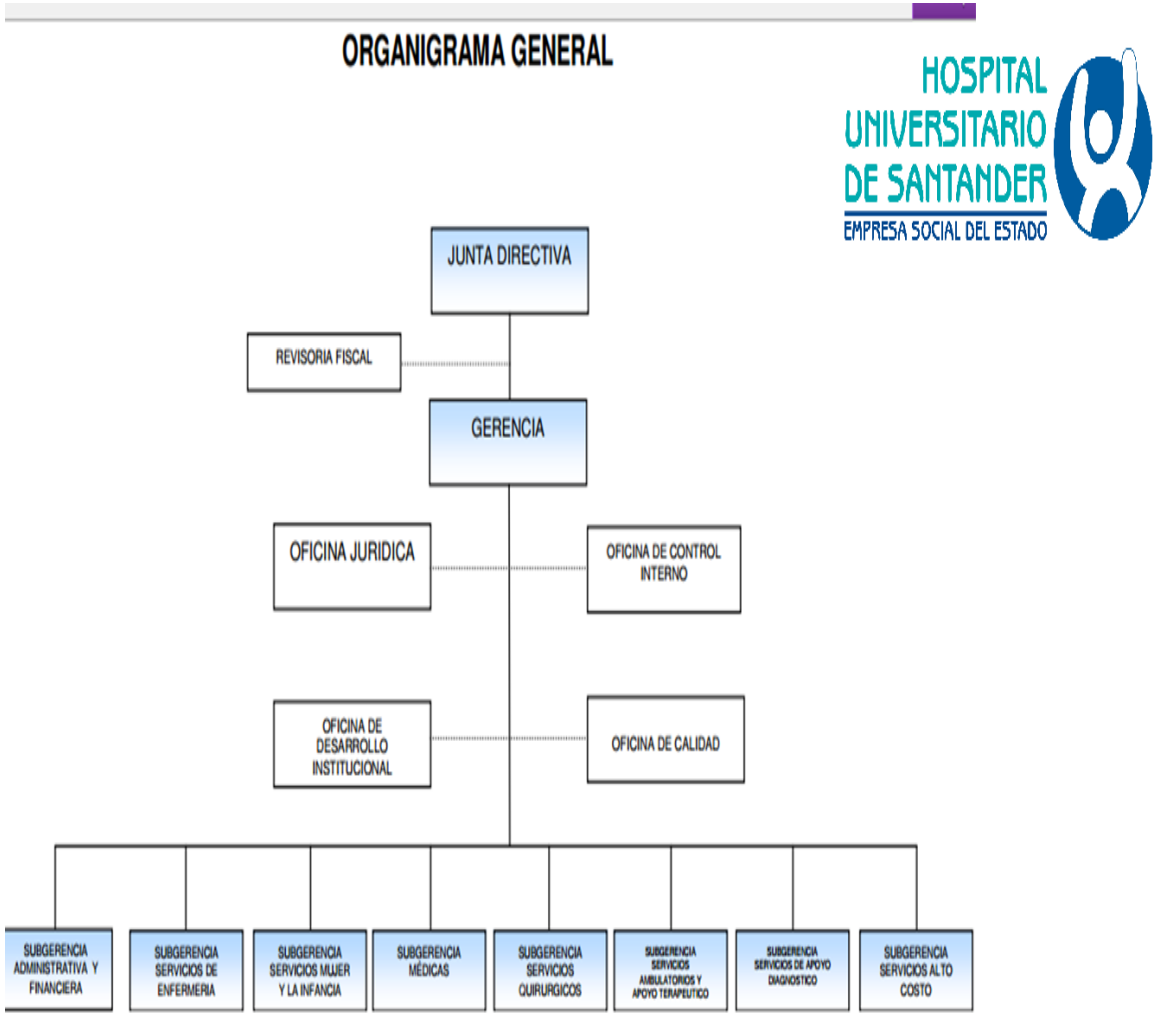
Solo se enuncia a continuación la política de gestión de la tecnología.

- **Política gestión de la tecnología**

La ESE HUS se compromete en la implementación de un Sistema de Gestión de Tecnología, que permita la adquisición, instalación, uso y mantenimiento seguro y eficiente de la tecnología biomédica y no biomédica, acorde a las necesidades de los pacientes y el nivel de complejidad de los servicios ofertados por la institución.

4.3.6 Estructura orgánica. Representada en el organigrama que se usa en la ESE Hospital Universitario de Santander como se observa en la figura 2 en la página siguiente, desde su creación y que hoy día por el proceso de acreditación que se lleva a cabo se encuentra en transición hacia una organización por procesos que se explica a fondo más adelante.

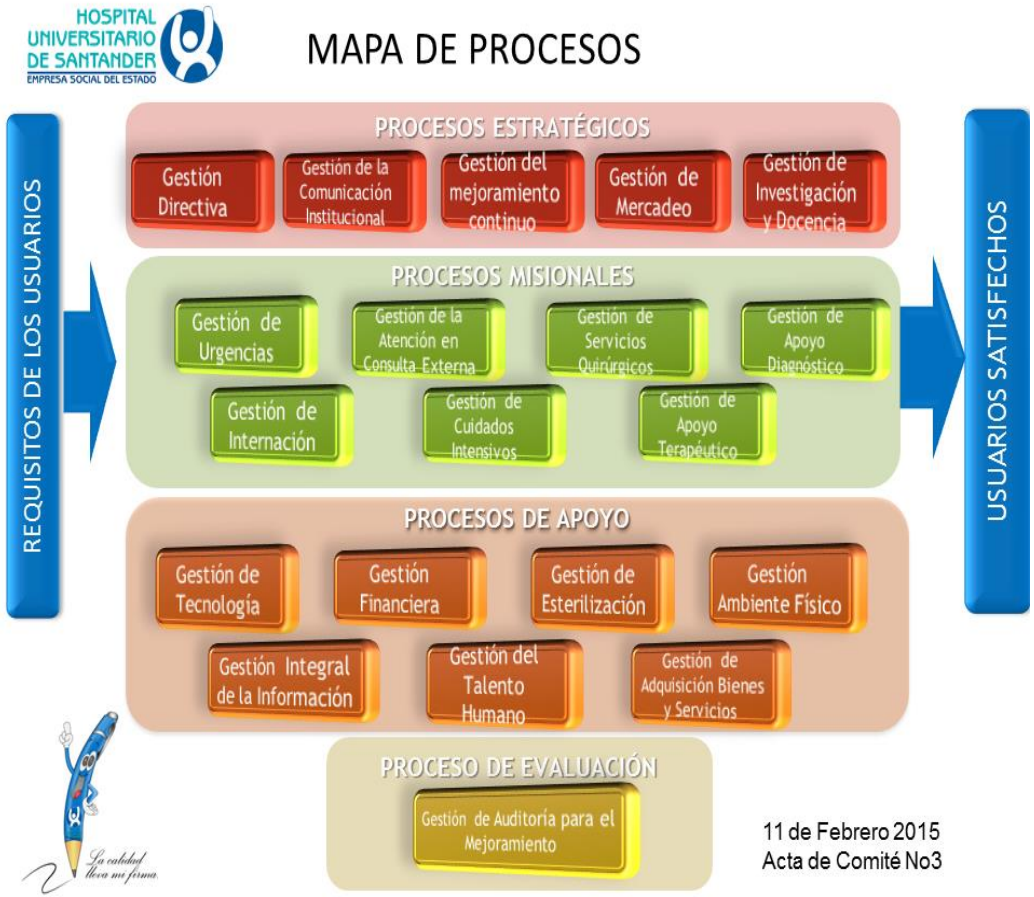
Figura 2. Organigrama general HUS



Fuente: http://hus.gov.co/index.asp?id_seccion=57&id=1&elado=

Se presenta el mapa de procesos como se observa en la figura 3, que entrara a reemplazar al organigrama general de la ESE HUS.

Figura 3. Mapa de procesos HUS



Fuente: http://hus.gov.co/index.asp?id_seccion=57&id=1&elado=

4.3.7 Descripción de los procesos relacionados. Solo se enuncian los procesos relacionados con la unidad Funcional de Recursos Informáticos y de Información.

"Procesos de Apoyo

- **Gestión de la Tecnología:** Establecer las necesidades de tecnología biomédica y desarrollar la correcta administración de los equipos biomédicos existentes en la ESE HUS de manera eficiente, segura y oportuna.

- **Gestión Integral de la Información:** Planear y administrar los sistemas de información e infraestructura tecnológica de la ESE HUS de manera oportuna, integral que asegure la continuidad del servicio, brindando estadísticas que permitan el estudio y análisis de indicadores, para la toma de decisiones, involucrando el manejo adecuado de la HISTORIA CLINICA , los documentos administrativos y asistenciales satisfaciendo las necesidades de información de la institución y la comunidad, proponiendo estrategias para la integralidad y confidencialidad de la información.

4.3.8 Perfiles de los profesionales que intervienen en el proceso de Seguridad Informática de la ESE HUS. De acuerdo a la estructura actual de la institución, la Unidad Funcional de Apoyo Tecnológico y de Información, en adelante UFATI, está dirigida por un Profesional Especializado, también cuenta con un Técnico que apoya las labores de toda la unidad, la UFATI tiene a cargo tres grupos de trabajo: Sistemas, Estadística y Gestión documental.

El grupo de trabajo de Sistemas de la Información está dirigido por un Profesional Universitario quien a su vez es el administrador de redes y que coordina la mano de obra tercerizada de soporte tanto en Hardware como en *Software* compuesto por cinco ingenieros, seis técnicos informáticos y un técnico administrativo.

En el proceso de Seguridad Informática intervienen integrantes de la Gerencia y de las diferentes subgerencias pero debido a lo específico de los temas que le competen son los tres profesionales de la UFATI los que se encargan de proponer, desarrollar proyectos, socializarlos y en fin cubrir lo relativo a la seguridad informática y telecomunicaciones. El comité de Seguridad Informática se creó mediante resolución 000405 del 17 de agosto de 2011 con el fin primordial de proteger la información mediante medidas de seguridad indistintamente si esta en papel o en forma electrónica y por qué medio se transmite"[5].

[5] **Fuente:** Tomado de los documentos privados de la ESE HUS.

“Por lo anterior se hizo necesario regular políticas de seguridad informática, esto se logró por medio de la creación de las Políticas de Seguridad Informática con la aprobación de la Resolución 000232 del 31 de mayo de 2012.

El perfil de la Profesional Especializada que está al frente de la UFATI es el siguiente:

- Título Profesional Universitario en Ingeniería de Sistemas o de Telecomunicaciones y Postgrado en Áreas relacionadas con las funciones del cargo o su equivalencia de acuerdo con el Artículo 25 del Decreto 785 de 2005.

Además conocimientos en:

- Gerencia en sistemas de información y redes.
- Manejo de Talento Humano.
- Presupuesto público.
- Contratación estatal.
- Salud Ocupacional.
- Modelos Estratégicos.
- Estructura organizacional.
- Estructura del estado Colombiano.
- Planeación estratégica.
- Sistema general de seguridad social.
- Norma Técnica de Control de Gestión Pública (NTCGP) 1000-2004.
- Norma ISO.
- Competencia comunicativa.
- Sistema tarifario sector salud.
- Facturación y glosas.
- Gestión de control.
- Actualización en normatividad vigente.
- Formulación de proyectos de investigación.
- Procesos, procedimientos y protocolos.
- Metodologías de investigación y diseño de proyectos.
- Metodología de evaluación de proyectos y desempeño laboral.

El perfil del Profesional Universitario que está al frente del Grupo de Sistemas es el siguiente:

- Título Profesional en Ingeniería de Sistemas o Telecomunicaciones”[6].

[6] **Fuente:** Tomado de los documentos privados de la ESE HUS.

“Además conocimientos en:

- Gerencia del manejo en sistemas de información.
- Conocimientos generales en contabilidad.
- Conocimientos generales presupuesto público y costos.
- Contratación estatal.
- Salud Ocupacional.
- Modelos Estratégicos.
- Estructura organizacional.
- Estructura del estado Colombiano.
- Planeación estratégica.
- Sistema general de seguridad social.
- Norma Técnica de Control de Gestión Pública (NTCGP) 1000-2004.
- Norma ISO.
- Competencia comunicativa.
- Sistema tarifario sector salud.
- Facturación y glosas.
- Gestión de control.
- Actualización en normatividad hospitalaria vigente.
- Procesos, procedimientos y protocolos.

El perfil del Técnico de la UFATI es el siguiente:

- Título de formación tecnológica o Técnica Profesional en Sistemas.

Además conocimientos en:

- Manejo de sistemas de información.
- Manejo de sistemas de software de oficina.
- Modelos Estratégicos.
- Estructura organizacional.
- Estructura del estado Colombiano.
- Sistema general de seguridad social.
- Competencia comunicativa.
- Gestión de control.
- Actualización en normatividad vigente.
- Procesos, procedimientos y protocolos.
- Planeación estratégicas *software* y *hardware* de última tecnología.
- Cableado estructurado.
- Conocimientos básicos de cada dependencia”[7].

[7] **Fuente:** Tomado de los documentos privados de la ESE HUS.

"La Dirección de la Unidad Funcional de Apoyo Tecnológico y de Información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con el Comité de Gerencia.

También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad.

El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente las actualizaciones. El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito.

Los usuarios son responsables de cumplir con todas las políticas de la organización relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Institución a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos del ESE-HUS a personas no autorizadas.
- No utilizar los recursos informáticos (*hardware, software* o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo.
- "Reportar inmediatamente a su jefe inmediato o a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Organización y sus recursos informáticos"[8].

[8] **Fuente:** Tomado de los documentos privados de la ESE HUS.

Todas estas normas y responsabilidades que se plasman en el anterior resumen tienen el fin primordial de reglamentar el buen funcionamiento del sistema de información para lo cual dos veces al año se capacita en especial al personal asistencial y de estudiantes de las diferentes universidades para que tomen conciencia que el mal uso de los recursos informáticos genera incidentes que los afecta a ellos directamente y por ende a toda la ESE HUS.

4.4 DISEÑO METODOLÓGICO PRELIMINAR

Tipo de trabajo: Teniendo en cuenta que el desarrollo de este trabajo pretende mejorar la seguridad de la red inalámbrica del Hospital Universitario de Santander se desarrollara por fases.

Población: Usuarios de la red de datos del Hospital Universitario de Santander.

Técnica de trabajo: Las técnicas que se utilizarán para el desarrollo de este trabajo son: el análisis bibliográfico y el análisis documental.

Con estos dos tipos de análisis se pretende partir de la lectura selectiva, comprensiva, estratégica y crítica de libros, material documental, manuales, estándares y/o artículos científicos obtener insumos teóricos, conceptos y datos relevantes sobre los diferentes estándares, configuraciones, procedimientos para la configuración y puesta en funcionamiento de un Servidor Radius.

Para este proceso se ha determinado segmentar la investigación en cuatro fases que se presentan a continuación:

Fase 1: Revisión de documentación y estándares internacionales aplicables a las redes inalámbricas y explicar cuáles son las amenazas y vulnerabilidades de la inalámbrica de la ESE HUS. En esta primera fase se pretende hacer una recopilación de información documental relacionada con los procesos, procedimientos, estándares internacionales usados en la configuración de un servidor Radius para mejorar la seguridad de una red inalámbrica. Justificar las amenazas y vulnerabilidades que llevan a la decisión de implementar un Servidor RADIUS en el hospital.

Fase 2: Recopilar información de las características técnicas de los dispositivos inalámbricos que se encuentran instalados en el edificio del

hospital. La segunda fase está enfocada en realizar un análisis minucioso de las características técnicas de los dispositivos que hacen parte de la red inalámbrica mediante un inventario que nos permita saber también el estado actual de los elementos.

Fase 3: Adecuar la máquina que va a servir de Servidor RADIUS, en lo referente a sistema operativo y actualizaciones. Se diagnosticara el Computador en hardware inicialmente y luego se procederá a instalarle el sistema operativo con sus respectivas actualizaciones y configuraciones de seguridad.

Fase 4: Configuración y puesta en funcionamiento de un Servidor Radius. Con base en el análisis realizado en las fases anteriores, en esta fase se pretende entregar la configuración y puesta en funcionamiento del Servidor Radius que mejorara la seguridad en el acceso a la red inalámbrica del Hospital Universitario de Santander.

5. IMPLEMENTACION DEL SERVIDOR RADIUS

5.1 REVISIÓN DE DOCUMENTACIÓN Y ESTÁNDARES INTERNACIONALES APLICABLES A LAS REDES INALÁMBRICAS

Se recolectó documentación e información relevante para el desarrollo del proyecto:

- Seguridad en *WLAN IEEE* 802.11: Evaluación de los mecanismos de cifrado y autenticación. Elaborado por: Dídac Mediavilla Urra. Universidad Politécnica de Cataluña. 2 de abril de 2009. El objetivo de este Proyecto Final de Carrera, es la evaluación del t*hroughput* y el consumo de baterías de los principales protocolos de cifrado. También se realiza la evaluación de la latencia y el consumo de baterías para los protocolos de autenticación. Para ello, se hace el estudio, la implementación y la comparación entre los protocolos de cifrado TKIP y CCMP y entre los protocolos de autenticación EAP-TLS, EAP-PEAP, EAP-TTLS y EAP-LEAP en redes IEEE 802.11, mediante el IEEE 802.1X-EAP. También se realiza una evaluación analítica de la latencia y el consumo de baterías con retransmisiones.

  El anterior proyecto final de carrera aporta al presente trabajo conocimientos sobre la implementación y comparación entre los protocolos de cifrados además de evaluación de protocolos de autenticación.

- Implementación de un servidor de autenticación RADIUS en un ambiente de pruebas para la red inalámbrica de la UPB – sede laureles. Articulo IEEE elaborado por: Velásquez S., Castro B., Velandia Andrés. Universidad Pontificia Bolivariana. Medellín, Colombia. 23 de agosto de 2014. Este artículo presenta un plan piloto para la implementación de un servidor RADIUS (*Remote Access Dial In User Service*) con el fin de proveer servicios de autenticación, autorización y contabilidad en la red inalámbrica de la Universidad Pontificia Bolivariana- sede Laureles.

  El anterior artículo aporta conocimientos sobre un Servidor AAA (autenticación, autorización y contabilidad).

- Seguridad Avanzada en Redes Wireless 802.1x. Elaborado por: Jimmy Arthur Villanueva Llerena. *JaCKSecurity.com*. Lima, Perú. Este trabajo trata temas como: Identificar amenazas y vulnerabilidades en la seguridad inalámbrica. Implementar los filtrados MAC, WEP, WPA, EAP. Entender adecuadamente las

técnicas de inspección del entorno así como las prácticas de seguridad. Realizar comparativas de diversos tipos de métodos de seguridad así como el análisis de sus ventajas y desventajas.

El anterior trabajo aporta conocimientos sobre: encriptación, configuración de redes *Wireless*, instalación y configuración de Radius.

- Diseño e implementación de una red *Lan* y *Wlan* con Sistema de control de acceso mediante servidores AAA. Elaborado por: Nuttsy Aurora Lazo García. Lima, Perú. Diciembre de 2012. Esta tesis de Ingeniería de Telecomunicaciones consiste en el diseño e implementación de una red *LAN* (*Local Área Network*) y *WLAN* (*Wireless Local Area Network*) con sistema de control de acceso AAA (*Authentication, Authorization and Accounting*).

  La anterior tesis aporta al presente trabajo conocimientos en estándar y protocolos de redes, configuración de servidores Radius.

5.1.1 Amenazas y vulnerabilidades en la red inalámbrica de la ESE HUS.

Debido a la cantidad de computadores portátiles personales que al iniciar cada semestre se les configuran a los estudiantes que hacen sus prácticas de medicina y enfermería en el Hospital se genera un riesgo alto de navegar en equipos posiblemente infectados de virus informáticos que pueden generar fallas a la red y también se está generando un problema de orden legal con *Microsoft* ya que la institución es responsable por todo equipo que se conecte a la red indistintamente si es propiedad de la entidad, tercerizado o de estudiantes.

Es muy común encontrar redes en las cuales el acceso a Internet se protege adecuadamente con cortafuegos bien configurado, en el caso de la ESE HUS se usa *Fortinet* para restringir el acceso a redes sociales y otros sitios que generen algún peligro o tráfico en internet como *youtube*, emisoras, etc. y el antivirus institucional de la empresa *ESET* en su última versión, al igual a las empresas contratistas se les exige el sistema operativo y el antivirus licenciado, pero al interior de la red existen puntos de acceso inalámbrico (AP) totalmente desprotegidos con alcance de señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal y use esos portátiles que cada semestre se configuran y se quedan con la configuración, tendrá acceso a la red del Hospital, con la posibilidad de navegar gratis en la Internet, emplear la red de la empresa como punto de ataque hacia otras redes para luego desconectarse y no ser detectado, robar *software* y/o información, introducir programas malignos entre muchas otras cosas.

No se hace un estudio de vulnerabilidades porque la preocupación principal es poder controlar el acceso de portátiles que en semestres anteriores ya quedaron configurados para ingresar a la red y al sistema Dinamica.net y puedan seguir conectándose sin ningún control.

5.2 RECOPILAR INFORMACIÓN DE LAS CARACTERÍSTICAS TÉCNICAS DE LOS DISPOSITIVOS INALÁMBRICOS QUE SE ENCUENTRAN INSTALADOS EN EL EDIFICIO DEL HOSPITAL

Actualmente hay en funcionamiento 12 Cisco AIR-AP1130 de los 35 que se instalaron inicialmente, ya por los años de uso las pastas de la mayoría se encuentran cristalizadas por lo que se están adquiriendo del modelo Cisco AIR-AP1620. Algunas áreas se están cubriendo con DLink DSL-2640B mientras se les cambia la configuración a los AP1620 que vienen para trabajarlos con consola.

5.2.1 *Access Point* Cisco AIR-AP1130AG-A-K9. El AP Cisco AIR-AP1130AG-A-K9 se observa en la figura 4.

Figura 4: Modelo de Access point antiguo de la ESE HUS

Fuente: http://www.ipexpress.cl/pyme/images/AIR-AP1131AG-A-K9-1.png?osCsid=770023f8a31327

"Destacamos:

- *Access Point* de funcionamiento "Autónomo"
- Soporte para 802.11a y 802.11g

- Hasta 108 Mbps de capacidad.
- Soporta hasta 15 canales *Nonoverlapping*
- Bajo potencial de interferencia con vecinos.
- Diseño bajo en errores de transmisión provee un alto "*throughput*" y una señal robusta aún en largas distancias
- Control de potencia variable}
- Antenas integradas
- Encryptación en *Hardware*
- Cisco *Unified* IDS/IPS
- IEEE 802.11i *Compliant*
- Certificado para WPA2- y WPA
- Soporte PoE (IEEE 802.3af y Cisco *Inline Power*)

Aspectos generales

Los puntos de acceso de Cisco *Aironet* 1130AG/1240AG Series admiten:

- **Amplia cobertura:** Las antenas y radio de Cisco están diseñadas para proporcionar la máxima cobertura posible.

- **Rendimiento:** Las radios duales de alta capacidad proporcionan flexibilidad, capacidad y rendimiento para admitir una amplia gama de aplicaciones móviles como un acceso de invitado y voz en la red *LAN* inalámbrica.

- **Seguridad:** Los puntos de acceso de Cisco (AP) se conocen por su reconocida implementación de las opciones de seguridad avanzadas y basadas en estándares.

- **Escalabilidad:** Los AP pueden trabajar por si mismos para obtener los servicios de cobertura y movilidad con los controladores *LAN* inalámbricos de Cisco para aplicaciones más avanzadas y una administración centralizada de varios puntos de acceso"[9].

- **"Flexibilidad:** Los AP de Cisco 1130AG están diseñados para oficinas, mientras que los AP 1240AG son menos decorativos y son la mejor opción para fábricas, almacenes y entornos de comercio minorista.

[9] Texto recuperado de la página: http://www.ipexpress.cl/pyme/product_info.php/access-point-cisco-air-ap1131ag-k9-p-322

Los puntos de acceso Cisco *Aironet* 1130AG/1240AG Series ofrecen:

- Las radios duales proporcionan soporte para varias opciones de red inalámbrica que funcionan en bandas de 2,4 y 5 GHz para obtener una mejor flexibilidad, cobertura y soporte de dispositivos de cliente
- Capacidad para asignar cobertura incluso con obstrucciones e interferencias potenciales
- Fácil instalación en techos retráctiles
- Integración con la administración inalámbrica de Cisco y el *software* de supervisión
- Sistema de montaje seguro y con posibilidad de bloqueo con carcasa de plástico ligera (punto de acceso 1130AG) o rugosa (punto de acceso 1240AG)

Características

- *Access Point* autónomo
- Diseño ligero y discreto para entornos de oficina
- Hasta 108 Mbps de capacidad
- Antena integrada
- Admite varios estándares de seguridad para la protección y autentificación de identidad
- Número ilimitado de puntos de acceso
- Soporte PoE
- Funciona con Cisco *Unified Wireless Network*
- Diseñado para ser flexible al ajustar las capacidades de cobertura
- Reducción de interferencias
- Funcionamiento independiente o con los controladores *WLAN* de Cisco para los servicios de movilidad avanzados

General

Tipo de dispositivo Punto de acceso inalámbrico
Anchura 19.1 cm
Profundidad 3.3 cm
Altura 19.1 cm
Peso 0.67 kg
Procesador / Memoria / Almacenamiento”[10]
“RAM instalada (máx.) 32 MB
Memoria *flash* instalada (máx.) 16 MB *Flash*.

Conexión de redes

[10] Texto recuperado de la página: http://www.ipexpress.cl/pyme/product_info.php/access-point-cisco-air-ap1131ag-k9-p-322

Factor de forma Externo
Tecnología de conectividad Inalámbrico
Velocidad de transferencia de datos 54 Mbps
Formato código de línea CCK, OFDM
Protocolo de interconexión de datos IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
Protocolo de gestión remota SNMP, Telnet, HTTP, HTTPS
Alcance máximo en interior 137 m
Alcance máximo al aire libre 290 m
Indicadores de estado Activo, error, estado
Características Enlace ascendente, auto-sensor por dispositivo, soporte BOOTP
Algoritmo de cifrado LEAP, AES, WEP de 128 bits, WEP de 40 bits, TLS, PEAP, TTLS, TKIP, WPA, WPA2
Método de autentificación *Secure Shell* (SSH), MS-CHAP
Cumplimiento de normas IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, Wi-Fi CERTIFIED

Directividad Omnidireccional
Expansión / Conectividad
Interfaces 1 x red / energía - *Ethernet* 10Base-T/100Base-TX - RJ-45

Diverso
Cumplimiento de normas VCCI, EN 60950, ICES-003, IEC 60950, UL 60950, CSA 22.2 No. 60950, EN 300.328, EN 301.489.1, EN 301.489.17, FCC Part 15.247, OET 65 C, RSS-210, RSS-102, UL 2043, FCC

Alimentación
Alimentación por Ethernet (PoE) Sí
Dispositivo de alimentación Adaptador de corriente - externa
Voltaje necesario CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento 12.2 vatios

Garantía del fabricante
Servicio y mantenimiento 1 año de garantía"[11]
"Detalles de Servicio y Mantenimiento Garantía limitada - 1 año

Parámetros de entorno
Temperatura mínima de funcionamiento 0 °C

[11] Texto recuperado de la página: http://www.ipexpress.cl/pyme/product_info.php/access-point-cisco-air-ap1131ag-k9-p-322

Temperatura máxima de funcionamiento 40 °C
Ámbito de humedad de funcionamiento 10 - 90%”[12]

5.2.2 *Router* / AP *Dlink* DSL-2640B. El *router* AP *Dlink* DSL-2640B se observa en la figura 5.

Figura 5 Router Dlink DSL-2640B

Fuente: http://www.zero13wireless.net/wireless/Analisis/APs/DLink_DSL-2640B/dsl-2640b.jpg

“Especificaciones
Marca: *DLink*
Modelo: DSL-2640B
Wireless: b/g
Tipo: *Router* / AP
Idiomas Firmware: Español + Otros
Consiste en un *módem/router* ADSL2+ DSL-2640B y un adaptador DWA-111 USB2.0”[13].

“Velocidad *LAN* inalámbrica de 54 Mbps, basada en la especificación IEEE 802.11g.
Encriptación inalámbrica (WEP/WPA/WPA2).

[12] Texto recuperado de la página: http://www.ipexpress.cl/pyme/product_info.php/access-point-cisco-air-ap1131ag-k9-p-322

[13] Texto recuperado de la página: http://www.gigaclip.cl/motor_generapagina.php?NINTER=1399

D-Link Click Connect (DCC 2), asistente que facilita la configuración y ayuda en el proceso de instalación del adaptador.

"*Router*/AP
Módem ADSL2+ integrado, con una velocidad de datos de hasta 24 Mbps para el flujo descendente y 1 Mbps para el flujo ascendente.
4 puertos *switch Ethernet* integrados.
1 antena extraíble (conector SMA inverso, hembra).
QoS inalámbrica 802.11e (WMM/WME).
3 colas de prioridad para la priorización del tráfico (QoS).
Control parental con bloqueo de URL y programación.
Firewall NAT y SPI (*Stateful Packet Inspection*) con paso por varias VPN.
UPnP

Información detallada:
El *router módem* ADSL2+ *Wireless* G DSL-2640B ofrece a los usuarios particulares una forma económica de compartir una conexión de banda ancha a internet basada en ADSL, ADSL2 o ADSL2+.

Conexión ADSL de alta velocidad
El DSL-2640B soporta los últimos estándares ADSL2/ADSL2+, con lo que ofrece velocidades de hasta 24 Mbps para el flujo descendente y 1 Mbps para el flujo ascendente (ADSL2+), o 12 Mbps para el flujo descendente y 1 Mbps para el flujo ascendente (ADSL2). Es compatible con la mayoría de los proveedores de servicios de Europa.

El DSL-2640B incluye un punto de acceso 802.11g que soporta velocidades inalámbricas de hasta 54 Mbps1 y con interoperabilidad con los dispositivos inalámbricos 802.11b en la banda de frecuencia de 2,4 GHz. También cuenta con cuatro puertos *switch Ethernet* a 10/100 Mbps para conectar cuatro estaciones de trabajo. Estas funciones integradas son un ahorro de dinero y de problemas, puesto que no es necesario instalar un punto de acceso y un *switch Ethernet*"[14].

"Protección de red
El *firewall* SPI (*Stateful Packet Inspection*) integrado en el *router* dificulta el acceso de los *hackers* a la red. También se incluyen potentes controles parentales, que

[14] http://www.gigaclip.cl/motor_generapagina.php?NINTER=1399

permiten bloquear o permitir el acceso a determinados sitios web completamente o a unas horas del día establecidas. Esta característica de seguridad se configura en el *router* de una forma excepcionalmente fácil.

"En el lado inalámbrico, se puede configurar el filtrado MAC y una potente encriptación para asegurar las transferencias de datos y para evitar el acceso de intrusos a la conexión de banda ancha.

El *router* también soporta el paso por VPN, lo que permite a los usuarios móviles acceder con seguridad a los archivos de la oficina y al correo electrónico desde su casa.

Características de calidad de servicio (QoS)
El DSL-2640B admite varias colas de prioridad, lo que posibilita que un grupo de usuarios, en el hogar o en la oficina, puedan disfrutar de una conectividad sin problemas causados por la congestión de la red. La calidad de servicio (QoS) ofrece a los usuarios la transmisión sin demoras para aplicaciones como VoIP, *streaming* multimedia y juegos en línea por internet.

La velocidad máxima de la señal inalámbrica la definen las especificaciones del estándar IEEE 802.11g. El rendimiento real variara. Las condiciones de la red y los factores medioambientales, como el volumen de tráfico por la red, los materiales de construcción y las edificaciones, pueden disminuir la velocidad real de los datos. Los factores medioambientales pueden afectar negativamente al alcance de la señal inalámbrica.

Hardware
- *Modem* ADSL/ADSL2/ADSL2+ integrado (Anexo A).
- Especificación LAN inalámbrica IEEE 802.11g, velocidad bruta de datos de hasta 54 Mbps.
- 1 antena extraible (conector SMA inverso, hembra).
- 4 puertos *switch* 10/100Base-TX integrados con auto-MDI/MDIX.
- Microfiltro incluido (solo para R. U.)"[15].

Wireless
· Certificación *Wi-Fi*.
· QoS inalámbrica 802.11e (WMM/WME).

[15] http://www.gigaclip.cl/motor_generapagina.php?NINTER=1399

· SSID múltiple.
· Encriptación WEP 64/128-bit.
· Encriptación WPA/WPA2 con TKIP/AES.

“QoS
· Priorización del tráfico con 3 colas de prioridad.

Seguridad
· SPI (*Stateful Packet Inspection*).
· *Firewall* NAT integrado.
· Denegación de servicio (DoS).
· Múltiple paso por IPSEc/PPTP/L2TP.
· Control parental con bloqueo de URL y programación.
· Filtrado de direcciones MAC.

Protocolos de red
· Autonegociación G.hs de distintas versiones de ADSL.
· DNS dinámico.
· Enrutamiento IP estático.

Configuración/gestión
· *D-Link Click'n Connect* (DCC 2), asistente para la fácil configuración.
· Gestión basada en *web*.
· Soporte UPnP”[16].

5.2.3 *Access Point* Cisco AIR-CAP1602I-A-K9. En la pagina 38, en la figura 6 se observa AP Cisco AIR-CAP1602I-A-K9.

[16] Texto recuperado de la página: http://www.adslzone.net/postt242633.html

Figura 6 Nuevo modelo de AP adquirido por la ESE HUS

Fuente: http://cisco.solutekcolombia.com/acces_point_cisco/air-cap1602i-a-K9/

"El Cisco *Aironet* ® 1600 Series *Access Point* es de clase empresarial, de nivel de entrada, el Access point basado en 802.11n está diseñado para atender las necesidades de conectividad inalámbrica de redes de empresas pequeñas y medianas.

La serie *Aironet* 1600 incluye la tecnología basada en 802.11n 3x3 múltiples entradas múltiples salidas (MIMO) con dos flujos espaciales, por lo que es ideal para pequeñas y medianas empresas.

Excelencia RF

Sobre la base del patrimonio Cisco *Aironet* de excelencia de RF, la serie Cisco *Aironet* 1600 ofrece conexiones inalámbricas seguras y fiables. *Chipsets* de clase empresarial y radios optimizados ofrecen una experiencia de movilidad robusta con:

● 802.11n 3x3 con múltiples entradas y múltiples salidas (MIMO) la tecnología con dos flujos espaciales, que sostiene a 300 Mbps tasas en un rango mayor de más capacidad y fiabilidad que compiten los puntos de acceso"[17].

● gestión de recursos radio (RRM): la auto-sanación automatizado optimiza la imprevisibilidad de RF para reducir los puntos muertos y ayudar a asegurar las conexiones de clientes de alta disponibilidad.

[17] Texto recuperado de la página: http://cisco.solutekcolombia.com/acces_point_cisco/air-cap1602i-a-K9/

● *CleanAir Express*: detecta eficazmente la interferencia de RF y proporciona la capacidad de análisis de espectro básico al tiempo que simplifica las operaciones en curso.

● La tecnología Cisco *ClientLink* 2.0: Mejora el rendimiento del enlace descendente a todos los dispositivos móviles, incluyendo 802.11n al tiempo que mejora la vida de la batería en los dispositivos móviles como teléfonos inteligentes y tabletas.

● Cisco *BandSelect* tecnología: Mejora las conexiones de cliente 5-GHz en entornos de clientes heterogéneos.

Escalabilidad: La serie Cisco *Aironet* 1600 es un componente de la red inalámbrica unificada de Cisco, que se puede ampliar a un máximo de 18.000 puntos de acceso con plena movilidad de Capa 3 a través de localizaciones centrales o remotas en el campus de la empresa, en las sucursales, y en sitios remotos. El Cisco *Unified Wireless Network* es la arquitectura más flexible, resistente y escalable de la industria de la entrega de un acceso seguro a los servicios de movilidad y aplicaciones, y ofrece el menor costo total de propiedad y protección de la inversión mediante la integración sin problemas con la red cableada existente. [18]

5.3 ADECUACION DE LA MÁQUINA QUE VA A SERVIR DE SERVIDOR RADIUS, EN LO REFERENTE A SISTEMA OPERATIVO Y ACTUALIZACIONES

Para comprobar las características adecuadas de la máquina, sistema operativo y correcta configuración de los dispositivos se sacó un diagnostico con el comando dxdiag:

System Information

Time of this report: *9/28/2015, 07:37:40*

[18] Texto recuperado de la página: http://cisco.solutekcolombia.com/acces_point_cisco/air-cap1602i-a-K9/

Machine name: PCSISTEM20
Operating System: Windows 7 Professional 64-bit (6.1, Build 7601) Service Pack 1 (7601.win7sp1_gdr.150427-0707)
Language: Spanish (Regional Setting: Spanish)
System Manufacturer: Hewlett-Packard
System Model: HP Compaq Pro 4300 SFF PC
BIOS: BRCM MBA Slot 0500 v15.0.11
Processor: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz (4 CPUs), ~3.3GHz
Memory: 8192MB RAM
Available OS Memory: 8080MB RAM
Page File: 2773MB used, 13384MB available
Windows Dir: C:\Windows
DirectX Version: DirectX 11
DX Setup Parameters: Not found
User DPI Setting: Using System DPI
System DPI Setting: 96 DPI (100 percent)
DWM DPI Scaling: Disabled
DxDiag Version: 6.01.7601.17514 64bit Unicode

DxDiag Notes

Display Tab 1: No problems found.
Sound Tab 1: No problems found.
Input Tab: No problems found.

DirectX Debug Levels

Direct3D: 0/4 (retail)
DirectDraw: 0/4 (retail)
DirectInput: 0/5 (retail)
DirectMusic: 0/5 (retail)
DirectPlay: 0/9 (retail)
DirectSound: 0/5 (retail)
DirectShow: 0/6 (retail)

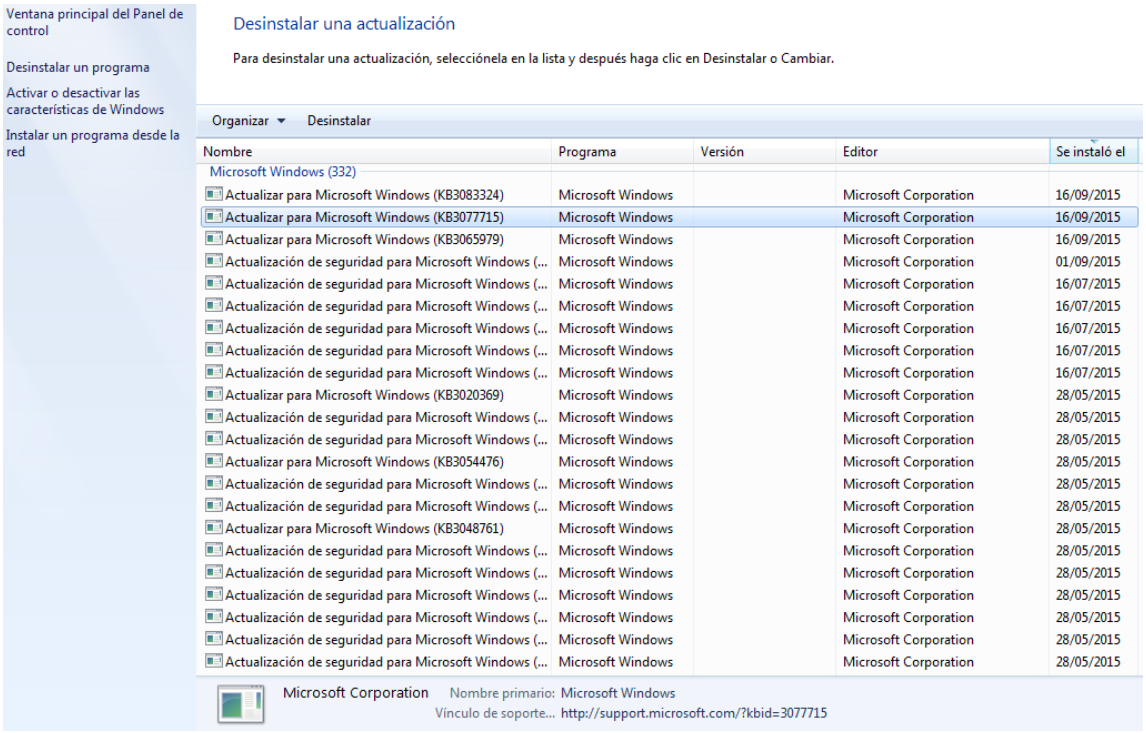
Display Devices

Card name: Intel(R) HD Graphics
Manufacturer: Intel Corporation

Chip type:	*Intel(R) HD Graphics Family*
DAC type:	*Internal*
Device Key:	*Enum\PCI\VEN_8086&DEV_0152&SUBSYS_2ADE103C&REV_09*
Display Memory:	*1696 MB*
Dedicated Memory:	*64 MB*
Shared Memory:	*1632 MB*
Current Mode:	*1366 x 768 (32 bit) (60Hz)*
Monitor Name:	*Monitor PnP genérico*
Monitor Model:	*HP LV1911*
Monitor Id:	*HWP3005*
Native Mode:	*1366 x 768(p) (59.790Hz)*
Output Type:	*HD15*
Driver Name:	*igdumd64.dll, igd10umd64.dll, igd10umd64.dll, igdumd32, igd10umd32, igd10umd32*
Driver File Version:	*9.17.0010.3517 (English)*
Driver Version:	*9.17.10.3517*
DDI Version:	*11*
Driver Model:	*WDDM 1.1*
Driver Attributes:	*Final Retail*
Driver Date/Size:	*12/13/2014 13:37:15, 12617728 bytes*
WHQL Logo'd:	*Yes*
WHQL Date Stamp:	
Device Identifier:	*{D7B78E66-4212-11CF-317E-D40AB7C2C435}*
Vendor ID:	*0x8086*
Device ID:	*0x0152*
SubSys ID:	*0x2ADE103C*
Revision ID:	*0x0009*
Driver Strong Name:	*oem45.inf:Intel.Mfg.NTamd64:iIVBD0:9.17.10.3517: pci\ven_8086&dev_0152*
Rank Of Driver:	*00E02001*
Video Accel:	*ModeMPEG2_A ModeMPEG2_C ModeWMV9_C ModeVC1_C*

En la captura de pantalla que se observa en la figura 7 se evidencian las últimas actualizaciones del sistema operativo del Servidor:

Figura 7 Actualizaciones del Sistema Operativo del Servidor



Fuente: El autor

5.4 CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN SERVIDOR RADIUS

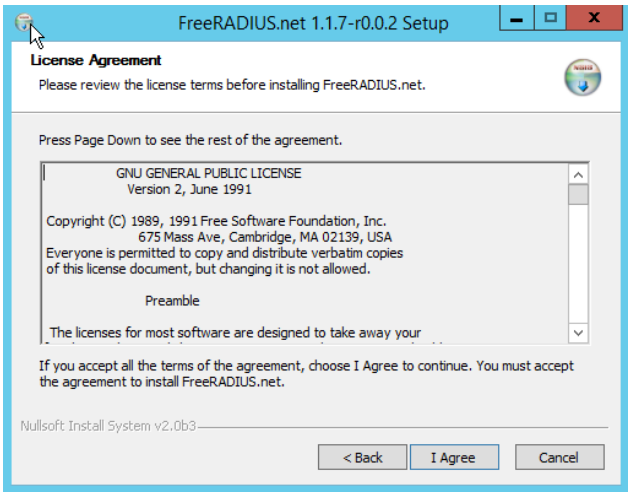
Después de tener lista la máquina seleccionada para Servidor en cuanto a Sistema Operativo y actualizaciones de *Windows* se procede a instalar el Servidor Radius con el instalador: FreeRADIUS.net 1.1.7-r0.0.2 al cual se le da doble clic para ejecutarlo y para empezar se da clic al botón "*Next*", como se observa en la figura 8.

Figura 8 Instalación del Servidor RADIUS

Fuente: El Autor

Se acepta el contrato de Licencia dando clic en el botón "*I Agree*", como se observa en la figura 9.

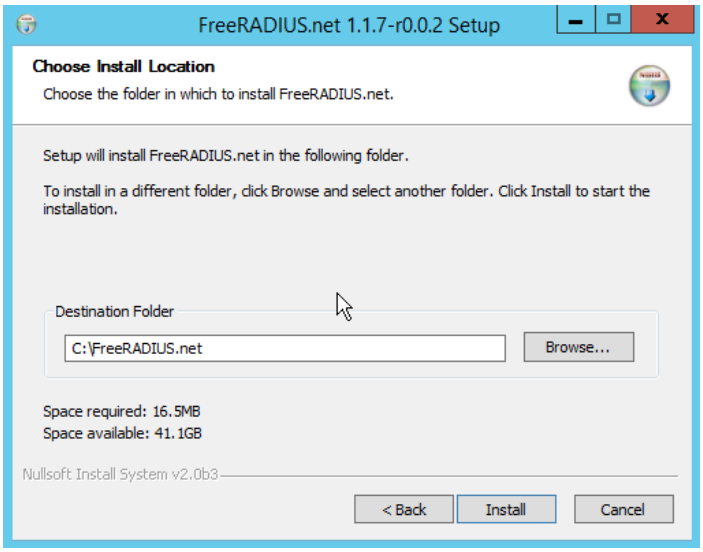
Figura 9 Instalación del Servidor RADIUS



Fuente: El Autor

El Servidor RADIUS se instalara en la siguiente ruta C:\, luego se da clic en el botón "*Install*", como se observa en la figura 10.

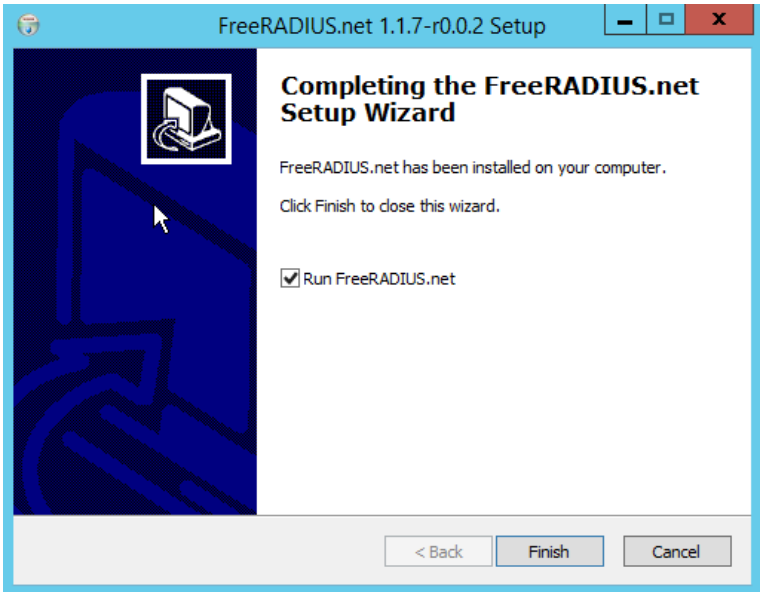
Figura 10 Instalación del Servidor RADIUS



Fuente: El Autor

Una vez finalizada la instalación se observa una ventana de alerta la cual se procede a dar clic en el botón "*Finish*", como se observa en la figura 11.

Figura 11 Instalación del Servidor RADIUS

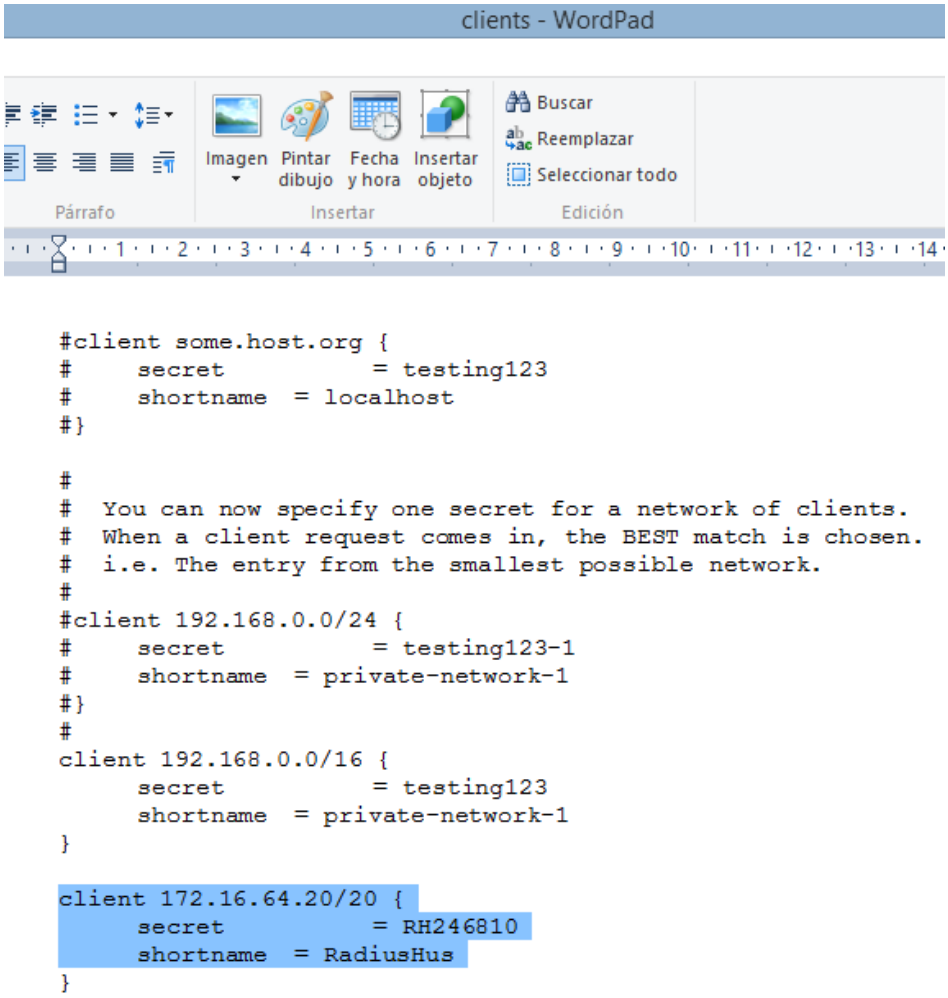


Fuente: El Autor

Ahora se editan los archivos de configuración del Servidor RADIUS. Se dirige a la ruta C:\FreeRADIUS.net\etc\raddb y da doble *clic* al archivo *clients.conf* o preferiblemente lo abre con *Worpad*.

Como se observa en la figura 12, busca la línea *client* y le coloca la dirección del AP al cual se conectaran los portátiles en forma inalámbrica. En *secret* coloca una clave compartida entre el Servidor RADIUS y el AP y finalmente en *shortname* coloca un nombre para el *Access Point*. Guarda los cambios y cierra el archivo.

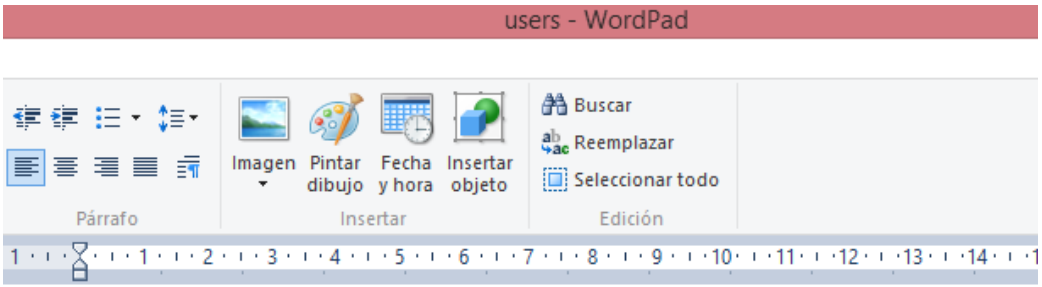
Figura 12 Configuración del Servidor RADIUS



Fuente: El Autor

En la misma ruta encuentra el archivo *users.conf*, lo edita y busca una línea "*testuser*", como se observa en la figura 13, donde coloca las credenciales de los clientes para que puedan ingresar a la red inalámbrica, cambia la palabra *testuser* por el usuario que al igual que los que se crean en Dinamica.net se forma con las iniciales del nombre por ejemplo "cafs" y para la clave cambia "testpw" por "hus2015" y de igual manera por cada usuario que quiera ingresar a la red se le asigna una clave diferente.

Figura 13 Configuración del Servidor RADIUS

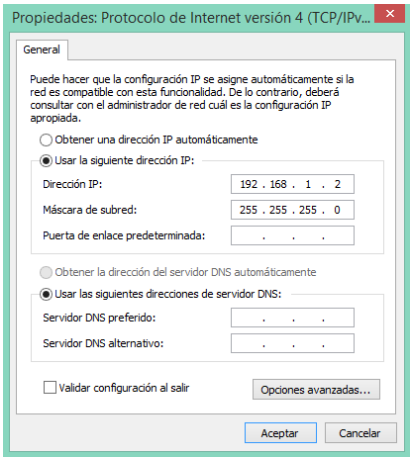



```
#          Reply-Message = "Your account has been disabled."

#
# Deny access for a group of users.
#
# Note that there is NO 'Fall-Through' attribute, so the user
will not
# be given any additional resources.
#
#DEFAULT   Group == "disabled", Auth-Type := Reject
#          Reply-Message = "Your account has been disabled."
#

############## RFC3580 ################
## Also the "eap.conf" MUST be modified to include the follow
line:
## "use_tunneled_reply = yes"
## the default is "use_tunneled_reply = no"
## this allow the "Tunnel*" AV's to be passed outside the eap
tunnel
## otherwise the switch will NOT see the VLAN to place the port
into
#### Comments added by Jeff Reilly ####

cafs  User-Password == "hus2015"
magp  User-Password == "hus2016"
goca  User-Password == "hus2017"
jfvm  User-Password == "hus2018"

FreeRADIUS.net-Client User-Password == "demo"
```

Fuente: El Autor

Después se configura el *Access Point* para lo cual se asigna una dirección IP fija a la tarjeta de red del equipo que este en el mismo segmento de red del AP como se observa en la figura 14, luego en un navegador de internet ingresa al AP digitando la dirección 192.168.1.1 con usuario y clave: “admin”, después de ingresar se configura una dirección dentro del segmento que se utiliza en la ESE HUS, en este caso se usa la IP 172.16.64.20 y se guardan los cambios. También se vuelve a cambiar la IP de la tarjeta de red del Servidor a: 172.16.64.21.

Figura 14 Configuración del Access Point



Fuente: El Autor

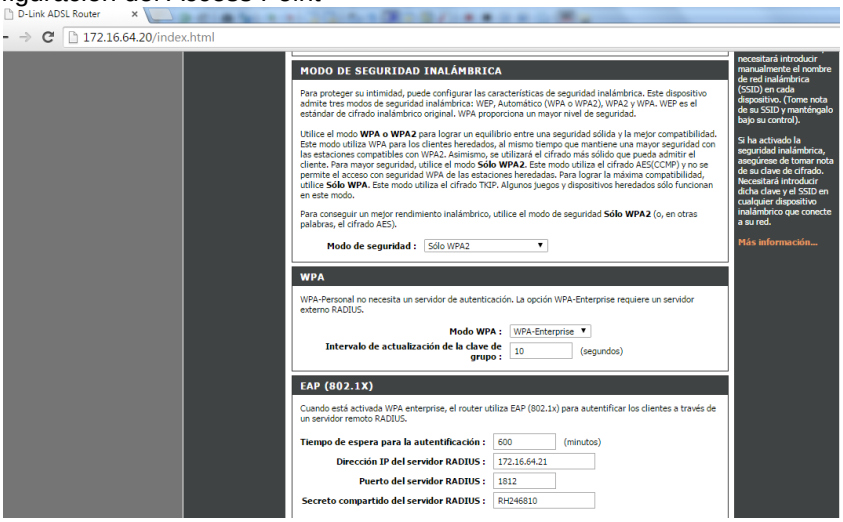
En el navegador de internet se digita la IP 172.16.64.20 para volver a conectar al AP, se ubica en “configuración inalámbrica” y en “Nombre de la red inalámbrica” se escribe RadiusHus, como se observa en la figura 15.

Figura 15 Configuración del Access Point

Fuente: El Autor

Se ubica en “MODO DE SEGURIDAD INALÁMBRICA” y en “Dirección IP del servidor RADIUS” se escribe: 172.16.64.21, el puerto se deja: 1812 y en “Secreto compartido del servidor RADIUS” se escribe: RH246810 como en *clients.conf*, como se observa en la figura 16.

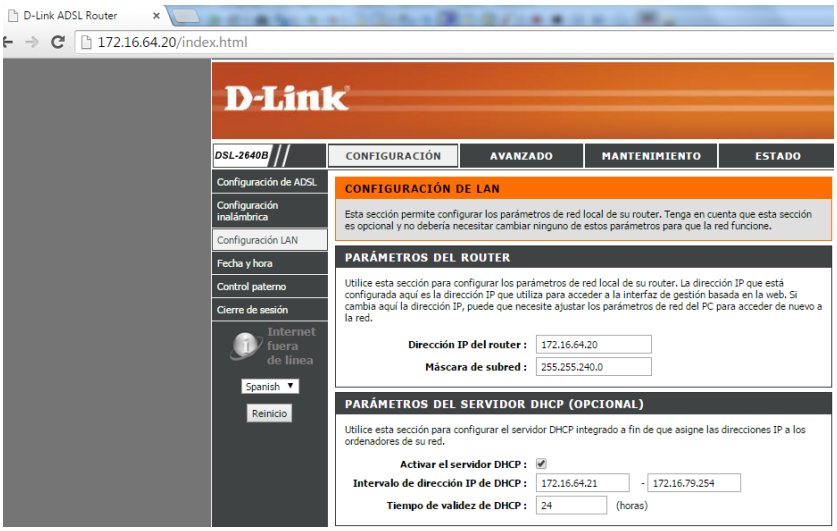
Figura 16 Configuración del Access Point



Fuente: El Autor

En “configuración *LAN*” se configura el “Intervalo de dirección de DHCP: 172.16.64.21 al 172.16.79.254, como se observa en la figura 17.

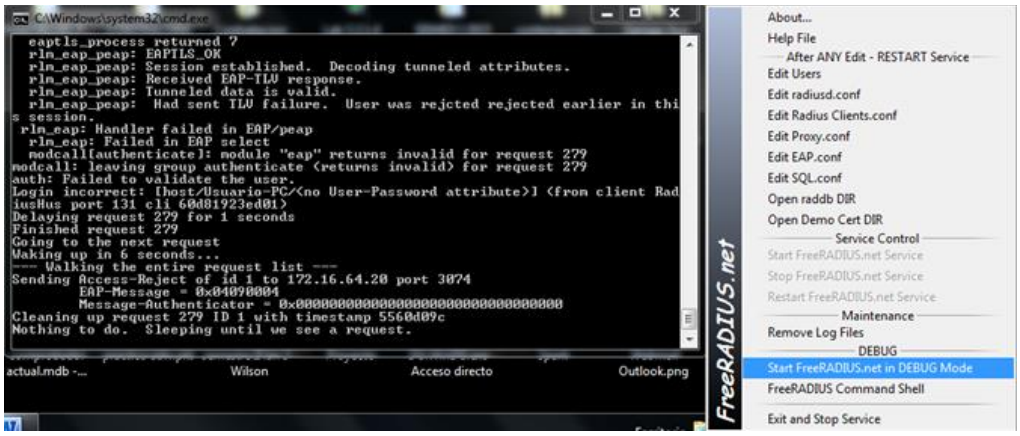
Figura 17 Configuración del Access Point



Fuente: El Autor

Para hacer correr el Servidor RADIUS, se busca en la parte inferior derecha el icono y se da *clic* derecho, clic en "*Start* FreeRADIUS.net *in DEBUG Mode*", se ejecuta y queda listo para autentificar los usuarios, como se observa en la figura 18.

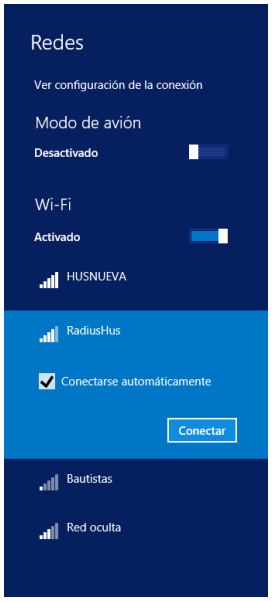
Figura 18 Configuración del Access Point



Fuente: El Autor

Después se configura un cliente en un computador portátil, se da clic al icono de autenticación de la red inalámbrica, como se observa en la figura 19.

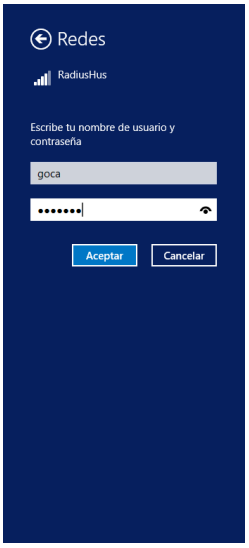
Figura 19 Configuración del Cliente



Fuente: El Autor

Se selecciona la inalámbrica “RadiusHus” y se da clic en “Conectar”, posteriormente se digita el usuario y la contraseña, como se observa en la figura 20.

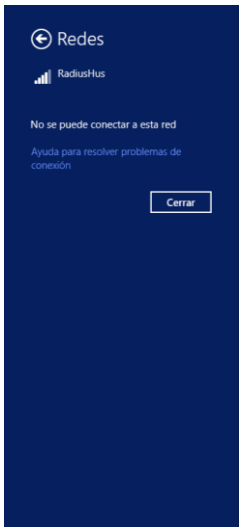
Figura 20 Configuración del Cliente



Fuente: El Autor

Se emite un mensaje “No se puede conectar a esta red” porque no están configuradas las credenciales, como se observa en la figura 21.

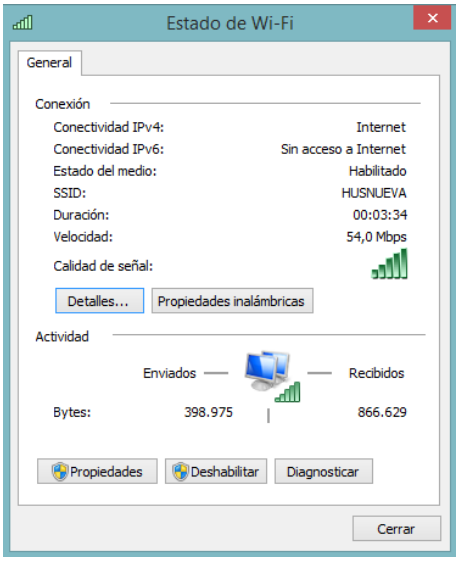
Figura 21 Configuración del Cliente



Fuente: El Autor

En configuración de red se da clic izquierdo en propiedades al icono de la tarjeta de red inalámbrica, luego clic en el botón “Propiedades inalámbricas”, como se observa en la figura 22.

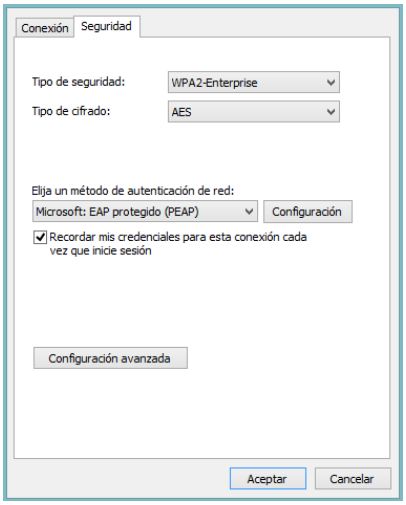
Figura 22 Configuración del Cliente



Fuente: El Autor

En la pestaña “Seguridad” Se cambia el tipo de seguridad y en “Elija un método de autenticación de red” debe quedar: “*Microsoft*: EAP protegido (PAEP) y se da clic en el botón “Configuración”, como se observa en la figura 23.

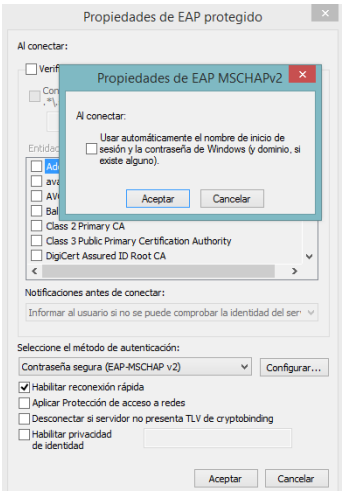
Figura 23 Configuración del Cliente



Fuente: El Autor

Se desmarca el *check* a “Verificar la identidad del servidor validando el certificado”, en la parte de abajo va al botón “Configurar” y se desmarca el *check* a: “Al conectar:” para no usar la contraseña del usuario de *Windows* para poder ingresar al Servidor RADIUS y se da clic en “Aceptar” en todas las ventanas que se abrieron, como se observa en la figura 24.

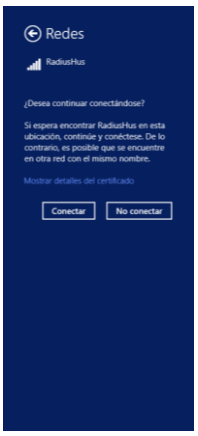
Figura 24 Configuración del Cliente



Fuente: El Autor

Ahora se trata de ingresar nuevamente a la inalámbrica “RadiusHus”. Se digita el usuario y contraseña, se da clic en “aceptar”, pregunta: Desea continuar conectándose?, se da clic en “Conectar”, como se observa en la figura 25.

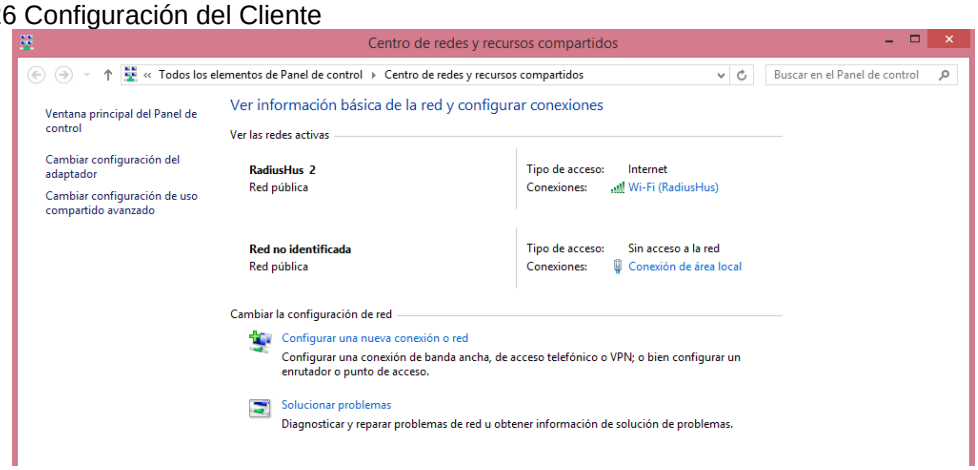
Figura 25 Configuración del Cliente



Fuente: El Autor

Ya está conectado a la red el cliente y podrá ingresar al programa Dinamica.net, a los discos de red, como se puede observar en la figura 26.

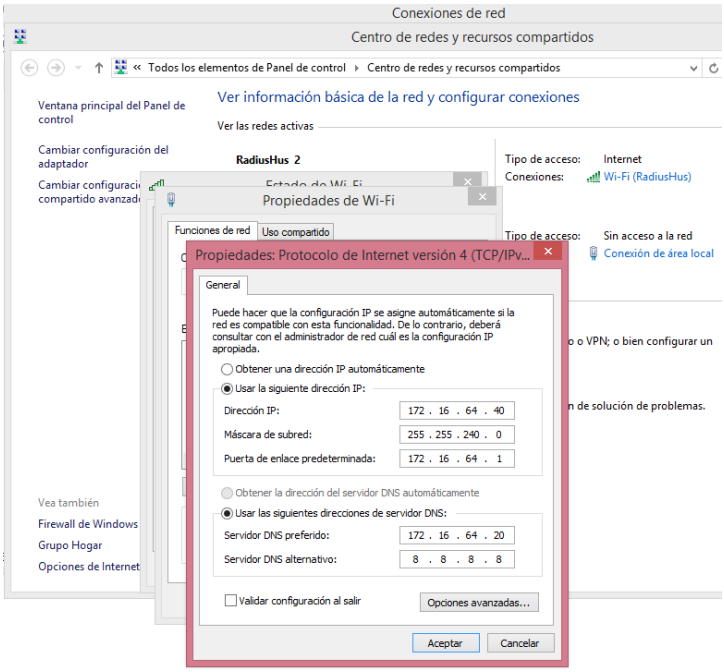
Figura 26 Configuración del Cliente



Fuente: El Autor

Si además de ingresar a la red también se le va a dar permiso de navegar en internet, se le implementa por completo la configuración descrita en la figura 27.

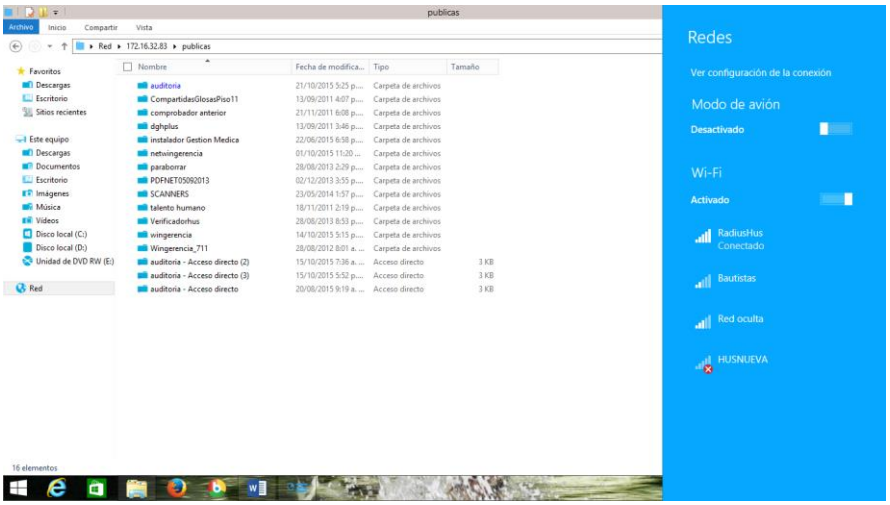
Figura 27 Configuración del Cliente



Fuente: El Autor

Para evidenciar como se ve la conexión al Servidor RADIUS desde un cliente se captura la pantalla de la figura 28 en la que se observa el acceso a un disco de red del Servidor Principal desde el que se instalan y corren los aplicativos de la ESE HUS.

Figura 28 Conexión al Servidor FreeRADIUS



Fuente: El Autor

Una segunda evidencia de la conexión al Servidor desde un cliente es observa en la figura 29 con la navegación en una página *web*.

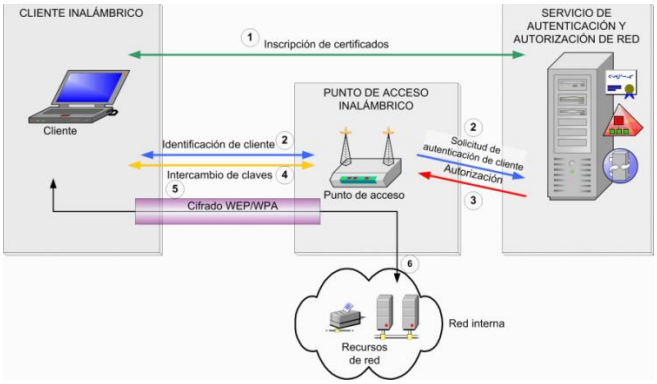
Figura 29 Conexión al Servidor FreeRADIUS

Fuente: El Autor

Autenticación de usuario cliente al servidor

La autenticación inicia con una petición que solicita el usuario cliente, llega al AP y este último la envía al Servidor, ahora el Servidor pregunta usuario y contraseña, llega al AP y la envía al cliente, luego el cliente envía su usuario y contraseña al Servidor pasando por el AP, el Servidor compara con la lista que él tiene en el archivo *users.conf*, como se observa en la figura 30.

Figura 30 Autenticación de un cliente al Servidor FreeRADIUS



Fuente: http://www.microsoft.com/latam/technet/articulos/wireless/pgch03.mspx

5.5 OTRAS CONSIDERACIONES

5.5.1 Problemas de seguridad que puede presentar FreeRADIUS. Tener configurado el Servidor RADIUS en una máquina que administra otros programas podría aumentar los riesgos de inseguridad por este motivo es recomendable que el equipo solo esté dedicado a este aplicativo.

Siempre existirá el riesgo de ataques como denegación de servicio contra el Servidor o ataques de fuerza bruta y diccionario, aunque se supone que esta vulnerabilidad se presentaba con el protocolo *WEP*, pero para aumentar la seguridad es recomendable que tanto el secreto compartido como las claves de los usuarios de los clientes sean complejos y largos.

5.5.2 Plan de contingencia. El plan de contingencia es la actividad que se ejecuta para darle continuidad al servicio que sufre una interrupción prolongada.

OBJETIVO

Establecer las actividades a desarrollar ante una situación de emergencia que impida el normal funcionamiento de los sistemas de información, identificando las actividades a realizar antes, durante y después del evento.

OBJETIVO ESPECÍFICO:

Determinar el riesgo, identificando las amenazas y las vulnerabilidades que se puedan presentar en los sistemas de información manuales y electrónicos de la ESE HUS.

DEFINICIONES

AMENAZA: Es un evento que puede desencadenar un suceso en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

VULNERABILIDAD: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

RIESGO: Posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

RESPONSABLE: Unidad Funcional de Apoyo Tecnológico y de Información.

INTRODUCCION: El Plan de Contingencia es el instrumento de gestión para el buen manejo de las tecnologías de la Información. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la Entidad, ya que los activos informáticos están expuestos a diversos factores de riesgos humanos y físicos; estos problemas pueden originar pérdidas catastróficas de la información a partir de fallos de componentes críticos, por grandes desastres o por fallas técnicas (errores humanos, virus informático), etc, que producen daños irreparables.

El propósito del Plan de Contingencia es prepararse para enfrentar situaciones de emergencia, por lo cual dicho documento contiene la descripción de las actividades a realizar en situaciones específicas que puedan presentarse, con lo cual se minimizan el riesgo en la prestación del servicio y la perdida de información.

Este plan de contingencia le apunta a definir un plan preventivo, predictivo y reactivo garantizado que la entidad se encuentre preparada para asumir cualquier eventualidad; por este motivo se hace necesario que la ESE HUS cuente con un plan de contingencia adecuado de forma que ayude a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la entidad.

EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

DESTRUCCIÓN DEL CENTRO DE CÓMPUTO

- Contar con el inventario total de los sistemas de información actualizado y conocerlo.
- Contar con el inventario total de recursos de hardware actualizado y conocerlo.
- Contar con los *backups* de información realizados y actualizados.
- Conocer ante el evento como sería la adecuación del nuevo espacio para restaurar el Centro de Cómputo.
- Presupuestar la adquisición de *software*, *hardware*, materiales, personal y transporte.
- Adquisición de recursos de *software*, *hardware*, materiales y contratación de personal.
- Iniciar con la instalación y configuración del nuevo centro de cómputo.
- Puesta en marcha de los sistemas de información y puesta en marcha del centro de cómputo.

Recursos de Contingencia

- Asignación de nuevo espacio para montaje de servidores.
- Servidores de contingencia.
- Personal adicional experto en implementación de *Datacenter*.
- Elementos físicos de redes de datos y comunicaciones.
- Asignación de recursos para componentes de la red eléctrica y aires acondicionados mínimos.

NO HAY COMUNICACIÓN ENTRE CLIENTE – SERVIDOR DE LA ESE HUS

- Requerimiento del usuario, que no cuenta con acceso a la red.
- El técnico de sistemas procederá a identificar el problema.
- Realizar las actuaciones correspondientes para dar solución al problema.
- Recuperación del sistema de red para el usuario.
- Recursos de Contingencia.
- Componentes de Remplazo.
- Diagrama Lógico de la red.

Recursos de Contingencia

- Componentes de Remplazo
- Diagrama Lógico de la red

FALLA DEL SERVIDOR

Puede presentarse por pérdida/daño de *hardware* y *software* (Algunas causas del fallo en un Servidor pueden ser: Error Físico en una cuchilla, Error de Memoria RAM, Error de Tarjeta(s) Controladora(s) de Disco, Error Lógico de Datos, error en Sistema Operativo). Perdida del proceso automático de *Backup* y *Restore* e Interrupción de las operaciones.

Recursos de Contingencia

- Componente de Remplazo (Memoria, Disco Duro, etc.).
- Replica a un servidor diferente de los aplicativos y bases de datos de la institución.
- Copia de Seguridad diaria de la base datos.
- Copia mensual de la base datos que se quema en cd y se guarda en el archivo central.
- Se genera *backup* diario de la página *WEB* y de la Intranet.
- Se cuenta con el soporte 24x7X365 con el proveedor de la página y del servicio.
- Existencia de un *Datacenter* donde se tiene la infraestructura que almacena los sistemas de información utilizados en la institución. Protegido por un sistema de control de acceso, aire acondicionado de precisión, detección y control de incendios, monitoreo diario del comportamiento de esta infraestructura que está alimentada por dos circuitos eléctricos independientes que llegan a dos ups autónomas. Una respaldo de la otra.

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.

- La unidad de emergencias y desastres pondrá en funcionamiento la planta de energía de la institución.
- Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones, para que no corten bruscamente el proceso que tienen en el momento del apagón.
- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de UPS a corriente normal (Corriente brindad por la empresa eléctrica).

- El centro de datos está conectado con la planta de la institución. De esta manera garantizamos que mientras la planta funcione el centro de datos podrá prestar sus servicios.

Recursos de contingencia

- Asegurar que el estado de las baterías del UPS, se encuentren siempre cargadas.
- Asegurar o garantizar que el funcionamiento de la UPS sea el óptimo de manera que funcione en el día del evento.

RESPONSABLES DEL PLAN DE CONTINGENCIA

El paso inicial en el desarrollo del plan es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia, para la cual se definen los siguientes responsables:

- Profesional Especializado – Unidad Funcional de Apoyo tecnológico y de Información.
- Profesional Universitario – Unidad Funcional de Apoyo Tecnológico y de Información.
- Técnico de Planta – Unidad Funcional de Apoyo Tecnológico y de Información.
- Equipo Técnico y Profesional que hacen parte de la Unidad Funcional de Apoyo Tecnológico y de Información.
- Profesional Universitario Estadística.
- Profesional Universitario Gestión Documental.

PASOS A SEGUIR PARA REPORTAR UN EVENTO DE CAIDA O FALLA DE LOS SISTEMAS DE INFORMACION

Reportar el servicio afectado a la UFATI.

El personal de UFATI que recibe la notificación del evento se desplazara de ser necesario al sitio para revisar la situación reportada.

Diligenciamiento por el personal de UFATI el formato Reporte de Daños a los Sistemas de Información (GII-SISFO-02).

Soluciones al evento

El profesional de sistemas realizará las siguientes acciones:

- Ejecutar el plan de contingencia.
- Cadena de llamadas del plan de contingencia. La cadena de llamadas se activa por el técnico y/o ingeniero de turno y que atendió el llamado, quien

debe proceder a informar al profesional universitario de sistemas, dependiendo de la magnitud del suceso seguirá el conducto regular.

- Analizar el tipo de riesgo y el impacto en el hospital.
- Determinar las prioridades del proceso, que indique cuales son las aplicaciones y sistemas críticos en el momento de ocurrencia del desastre y el orden de proceso correcto.
- Coordinar con los diferentes responsables de los procesos del plan de contingencia.
- Realizar seguimiento de la ejecución de los procesos.
- Recuperación de las copias de seguridad.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores.
- Conexión de emergencias y desastres. Si dentro de la ejecución de las actividades encontradas están contempladas en el plan de emergencias y desastres, el comité de este plan de contingencia emitirá una comunicación al comité de emergencias y desastres.

El profesional de sistemas que activó el plan de contingencia debe diligenciar los datos de lo ocurrido en el Formato de reporte de Daños a los Sistemas de Información (GII-SIS-FO-02), que posteriormente será complementado y evaluado.

Durante la suspensión del sistema de información (si es programado) o en el momento de presentarse la falla, los diferentes servicios darán aplicación en forma manual a los formatos establecidos por la institución.

ACTIVIDADES DESPUÉS DEL DESASTRE

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro:

Evaluación de daños. El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de la ESE HUS se deben atender los procesos misionales, de apoyo y demás sistemas de Información primordiales para el funcionamiento de la Entidad, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

Priorizar Actividades. La evaluación de los daños reales dará una lista de las actividades que se deben realizar, preponderando las actividades estratégicas y urgentes de la institución. Las actividades comprenden la recuperación y puesta

en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

Ejecución de actividades. La ejecución de actividades implica la colaboración de todos los funcionarios, creando equipos de trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones.

Los trabajos de recuperación se iniciaran con la restauración del servicio usando los recursos de la institución. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

Evaluación de Resultados. Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por el siniestro, se debe evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

Retroalimentación de Actividades. Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

Cargue de la información a los aplicativos de ESE HUS. Una vez pasado el evento los responsables o delegado de cada servicio se comprometen a subir la información en los aplicativos correspondientes, en un lapso de tiempo no mayor a 48 horas después de restaurado el servicio, presentándose el debido informe al Jefe del Servicio.

Presentar Reclamación al área encargada de exigir pólizas de cumplimiento. Ante el siniestro presentado, se realizará el levantamiento de los daños

ocasionados y se enviará el informe al área de almacén, para que estos tramiten el proceso de reclamación de las pólizas correspondientes.
Una vez restablecido el servicio del software estos formatos serán diligenciados por los responsables en el sistema, igualmente estos formatos serán enviados a estadística para ser archivados en las respectivas historias clínicas físicas.

Recursos económicos. La ESE HUS debe disponer de recursos económicos en su presupuesto para restablecer los sistemas de información.

En este caso del Servidor FreeRADIUS entra en funcionamiento otro Servidor FreeRADIUS configurado en una máquina que se encuentra ubicado en la casa de la Gerencia y lo único que se necesitaría seria actualizar la lista de usuarios con sus contraseñas que se encuentran en el archivo users.conf e iniciar el Servidor como tal.

6. CONCLUSIONES

- Como resultado de este trabajo se observa que se realizó la revisión a las normas y estándares internacionales que tienen que ver con las redes inalámbricas así como también se tomó la decisión de superar la vulnerabilidad en las claves de acceso a la red con la implementación del Servidor RADIUS.

- Se realizó el análisis a los diferentes modelos de Access Point que se encuentran en la institución para obtener la configuración adecuada de acuerdo a sus características.

- Se adecuó la máquina que se escogió de Servidor tanto en su Sistema Operativo como con todas las actualizaciones necesarias para evitar que sea vulnerable a cualquier ataque y así poner en riesgo la seguridad de la red.

- Se configuró el Servidor RADIUS y se puso a prueba en el primer piso del edificio del Hospital ya que es el área donde se encuentran las oficinas de la Unidad Funcional de Apoyo Tecnológico y de Información y de esta manera se hace un monitoreo permanente durante un periodo de prueba.

BIBLIOGRAFÍA

Cisco. Terminal Access Controller Access System (TACACS+) [en línea]. <http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/sctplus.html> [citado en 6 de septiembre de 2014]

Answer.yahoo.com. Bueno un hacker es una persona que (burla la seguridad para dañar sistemas, archivos, robas cuentas, contraseñas y demás) [en línea]. <https://espanol.answers.yahoo.com/question/index?qid=20100519142203AAh1BKT> [citado en 6 de septiembre de 2014]

La Web del Programador. Diccionario informático [en línea]. <http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=N> [citado en 6 de septiembre de 2014]

Yahoo! Respuestas. ¿Que es una norma? Son un conjunto de reglas o pautas a las que se ajustan las conductas o normas sociales que constituyen un orden de valores orientativos [en línea]. <https://espanol.answers.yahoo.com/question/index?qid=20070601172032AAxWK6b> [citado en 6 de septiembre de 2014]

www.mailxmail.com. Introducción a las redes inalámbricas, Capitulo Introducción a las redes inalámbricas [en línea]. <http://www.mailxmail.com/curso/informatica/wifi/capitulo1.htm> [citado en 6 de septiembre de 2014]

www.monografias.com. Protocolos de Seguridad web [en línea]. <http://www.monografias.com/trabajos14/segur-wlan/segur-wlan.shtml#intro> [citado en 6 de septiembre de 2014]

CISCO. Protección de las redes inalámbricas [en línea]. <http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html> [citado en 11 de septiembre de 2014]

Windows.microsoft.com. Cuáles son los diferentes métodos de seguridad en redes inalámbricas? [en línea]. <http://windows.microsoft.com/es-xl/windows/what-are-wireless-network-security-methods#1TC=windows-7> [citado en 11 de septiembre de 2014]

Bitacoraderedes.wordpress.com. Configuración de un servidor radius en Windows server 2012 [en línea]. <http://bitacoraderedes.wordpress.com/2013/07/30/configuracion-de-un-servidor-radius-en-windows-server-2012-parte-2a/> [citado en 11 de septiembre de 2014]

SCHWARTZKOPFF, Michael. Acceso Seguro a Redes con 802.1X, RADIUS y LDAP [En línea] <http://www.linuxmagazine.es/issue/05/Radius.pdf> [citado en 11 de septiembre de 2014]

ANEXO A

GLOSARIO

ACCESS POINT: los puntos de acceso, también llamados APs o wireless access point, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El access point o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

ACL: significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

HACKER: es una persona que burla la seguridad para dañar sistemas, archivos, robar cuentas, contraseñas y demás.

OSA VS. SKA: OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

RED DE COMPUTADORAS: como una colección de estaciones de trabajo autónomas que son capaces de intercambiar información entre ellas. Existen varios criterios para clasifica redes de computadoras. Un criterio es la estructura de interconexión, otro es el modo de transmisión, y el tercero lo representa la distribución geográfica.

BANDWIDTH: ancho de Banda. Capacidad de un medio de transmisión.

CABLEAR: acción de tender cables para la transmisión de voz, datos o cualquier otro tipo de información, en un entorno determinado. En la actualidad, el término se utiliza con cierta frecuencia al referirse a edificios de nueva construcción o edificios inteligentes. Este tipo de edificios son cableados en la fase de construcción, con el fin de ofrecer puntos de acceso a ordenadores, teléfonos, etc., evitando la operación posterior de tendido de cables. Para ello se utiliza un espacio habilitado mediante un falso techo o un falso suelo, en el que se alojan los cables y demás elementos de conexión.

CAÍDA: resulta muy habitual aunque no por ello menos incorrecto asegurar que el ordenador se ha caído, para indicar que no funciona correctamente en un momento determinado por interrupción de la comunicación con el ordenador central u otras causas.

FIBRA ÓPTICA: sistema de transmisión que utiliza fibra de vidrio como conductor de frecuencias de luz visible o infrarroja. Este tipo de transmisión tiene la ventaja de que no se pierde casi energía pese a la distancia (la señal no se debilita) y que no le afectan las posibles interferencias electromagnéticas que sí afectan a la tecnología de cable de cobre clásica.

NETWORK: RED: conjunto de hardware y software de gestión necesario para la conexión de múltiples ordenadores con el fin de que puedan intercambiar información entre ellos y compartir recursos. La Red puede ser de área local (LAN) o de área amplia (WAN).

SSID: Significa Service Set IDentifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TR(s) deben conocer el nombre de la red para poder unirse a ella.

WI-FI ZONE: son redes hot spot inalámbricas a las que los usuarios pueden acceder cuando están en lugares públicos. Generalmente se encuentran en aeropuertos, cafés, etc. Solo los proveedores de servicios que cumplen los estándares de implantación y servicio de zonas Wi-Fi pueden mostrar este logotipo.