UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO - CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS Y DISEÑO DE LINEAMIENTOS PARA GENERAR UNA PROPUESTA DE SOLUCIONES DE SEGURIDAD PARA LA GESTIÓN DE USUARIOS SOBRE EL SEGMENTO WLAN DE LA EMPRESA PRONACA UBICADO EL CENTRO DE DISTRIBUCIÓN "CD QUITO SUR", COMO PROTOTIPO

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

JORGE LUÍS MENA LUDEÑA

DIRECTOR: ING. JORGE LÓPEZ

Quito D.M., Enero 2013

DECLARACIÓN

Yo, Jorge Luis Mena Ludeña, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Jorge Luis Mena Ludeña

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Luis Mena Ludeña, bajo mi dirección.

_____

Ing. Jorge López

Director de tesis

AGRADECIMIENTOS

A Dios, San Josemaría Escrivá de Balaguer por sus bendiciones, mis padres Luis Mena y Martha Ludeña, mi hermana Dorys Mena Ludeña y su familia, mi novia Aracely Pérez; que con su esfuerzo y dedicación supieron apoyarme para lograr culminar mi carrera universitaria.

A PRONACA, por brindarme las facilidades para realizar este trabajo.

Al Ing. Jorge López, por su guía, paciencia y conocimientos que me ayudaron a culminar este proyecto.

_____

Jorge Luis Mena Ludeña

DEDICATORIA

A Dios, San Josemaría Escrivá de Balaguer, mis padres Luis Mena y Martha Ludeña, mi hermana Dorys Mena Ludeña y su familia, mis amigos y a todos los que siempre han creído en mí, porque sin ustedes mi vida no tendría sentido.

_____

Jorge Luis Mena Ludeña

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto habla sobre el análisis y diseño de lineamientos parar generar una propuesta de soluciones de seguridad para la gestión de usuarios sobre el segmento WLAN de la Empresa PRONACA ubicado en el Centro de Distribución “CD Quito Sur”, como prototipo.

En el primer capítulo esta la descripción del problema, los objetivos de la investigación, justificación del proyecto, el alcance del mismo y los aspectos metodológicos.

En el segundo capítulo se encuentra el marco teórico donde se tiene: la introducción, historia, medios de transmisión, características estándares, seguridades vulnerabilidades e impacto de las redes wifi.

En el tercer capítulo se tiene los esquemas del diseño de la red, el análisis de los lineamientos para definir las políticas de seguridad y la descripción de todos los dispositivos que se necesitan para crear una red wifi.

El cuarto capítulo trata de la definición de las políticas de seguridad para cada usuario que trabaje en la empresa y de la gestión de usuarios dependiendo el cargo que cada uno de ellos mantenga.

Finalizando, está el quinto capítulo en donde se tiene las conclusiones, recomendaciones, bibliografía, net grafía, y el glosario de términos**.**

CAPÍTULO 1

1 INTRODUCCIÓN

1.1 ANTECEDENTES

La seguridad es una de las partes importantes en la implementación y administración de redes. Tiene el desafío de encontrar un punto medio entre dos requerimientos que son de gran importancia: la necesidad de cuidar y proteger aquella información que sea privada, y escalabilidad para respaldar las oportunidades comerciales en evolución.

La aplicación de una solución de seguridad eficaz es un paso importante que puede dar una organización para proteger su red. Brinda pautas acerca de las actividades que deben llevarse a cabo y los recursos que deben utilizarse para proporcionar seguridad a la red de una organización.

La solución que necesitan las empresas para proteger su información y a su vez tener mayor independencia de movimiento son las WLAN[1], ya que esta red les brinda mayor flexibilidad al momento de adaptarse a los cambios frecuentes.

La empresa PRONACA ha considerado la implementación de una red WLAN, no obstante, aun no cuenta con soluciones de seguridad y gestión de usuario que le aseguren la confidencialidad de los datos y las comunicaciones que se manejen por este canal.

Toda la información digital que PRONACA maneja, incluyen cifras, direcciones, nombres, cantidades, entre otros datos relacionados con los clientes, y referente a la propia empresa, por lo que la implementación de la red WLAN, si bien es inminentemente necesaria, causa temor en el sentido de la vulnerabilidad de la información.

---

1 WLAN (Wireless Local Area Network-Red de Área Local Inalámbrica)

Este suceso aparece en todas las empresas al momento que un hacker intenta acceder a las bases de datos y robar los datos de sus clientes para suplantar identidades o para hacer mal uso de ellos.

Debido al incremento de host, la seguridad se debe incrementar por que el medio por el cual se transmite la información es fácil de interceptar, extraer o robar la información de la persona que la está transmitiendo.

Un creciente número de empresas son víctimas de lo que se puede denominar como “Fugas y Fraudes”[2] en los “Sistemas Internos y Externos de la Información”[3]. Estas “Fugas y Fraudes”, combinadas con los crecientes “Delitos Electrónicos”[4], son difíciles de cuantificar económicamente. Las consecuencias son imperceptibles y catastróficas.

Tanto para la sociedad civil, el sector privado y el Estado, la información es poder. El incorrecto uso de la información, desinformación, manipulación, la falta de ética en la industria de las NTCI’s[5], los sitios Web cuestionables y otros elementos están desarticulando a miles de empresas, especialmente a las pequeñas y medianas empresas.

La sociedad de la información ha rediseñado una serie de valores, ha redefinido la cultura y la manera de cómo muchas personas actúan.

Para las empresas es importante que el intercambio de datos en la red sea la capacidad para mantener la seguridad de los mismos. Por temor a los crecientes problemas de seguridad, algunos administradores de redes evitan instalar redes WLAN, desperdiciando las ventajas que ofrecen.

---

5 NTCI (Normas Técnicas de Control Interno)

En la actualidad, el panorama de la seguridad inalámbrica ha cambiado, por lo que los gerentes de IT[6] pueden implementar redes WLAN con confianza.

PRONACA cuenta con infraestructura Cisco lo que significa que hoy en día mediante la red inalámbrica unificada, ofrece una solución de seguridad de WLAN basada en normas de clase empresarial que admite las siguientes funciones para productos inalámbricos de Cisco, y host clientes WLAN compatibles con Cisco.

- Compatibilidad con la norma IEEE 802.11i.
- Compatibilidad con las certificaciones de seguridad de Wi-Fi Alliance: WPA[7] y WPA2[8].
- Autenticación segura, mutua, y administración dinámica de claves de cifrado mediante la compatibilidad con la norma IEEE 802.1X.
- Cifrado de datos mediante la norma AES[9] o el protocolo TKIP[10].
- Compatibilidad con la más amplia gama de tipos de autenticación 802.1X, dispositivos clientes y sistemas operativos clientes del mercado.
- Mitigación de ataques activos y pasivos a la red.
- Integración con la Red de autodefensa de Cisco y el Control de admisión a la red NAC[11].
- Funciones del Sistema de prevención de Intrusiones llamado IPS[12] y servicios avanzados de ubicación con visibilidad de la red en tiempo real

---

6 IT (Information Technology -Tecnologías de la Información)

7 WPA (Wireless Protected Access - Acceso Inalámbrico Protegido)

8 WPA2 está basada en el nuevo estándar 802.11i, creado para corregir las vulnerabilidades detectadas en WPA.

9 AES (Advanced Encryption Standard)

10 TKIP (Temporal Key Integrity Protocol - Protocolo de integridad de clave temporal)

11 NAC (Network Access Control - Control de Acceso a la Red)

12 IPS (Intrusion Prevention Systems - Sistema de detección de Intrusos y Prevención)

convergencia de la seguridad Wi-Fi interior y exterior con la solución de red de malla inalámbrica de Cisco.

La tecnología es sin lugar a dudas una importante llave en el nuevo modelo de la gestión de negocios, pero esta llave abre otras puertas. Una de ellas es la vulnerabilidad de la empresa. Preparar el negocio para la conectividad exige que simultáneamente se implementen una serie de medidas estratégicas que no pongan en riesgo la seguridad de la información. El fruto intangible de muchos años de trabajo como es la información sobre los clientes, los planes de negocios, presupuestos, estados financieros e informaciones valiosas no pueden correr el riesgo de ser accedida por cualquier particular.

El presente proyecto surge como respuesta a esta necesidad de PRONACA de mejorar la seguridad en su información y definir soluciones de seguridad para los usuarios y la gestión de los mismos en su segmento WLAN.

1.2 JUSTIFICACIÓN

El Centro de Distribución Sur de PRONACA tiene actualmente antenas para conexión inalámbrica, las cuales fueron instaladas con el propósito de conectar las PDA's al momento de descargar los contenedores, sin embargo, el proyecto se pospuso por lo que se optó por utilizar estas antenas para la conexión de los usuarios del centro de operaciones a través de un segmento WLAN.

Se reutilizara la infraestructura ya instalada y se aprovechara la misma, con las limitaciones de que estas antenas son direccionales, por ende, existirán usuarios que no puedan conectarse a la red una vez salgan del rango al que este apuntando la antena, lo que no pasa con las antenas omnidireccionales que emiten la señal en un radio determinado.

El desarrollo del presente proyecto se justifica debido a que no se cuenta con soluciones de seguridad para conexiones wireless, ya que se tiene solo accesos

inalámbricos por AP[13], los cuales se validad en un switch capa 3 dentro de este en la ACL[14], ubicado en centro de operación.

En la actualidad la mayor parte de empresas del país utilizan conexiones inalámbricas para ejecutar aplicaciones, transferencia de archivos, compartir recursos, entre otros. Dichas organizaciones requieren tener soluciones de seguridad que permitan a los administradores de la red otorgar los permisos necesarios a los usuarios para acceder aplicaciones, archivos, recursos y de esa forma evitar que la empresa se vea vulnerable al acceso de intrusos sea este interno o externo.

Una red wireless, autentificar usuarios y realizar soluciones de seguridad para mantener la confidencialidad de los datos, es difícil que una LAN.

Acceder a los datos de un usuario, violar la seguridad y autenticación es fácil, ya que cuando un usuario tiene los permisos necesarios, no tiene ningún tipo de control en alguna instalación física como la LAN, de la misma manera se puede violar la confidencialidad de los datos, debido a que este tipo de transmisiones se las realiza por ondas de radio frecuencia, y estas a la vez viajan a través de la organización sin ningún tipo de control, ya sea por las paredes e incluso fuera de la misma empresa, lo que permite al fácil acceso de los intrusos a la red.

Este recurso de seguridad, compuesto por las soluciones y la gestión de usuarios, no existe actualmente en el Centro de Distribución Sur de la empresa PRONACA, por lo que se contempla como fundamental y necesario el análisis y diseño de los lineamientos para poder definir soluciones de seguridad y gestión de usuarios para su implementación en el centro de distribución.

Las redes inalámbricas son sensibles a violaciones de seguridad, debido al tipo de políticas utilizadas para la autentificación y confidencialidad de información,

13 AP (Acces Point - Punto de Acceso)

14 ACL (Access Control List -Listas de Control de Accesos)

pues al tratarse de ondas de radio, estas pueden ser interceptadas sin que la organización pueda controlar este hecho.

La información que se transmite por este medio puede ser de tipo confidencial, por lo que es inminente el diseñar soluciones de seguridad y gestión de datos a fin de proteger la integridad de la información.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Analizar y diseñar los lineamientos para generar una propuesta de soluciones de seguridad para la gestión de usuarios sobre el segmento WLAN de la empresa PRONACA ubicado el centro de distribución "CD QUITO SUR", como prototipo piloto.

1.3.2 OBJETIVOS ESPECÍFICOS

- Determinar el estado de la red wlan de PRONACA para detectar los puntos más vulnerables a través de investigación de campo.
- Definir los lineamientos para generar soluciones que sean destinadas a los usuarios y promover el buen uso de los equipos y la confidencialidad de los datos que a cada uno se les asigna.
- Establecer los perfiles a cada usuario para que manejen información específicamente asignada.
- Proporcionar posibles métodos de seguridad a la configuración de la red WLAN para ser tomados en cuenta y sean considerados como una buena opción para ser aplicados.
- Diseñar soluciones mediante el uso y aplicación de políticas para los colaboradores que labora en las áreas operativas de planta y parte de la administrativa.
- Analizar las soluciones una vez definidas, para que concuerde con el cumplimiento de las normativas que estén establecidas en la empresa.

- Presentar la propuesta de las soluciones de seguridad para que sea analizado por el personal de sistemas de PRONACA y consideren una implementación.

1.4 ALCANCE

El alcance de la investigación se refiere a los aspectos donde tendrá una incidencia directa en:

Realizar un análisis por escala del problema de seguridad con puntos centralizados de acceso, implementando dispositivos de seguridad en distintas áreas y tomar el control del acceso interno con políticas de seguridad de firewall.

Realizar una revisión del estándar IEEE[15] 802.11 y considerar las peculiaridades para trabajar en distancias largas.

Estudiar la posibilidad de añadir más seguridad y calidad a la red inalámbrica mediante el análisis de otros estándares del IEEE 802.11.

Establecer las políticas de seguridad basándose en dos puntos principales:

1.- Definir soluciones para los usuarios, de esa manera garantizar el buen uso de los host y de la información asignada, para que quede claro las reglas a las que están obligados a cumplir y caso contrario llevar a cabo una sanción para aquella o aquellas personas que no acaten las normas dispuestas por el departamento de sistemas y gerencial.

2.- Definir las soluciones para los encargados del proceso de gestión de usuarios, para poder así definir los perfiles que se les asignara a cada uno de los usuarios y puedan cumplir una tarea específica, de esa manera lograr la integridad de los datos y así no tengan los permisos para acceder a los datos más importantes.

---

15 IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos).

Establecer parámetros para definir los nombres de usuario y las contraseñas para que sean solidas y complejas de descifrar por personas que no pertenezcan a la institución.

Analizar el entorno, la población y radio-propagación de la zona para el diseño de la red inalámbrica utilizando distintas especificaciones y realizarlo bajo políticas estandarizadas.

Diseñar lineamientos mediante metodología de investigación para definir las soluciones en la seguridad, gestión de usuarios en cuanto a la validación y autentificación para establecerlos como parte de la seguridad de la empresa y poder brindar una comunicación más eficaz al centro de operacion.

Presentar el documento del prototipo de la implementación de soluciones de seguridad y gestión de usuarios para su respectivo análisis.

Proveer de un documento a cada uno de los colaboradores que conformen la empresa, para de esa manera fomentar el conocimiento de las normas que cada uno de ellos debe cumplir.

Entre los importantes aspectos se tiene:

- **Soluciones de seguridad**

Las soluciones de seguridad permite estructurar los permisos que se pueden asignar a los usuarios mediante 3 robustos esquemas incorporados en la plataforma que son los perfiles, facultades y los usuarios.

A los perfiles o roles, se les define los permisos a módulos, submódulos y funcionalidades. Posteriormente se definen las facultades vinculadas a cada perfil, las facultades permiten determinar los rangos de valores para los que puede intervenir un perfil. Finalmente se definen los usuarios del sistema y se los vincula a un perfil existente, con lo cual ese usuario empieza a desempeñar su rol.

Se va realizar una investigación experimental en relación a las soluciones de seguridades a desarrollar para la propuesta de implementación de la misma, con este esquema, ante un cambio en el desempeño de rol de un usuario, no es necesario redefinir todos los permisos sino simplemente efectuar el cambio de perfil.

- **Soluciones de mantenimiento**

El mantenimiento de la red es una de las actividades más importantes en una empresa, es el proceso de mejora y optimización de la red después de su entrega al usuario final, así como también corrección y prevención de los defectos.

Por razones en las cuales los usuarios manejan los host, se deberá realizar un documento en el que se explique el uso de estos para aprovecharlo al máximo, teniendo en cuenta la responsabilidad que lleva al uso de los mismos, esta actividad es parte fundamental que la empresa deberá cumplir ya que deben mantener la responsabilidad activa en cada uno de sus colaboradores.

1.4.1 ESTRUCTURA ORGANIZACIONAL[16]

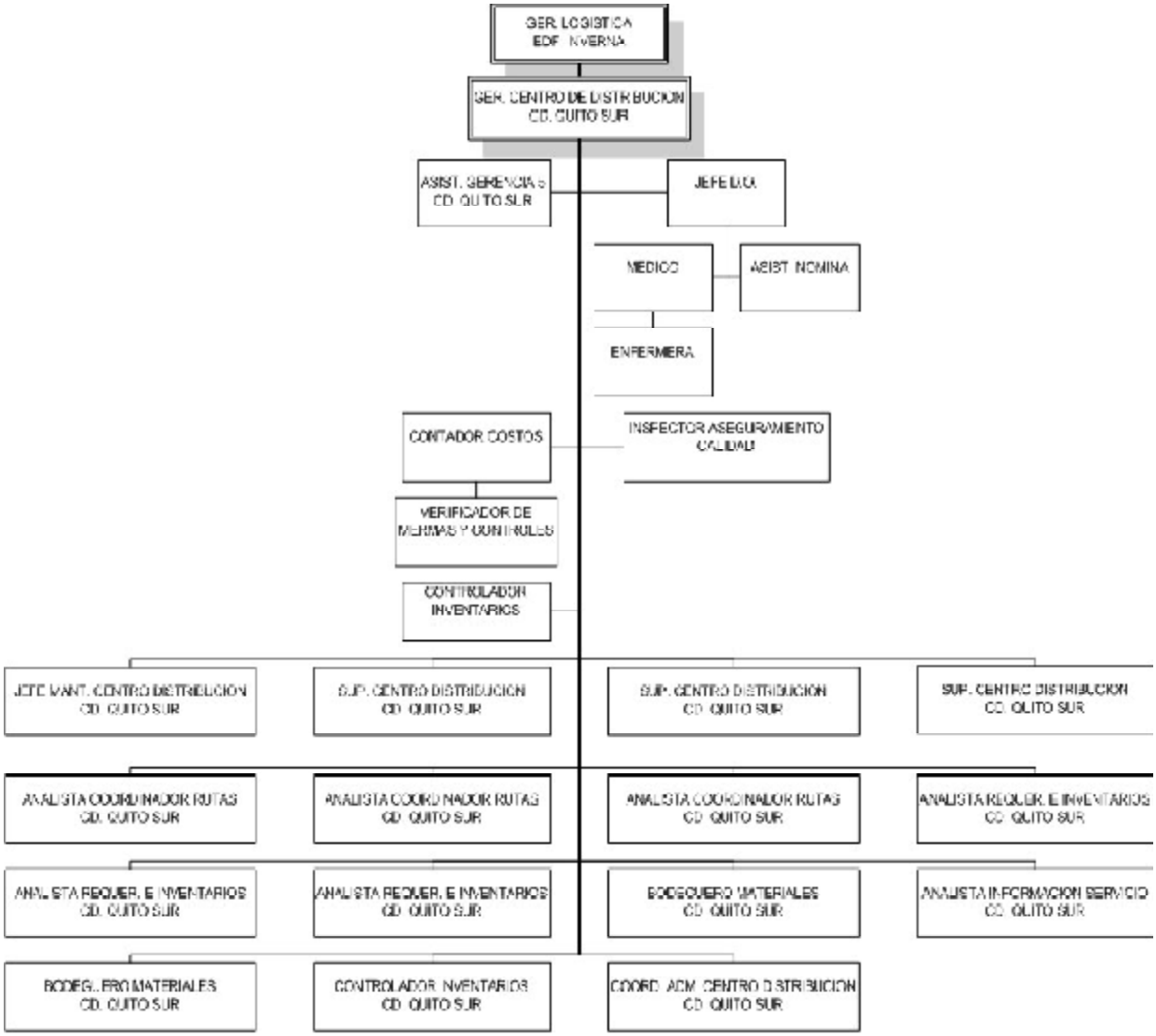

Figura 1.1 : Descripción Organizacional

Fuente: Dpto. Estructura y Compensación PRONACA, Ing. Raquel Ordoñez

CAPÍTULO 2

2 FUNDAMENTACIÓN TEÓRICA

2.1 PRECEDENTES

"Procesadora Nacional de Alimentos PRONACA es una empresa nacional líder en el mercado de alimentos. Tiene una integración vertical, pues produce su materia prima, la procesa y la vende a clientes finales. Luego de posicionarse en el mercado local empezó a expandir sus operaciones en el extranjero." [17]

El consumo en los hogares se ha incrementado a través de nuevos productos y nuevas líneas. En el mercado internacional incursionando en Brasil con una planta de palmito y, en Colombia, con una planta que elabora productos con valor agregado, como nuggets, hamburguesas, platos listos, empanadas, entre otros.

Son los primeros pasos de PRONACA fuera del Ecuador. Antes incursionaron en Estados Unidos y en Europa a través de la comercialización de productos producidos en el país, como palmito, camarón, tilapia y alcachofa. Hay líneas de mayor dinamismo, que van de la mano con los nuevos productos: pescado con la marca Mr.Fish, productos listos con la marca Mr.Cook, además de líneas de embutidos, pollo, cerdos, conservas, salsa de tomate, mayonesas, entre otros. La inversión ha sido mayor en los últimos tres años en infraestructura, marca, comunicación, capacitación, innovación y desarrollo.

2.2 RESEÑA HISTÓRICA

"PRONACA es una corporación constituida por varias compañías relacionadas con la industria avícola y alimenticia. En el año 1957 su fundador, Lodewijk Jan Bakker, de procedencia holandesa, constituye la empresa INDIA dedicada a la importación de artículos para la industria textil e insumo agrícolas. En el año 1958 el Sr. Lodewijk Jan Bakker junto a su hijo, Luis J. Bakker comienzan la actividad

avícola en el país, con la producción de huevos comerciales y la venta de pollitas importadas, actividad que se lleva a cabo en la hacienda La Estancia, ubicada en Puembo." [18]

En el año 1965, se ofrece oportunidades para desarrollar nuevas actividades debido a la gran demanda de pollos, en ese momento inauguran la Incubadora Nacional Compañía Anónima "INCA" y fue la única que utilizaba procesos tecnológicos en el Ecuador.

En ese mismo año nacen los primeros pollos. En 1974, se crea la empresa "INDAVES" y se integra para la producción de huevos que se pueda comercializar. A mediados de los setenta en Puembo se instala la granja nacional de aves "GRANADA", en donde empezaron con la primera producción de pollo de engorde.

En 1979 se instala la primera procesadora de pollos, con el nombre de Procesadora Nacional de Aves "PRONACA".

En 1981 se crea la división de alimentos que produce balanceado para las granjas. Bajo el concepto de crear una serie de industrias que se abastezcan entre sí, que permite una mayor productividad y eficiencia.

2.3 FILOSOFÍA DE LA EMPRESA[19]

En base a la información obtenida de la empresa PRONACA, la filosofía es la siguiente:

- **Proveedores**

  PRONACA cree y practica el respeto a sus proveedores, a quienes les ofrece un beneficio justo en cada negociación, dentro de un marco de

comportamiento ético. Promueve el cumplimiento de la ley y una conducta social responsable.

- **Colaboradores**

  PRONACA lidera a sus colaboradores con el ejemplo, en forma competente, justa y ética. Tiene un compromiso solidario y respetuoso con el bienestar de cada uno de ellos y no tolera la deshonestidad. Reconoce el talento y ofrece una remuneración equitativa. Promueve el trabajo en equipo y la delegación con responsabilidad en condiciones laborales de limpieza, orden y seguridad. Ofrece igualdad de oportunidades de empleo, desarrollo y promoción a todos quienes están calificados para ello. Motiva y acoge sugerencias y recomendaciones de sus colaboradores para el bien de la compañía.

- **Clientes**

  PRONACA trabaja junto a sus clientes ofreciendo siempre productos de calidad. Innova sus procesos y productos para liderar los mercados en los cuales está presente. Atiende los pedidos de sus clientes con un servicio rápido y prolijo.

- **Consumidores**

  La primera responsabilidad de **PRONACA** es proveer productos innovadores, saludables y de calidad que alimenten bien a sus consumidores y contribuyan al bienestar y satisfacción de sus familias.

- **Sociedad**

  PRONACA, en consonancia con su responsabilidad corporativa, actúa como un buen ciudadano, que siempre busca las mejores relaciones con los diferentes grupos de interés, en un ambiente de armonía y colaboración. Comparte su experiencia y conocimiento para contribuir al desarrollo y al mejoramiento de la calidad de vida de las áreas de influencia de sus operaciones. Alienta el civismo y paga los impuestos que le corresponden. Es respetuosa y solidaria con las personas y con el cuidado del equilibrio ambiental.

- **Asociados**

  PRONACA actúa responsablemente con productores y emprendedores. Invierte en investigación y desarrollo, y crea productos innovadores. Comparte su filosofía y crea oportunidades de negocio para sus asociados, con quienes mantiene una relación cercana, equitativa y provechosa.

2.4 VALORES DE LA EMPRESA[20]

- **Integridad**

  Ser integro exige coraje para decir siempre la verdad y obrar en forma recta y clara.
- **Responsabilidad**

  La responsabilidad garantiza el cumplimiento de los compromisos adquiridos y genera confianza y tranquilidad entre las personas.
- **Solidaridad**

  Cuando dos o más personas se unen y colaboran mutuamente para conseguir un bien común, hablamos de solidaridad.

2.5 MARCO REFERENCIAL

2.5.1 REDES INALÁMBRICAS

2.5.1.1 Introducción

El termino inalámbrico wireless se aplica al tipo de comunicación en la cual no se utiliza ningún medio guiado o propagación física, utiliza ondas electromagnéticas que se propagan en el espacio sin ningún tipo de medio físico como lo hace LAN.

En la actualidad, comunicar host por medios inalámbricos es lo que ha dado realce al crecimiento de la tecnología por lo que se está realizando amplias investigaciones en cuanto a diferentes tipos de ondas inalámbricas como son las ondas de radio, luz infrarroja y bluetooth. Estas redes facilitan la comunicación y

operaciones en lugares donde el host no permanece en un solo lugar, ya sea en almacén o en un edificio que tiene varias oficinas.

Tener en cuenta que una red inalámbrica el comportamiento es similar a una LAN, aunque varia la forma de acceder a la red. El principal problema con las redes inalámbricas es sin duda la seguridad, ya que puede o no ofrecer seguridad en cuanto al ingreso de intrusos a la red.

Se puede combinar una red cableada con una red inalámbrica y crear una red hibrida para poder resolver problemas en cuanto al alcance de las redes pero siempre tomando como prioridad a la red cableada para que la inalámbrica proporcione movilidad y así el colaborador se pueda desplazar en su lugar de trabajo.

Existen muchas aplicaciones que se puede realizar con redes inalámbricas y de este modo crear una nueva y moderna forma de utilizar la información, ya que estará al alcance de cualquier usuario a través del internet en cualquier lugar del mundo.

2.5.1.2 Redes de Área Local Inalámbrica WLAN

En la presente investigación se describe que una red inalámbrica es un medio de comunicación sin la necesidad de un medio guiado, como son las redes cableadas. Utiliza radiofrecuencia permitiendo que la transmisión sea por el aire y pueda haber mayor movilidad para los usuarios y así minimizar los gastos en cable. Las redes inalámbricas van ganando campo en las empresas por que permite la comunicación entre las oficinas, las diferentes áreas, y sobre todo en los hogares, ya que de esta manera se puede compartir el internet a varias host que existan en el hogar, como se muestra en la Figura 2.1.

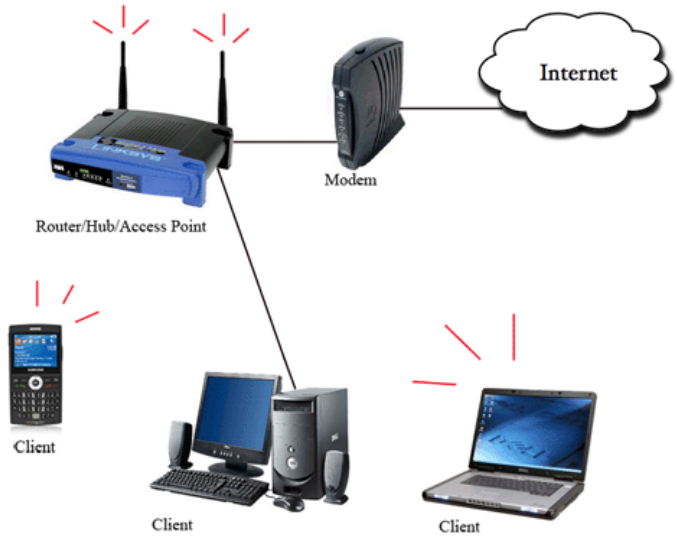

Figura 2.1: Redes de área local inalámbrica[21]

Fuente: http://padegaindia.in/2011/09/ccna-wireless-tutorial-and-questions/

2.5.1.3 Transmisión Inalámbrica

Al ser un medio de transmisión no guiado, utiliza ondas electromagnéticas para llevar la información de un lado a otro, referirnos a ondas electromagnéticas, se entiende que debe existir un host que emita ondas electromagnéticas por medio de una antena y luego se recibe esta energía con otra antena, del cual se extraen los paquetes de datos para ser receptados por el host conectado a la red.

Existen dos tipos de emisión y recepción de las ondas, direccional y omnidireccional.

En las antenas direccionales se transmiten las ondas de forma directiva lo cual tanto el emisor como el receptor deben estar alineados, lo que no sucede con el omnidireccional ya que esta emite las ondas en diferentes direcciones por lo que varias antenas pueden captarlas, mientras más fuerte sea la señal de transmisión mejor será la conectividad de los host.

2.5.1.4 Ventajas de la WLAN

Las WLAN ofrecen comodidad superior a las redes LAN porque cualquier usuario que tenga la cobertura para acceder a la red, puede conectarse en cualquier lugar en el cual se mantenga es espectro del radio, una vez que se haya configurado, la red inalámbrica permite la conexión de varios host al mismo tiempo, evitando gasto de infraestructura.

El Wi-Fi es un estándar de redes, que asegura la compatibilidad entre distintos productos con certificación Wi-Fi de otros fabricantes. Con una conexión Wi-Fi, los usuarios tienen compatibilidad con varios productos inalámbricos y así evitaran altos costos y no tendrán que regirse a soluciones propias de un solo fabricante.

Por otro lado, al elegir una solución inalámbrica basada en estándares, permitirá que la red inalámbrica trabaje sin interrupciones, incluso con una conexión ya existente de una red LAN.

Se debe asignar el protocolo DHCP[22], el cual asignará automáticamente direcciones IP a los host inalámbricos, reduciendo el tiempo que costaría asignar una dirección IP a cada host, tan solo utilizando un servidor que asigne automáticamente.

Esto ofrecerá a los usuarios movilidad dentro o fuera de sus puestos de trabajo.

Hay que tomar en consideración el ambiente, para seleccionar la mejor señal y obtener niveles de comunicaciones máximas entre la antena y el host, el usuario debe estar ubicado en espacios en la cual no exista interferencia por la que se pueda perder conexión.

Un AP deberá soportar varios usuarios simultáneos, permitiéndole expandir su red con minimización de costos, con simplemente instalar tarjetas inalámbricas en host adicionales. Las impresoras u otros dispositivos periféricos que no puedan

22 DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuración Dinámica de Host)

conectarse en red LAN, se conectan a su red inalámbrica con un adaptador USB inalámbrico.

Si se desea conectar varios host inalámbricos se debería considerar la opción de implementar AP que permita que el usuario pueda desplazarse de un lugar a otro sin perder conexión y sin la necesidad de volver a asignar una dirección IP, esto resulta útil para aquellas empresas grandes en al cual dispone de varias oficinas y estaciones de trabajos.

2.5.1.5 Desventajas de la WLAN

La redes inalámbricas también tienen vulnerabilidades en comparación a las LAN, los cuales se irán mencionando en el transcurso de esta investigación.

Entre algunas desventajas tenemos las siguientes:

La interferencia, se pueden ocasionar por dispositivos Wi-fi que trabajen en la misma frecuencia, también puede ser por redes wireless cercanas o también por otros equipos conectados a la misma red wireless.

En cuanto a velocidad, las redes cableadas alcanzan la velocidad de 100 Mbps, mientras que las redes inalámbricas alcanzan máximo 54 Mbps.

Tienen menor ancho de banda. La redes por cable trabajan a una velocidad de 100 Mbps mientras que la red wireless lo hace a 11 Mbps, existen estándares que logran una velocidad de 25 Mbps y en algunos casos a los 100 Mbps.

Su inversión inicial es mayor, al momento de adquirir equipos de red inalámbrica, ya que el costo de estos equipos es superior a los equipos que utilizan las redes cableadas.

La tecnología que se implementa en la actualidad y que ha adquirido una mayor popularidad es la tecnología Wi-Fi. Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y mayores niveles de seguridad.

Como es la tecnología Li-Fi[23], que está basada en la tecnología VLC[24], la que usa veloces pulsos de luz para transmitir datos, a la que realizaron algunas modificaciones para la transmisión con iluminación LED blanca de mayor intensidad, y además incrementar la velocidad de pulso, logrando con ello velocidades que van desde inicialmente 100 MB/s hasta los 500 MB/s. es posible que, cuando se popularice esta nueva tecnología, se deje de prestar tanto apoyo a la actual.

Una red cableada necesita acceder al medio que transmite la información mientras que en la red inalámbrica el medio es más accesible puesto se transmite por el aire.

El acceso a la red por parte de los intrusos es fácil porque no necesitan estar dentro del edificio o conectado a algún medio físico. Además el sistema de seguridad que ofrece el dispositivo Wi-Fi no es confiable, pero debido a estos problemas se han creado mejores sistemas de seguridad que hace que la red wireless tenga más confiabilidad.

Esta situación hace que no se tenga la entera confianza y la garantía de que el entorno radioeléctrico este libre y limpio para que la red funcione de la mejor manera y ofrezca su alto rendimiento, mientras más interferencia produzcan otros host, menor será el rendimiento de la red, pero el que exista la probabilidad de que se produzca interferencias no significan que se tenga.

2.5.1.6 Riesgos en las Redes Inalámbricas

Las redes inalámbricas sustituyen los cables por ondas de radio, por lo tanto ya no existirán los problemas y limitaciones con los host de conexión, pero también permite una mayor facilidad para que cualquier usuario tenga acceso a la información que se transmite por la red.

---

23 Li-Fi (Light Fidelity - Fidelidad de Luz)

24 VLC (Visible Light Communication - Comunicación de Luz Visible)

Si por la red cableada un atacante no podía tener acceso a un AP para poder realizar alguna acción, con las redes inalámbricas esto se vuelve aun fácil. Al no tener ningún componente físico que proteja los datos, estos quedan totalmente expuestos a los atacantes.

Por tanto, si se desea poder utilizar esta tecnología de forma segura, el modelo a realizar de la red inalámbrica debe aplicar el cifrado de sus datos.

2.5.1.7 Wireless Fidelity Wi-Fi

La tecnología Wi-Fi en la actualidad está invadiendo el mercado y ha tenido una muy buena acogida por la facilidad, agilidad y rapidez que esta tiene. Ahora todos los host móviles, tiene ya este mecanismo de conexión, pero para realizar una conexión, se necesita de un AP que habilite la cobertura y así poder estar conectados.

Estos dispositivos Wi-Fi son aprobados por la Wi-Fi Alliance[25], que es una organización que certifica estos dispositivos para su uso y su estándar IEEE 802.11, así no tendrán ninguna incompatibilidad con los demás dispositivos Wi-Fi que existan en el mundo.

Consiste en realizar estándares para las redes que no deseen cable, para que funcionen en base a protocolos ya establecidos. Aunque fue creado para acceder a las redes inalámbricas, hoy en día es usado frecuentemente para establecer las conexiones a internet y de hecho se ha convertido en el más utilizado.

Esta tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuera compatible entre los distintos host. En busca de esa compatibilidad fue que en 1999 las empresas 3com, Aironet, Intersil, Lucent

Technologies, Nokia y Symbol Technologies se reunieron para crear la WECA[26], actualmente llamada Wi-Fi Alliance.

Al año siguiente de su creación la WECA certificó que todos los host que cuenten con Wi-Fi serían compatibles entre sí, asegurando entonces que se cumple con los criterios estipulados en el protocolo que establece la norma IEEE 802.11. En concreto, a lo que respecta al usuario común, esta tecnología permite establecer conexiones a internet sin ningún tipo de cables y puede encontrarse en cualquier lugar que se haya establecido un Hotspot Wi-Fi[27].

La familia de estándares 802.11 ha ido evolucionando desde su creación, mejorando el rango y velocidad de la transferencia de información, entre otras cosas. La versión original de estándar está obsoleta, pero desde la 802.11a, la original con algunas modificaciones, se encuentran en uso diferentes versiones.

Para contar con este tipo de tecnología es necesario disponer por una parte de un AP, routers, y un dispositivo compatible con la tecnología Wi-Fi, como un host que sea capaz de aquello, o un modem externo que permita el acceso a estas redes.

Es importante mencionar que esta tecnología tienen un rango limitado de alcance, dependiendo de los host involucrados, es mas se puede incluso desplegar un sistema de antenas repetidoras que aumentan el alcance, pero lo importante es graficar que está pensada para el corto alcance o rango.

Aunque el sistema de conexión es sencillo, es común que traiga ciertas dificultades de configuración. Además trae consigo riesgos ya que la información se puede interceptar.

Para evitar este problema se recomienda la encriptación de la información, cuando se visita una página segura, por ejemplo la del banco, se da por sentada

---

26 WECA (Wireless Ethernet Compability Alliance -Alianza de Compatibilidad Ethernet Inalámbrica)

27 Hotspots WI-FI (Punto Caliente Wireless)

la encriptación, pero de todas maneras algunos expertos recomiendan no utilizar este tipo de redes para operaciones que involucren información personal sensible a la seguridad.

2.5.1.8 Seguridad Wi-Fi

Un principal problema en el cual decae la tecnología Wi-Fi en la actualidad es el constante uso del espectro, debido a la masiva cantidad de usuarios, esto afecta las conexiones sobre todo a las de distancias largas.

La conexión Wi-Fi está diseñado para conectar host en distancias cortas, al situarme en una posición alejada, se corre el riesgo de perder comunicación.

La mayoría de las redes wireless son instaladas sin considerar la seguridad, dejando así las puertas abiertas para los intrusos y exponiendo a la vulnerabilidad de proteger la información que se envía por este medio.

2.5.1.9 Políticas de Seguridad Wi-Fi

- **Tipos de vulnerabilidades**

Dado a la gran facilidad que tiene la implementación de una red inalámbrica, se debe considerar las principales vulnerabilidades en la cuales radica, como son:

  - Al momento de configurar los AP y el servidor.
  - Cuando se envía y recibe paquetes por medio de la comunicación inalámbrica.
  - Uso correcto y adecuado de método de encriptación.

- **Seguridad en el estándar IEEE 802.11**

La IEEE 802.11 provee seguridad a través de la encriptación y la autenticación, especifica una capacidad de encriptación opcional llamada WEP[28] lo que hace,

28 WEP (Wired Equivalent Privacy - Privacidad Equivalente Alambrada)

es establecer una seguridad conmensurable a las redes, que es encriptar las transmisiones que van por el aire.

El problema de seguridad que existe con este tipo de encriptación es que no se extiende a la transmisión punto a punto, ya que solo protege la información de datos y paquetes, y no la cabecera de la capa física, lo que permite que otro usuario de la red pueda manejarla y controlar los datos.

El primer estándar que aparece es el 802.11, el cual crea sus principios tecnológicos para los demás estándares. No tuvo relevancia por la baja velocidad binaria alcanzada, cerca de 2 Mbps, y la carencia de mecanismos de seguridad de las comunicaciones.

Después se publica el 802.11b, el cual es acogido con un gran éxito comercial. Opera en la banda de los 2,4 GHz y permite alcanzar velocidades binarias teóricas de 11 Mbps mediante el empleo de mecanismos de modulación de canal y protección frente a errores bastante robustos, aunque en la práctica es difícil superar un ancho de banda efectivo de 7 Mbps. Cuando el canal de transmisión es ruidoso, posee un mecanismo de negociación que reduce la velocidad binaria en escalones predefinidos, aumentando paralelamente la robustez de los mecanismos de protección frente a errores.

Pese a lo anterior, el éxito fue de tal magnitud que aceleró la liberación de nuevos estándares y reclamó una especial atención por entidades de regulación, que empezaron a valorar la ampliación del espectro para este tipo de usos.

El siguiente estándar fue el 802.11a, el cual tiene la particularidad de operar a un mayor rango de bits, hasta 54 Mbps, mediante unos esquemas de codificación de canal más sofisticados y sobre bandas en los 5 GHz. Su empleo no está tan extendido como el 802.11b por el menor rango de cobertura debido a la mayor atenuación de las frecuencias empleadas en algunos casos y la necesidad de mecanismos de control de potencia todavía no incluidos.

El estándar 802.11g, que mejora ostensiblemente en varios frentes: mantiene el rango de los 2,4 Ghz pero amplia el rango de bits hasta los 54 Mbps teóricos, mantiene la compatibilidad con el 802.11b y propone un protocolo de seguridad más robusto denominado WPA.

Los estándares a, b, g, n presentan unos parámetros de operación similares: para el nivel máximo de potencia permitido la cobertura en áreas abiertas en general no supera los 300 metros, mientras que en interiores se obtendrían 100 metros en el mejor de los casos. Es recomendable visibilidad directa entre los host emisor y receptor, sufriendo atenuaciones o incluso pérdida total de señal si hay obstáculos entre estos.

El 802.11i es realmente la formalización del WPA, el cual fue prematuramente lanzado con funcionalidades restringidas debido a la presión de mercado por encontrar una solución al problema de seguridad puesto de relevancia con el antiguo WEP.

Otro estándar importante será el 802.11e, el cual definirá los mecanismos para proporcionar calidades de servicio bajo las WLAN. Esto dará entrada a aplicaciones que permitirán ofrecer servicio de garantía por priorización del tráfico, necesario para usos como VoIP[29], televisión, videoconferencia y, por ende, ampliando el potencial de la tecnología.

También será de gran relevancia el 802.11h que permitirá incluir las nuevas condiciones de utilización que muchos países exigen para el uso de los rangos de frecuencias en torno a los 5 GHz para redes inalámbricas, como son el control automático de la potencia emitida, el análisis continuo del espectro para evitar el empleo de canales ya ocupados y la selección dinámica. Con ello se pretende solventar el problema de posibles interferencias de estas redes con las emisiones de satélite y militares que también las emplean y que son prioritarias.

---

29 VoIP (Voice Over Internet Protocol - Voz sobre Protocolo de Internet o Telefonía IP)

Una de las claves del éxito comercial ha sido la interoperabilidad existente entre host de diferentes fabricantes, labor que ha llevado a cabo la Wi-Fi Alliance. Este organismo, con cerca de 200 empresas entre sus miembros y 800 productos certificados ha fomentado la tecnología y garantizando su genérico buen uso.

Existen multitud de estándares definidos o en proceso de definición que es necesario conocer para una correcta interpretación de las redes wireless:

- 802.11a Estándar de comunicación en la banda de los 5 GHz.
- 802.11b Estándar de comunicación en la banda de los 2.4 GHz.
- 802.11c Estándar que define las características que necesitan los AP para actuar como puentes. Ya está aprobado y se implementa en algunos productos.
- 802.11d Estándar que permite el uso de la comunicación mediante el protocolo 802.11 en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.
- 802.11e Estándar sobre la introducción del QoS[30] en la comunicación actúa como árbitro de la comunicación. Esto permitirá el envío de vídeo y de VoIP.
- 802.11f Estándar que define una práctica recomendada de uso sobre el intercambio de información en el momento del registro a la red y la información que intercambian los AP para permitir la interportabilidad. La adopción de esta práctica permitirá el Roamming entre diferentes redes.
- 802.11g Estándar que permite la comunicación en la banda de los 2.4 Ghz.
- 802.11h Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HiperLAN. Además define el TPC[31] según el cual la potencia de transmisión se

30 QoS (Quality of Service -Calidad de Servicio)

31 TPC (Transmit Power Control - Control Transmisión de potencia).

adecúa a la distancia a la que se encuentra el destinatario de la comunicación.

- 802.11i Estándar que define la encriptación y la autentificación para complementar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del TKIP.
- 802.11j Estándar que permitirá la armonización entre el IEEE, ETSI HiperLAN2, ARIB e HISWANa.
- 802.11m Estándar propuesto para el mantenimiento de las redes inalámbricas.

- **Seguridad en el estándar IEEE 802.11b**

Al igual que su predecesor, trabaja en la banda de los 2.4 GHz y proporciona conectividad en cualquier país.

El estándar 802.11 b llega a una velocidad máxima de 11 Mbps, utiliza un método de modulación DSSS[32] y CCK[33].

Actualmente cuenta con el mayor grado de implementación al llevar varios años disponibles en el mercado, lo que ha permitido una muy notable reducción de los precios de los equipos requeridos para su uso, al querer expandir el estándar 802.11 b, viene a surgir un problema, debido al que el rango de frecuencia de este estándar provoca interferencias entre host , por motivos de incompatibilidad entre otros host que utilizaban otro tipo de frecuencia en la cual su zona de cobertura se encuentre en algún lugar sin espacios abierto, lo cual llevaría usar la red de manera ineficiente.

32 DSSS (Direct-Sequence Spread Sprectrum -Espectro Ensanchado por Secuencia Directa)

33 CCK (Complementary Code Keying - Llave de Código Complementario)

- **Seguridad en el estándar IEEE 802.11i**

El 802.11i se ratificó el 24 de Junio de 2004 para abordar el problema de la seguridad en redes inalámbricas. Se basa en el algoritmo de cifrado TKIP, como el WEP, pero también admite el AES[34].

WiFi Alliance creó una nueva certificación, denominada WPA2, para host que admiten el estándar 802.11i.

A diferencia del WPA, el WPA2 puede asegurar, tanto redes inalámbricas en modo infraestructura como también redes en modo "ad hoc"[35].

2.5.1.10 Amenazas Wi-Fi

Al operar un WLAN de la misma manera que una LAN, alberga la misma vulnerabilidad añadiéndole, algunas especificaciones más.

En esta parte se detalla algunos temas de amenazas en cuanto a redes inalámbricas, y entre ellas tenemos:

- **Escuchas ilegales**

En ocasiones pueden existir usuarios no autorizados, que escuchen de manera ilegal todas las señales que se transmiten entre los host inalámbricos, poniendo en riesgo la confidencialidad de la información, esto se debe que no se dan cuenta de que alguien los está afectando por una intrusión. Este es un ataque pasivo.

La dificultad para los que realizan escuchas ilegales radica principalmente en la decodificación de la señal digital y vencer el cifrado.

---

34 AES (Advance Encript Standar - Estándar de cifrado avanzado)

35 AD HOC (Red inalámbrica descentralizada)

- **Acceso no autorizado**

Intentan ingresar a la red enmascarándose como un usuario autorizado, una vez que ha ingresado este usuario puede violar la confidencialidad y alterar el flujo de datos y el tráfico de la red. Este tipo de ataques activos lo puede llevar a cabo con un adaptador inalámbrico que sea compatible con la red a la cual está atacando.

La mejor forma de proteger el acceso no autorizado es desplegar un mecanismo de autenticación para así asegurar que solo los usuarios autorizados puedan acceder a la red.

Otra de las formas de atacar a una red es implementado un falso AP e interceptar la red a la cual quiere introducirse y generar una señal más fuerte y así capturar los ingresos de los usuarios con sus claves para después ser utilizados.

La primera forma de ataque es complicada ya que para hacer ese tipo de ataques se debe conocer la estructura de la red y tener información detallada por lo cual podría ser logrado por alguien que sea un colaborador de la empresa.

En cuanto al segundo ataque es sencillo ya que lo único que tendría que hacer es implantar un receptor y una antena.

- **Interferencias**

Esta amenaza afecta a la seguridad y al traspaso de los datos. La mayoría de las veces estas interferencias son accidentales porque, al operar en radio frecuencia, otros host también pueden tomar la banda de los 2.4 GHz y saturar la red por completo.

Además de esto la interferencia también puede ser intencional, la cual podría ser causada por un usuario con un transmisor poderoso, generando una señal demasiado fuerte para debilitar a las débiles y así romper las comunicaciones, a

esto se lo conoce como JAMMING[36] y lo que hace es cubrir una frecuencia entera usada por la señal en uso pero de baja frecuencia y para después ser usada parte de la frecuencia por la seña en uso

Estos equipos pueden ser adquiridos a un consumidor o a su vez pueden ser creados por usuarios con conocimiento.

- **Amenazas físicas**

Las redes inalámbricas al ser un medio no guiado, también puede sufrir daños, al igual que una red cableada, las redes inalámbricas también tiene una infraestructura con componentes físicos, ya sea AP, routers, antenas y software.

Un daño en cualquiera de estos componentes afectaría en varias partes de la red como la intensidad de la señal, el límite del área cubierta o hasta reducir la velocidad del internet, lo que haría que los usuarios no puedan trabajar.

Este tipo de infraestructura son susceptibles a las condiciones del medio ambiente sobre todo en exteriores, ya sea por la lluvia, calor o por fenómenos naturales, lo que causaría el daño de los host.

Puede también estar sujeto a ataques por usuarios cerca a los componentes, lo que significa que podría haber sabotaje, robo de los host, o en el peor de los casos podría dañar o destruir los host causando que se rompa el funcionamiento de todos host conectados a la red.

2.5.1.11 Ataques en Redes Inalámbricas

Un ataque a WLAN tiene dos etapas, un ataque pasivo donde se obtiene información sobre la red y un ataque activo con el cual se consigue tener acceso a la red.

36 JAMMING (interferir con las comunicaciones o la vigilancia)

- **Ataques pasivos**

Los ataques pasivos más relevantes son:

Listens o Escuchas

Se produce cuando un atacante monitorea el contenido de los mensajes, utilizando un dispositivo inalámbrico y un software apropiado denominado Sniffer, para un posterior análisis del tráfico.

Estos usuarios amenazan la seguridad de los datos y su confidencialidad, por el hecho de que interfiere en las ondas de radio que emite el dispositivo, debido a que estos no siempre tienen un rango de ondas definido sino que muchas de las veces superan el límite e incluso atraviesan elementos físicos, permitiendo que cualquier persona pueda interferir en el acceso a la red.

Sniffers o Análisis de tráfico

Permite a un atacante obtener información que se transmite sin protección como passwords de sitios Web, correo, sesiones FTP[37] y Telnet[38]. De esta manera es posible acceder a los servidores y comprometer el sistema.

Es una técnica para obtener información de la comunicación, que consiste en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre los host monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre los host de la comunicación, para extraer información acerca de los períodos de actividad.

---

37 FTP (File Transfer Protocol - Protocolo de transferencia de archivos)

38 Telnet (protocolo estándar de Internet para conexión desde un terminal remoto)

- Los ataques pasivos son difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

- **Ataques activos**

Estas amenazas implican algún tipo de modificación en el proceso de transmisión de información a través de la red o la creación de un falso del mismo.

Generan acciones evidentes en la red, por lo que facilitan su detección pero son difíciles de prevenir. Existen cinco tipos de estos y son:

1. Costumers o Disfraz

Ocurre cuando un atacante accede a todos los recursos de la red inalámbrica haciéndose pasar por un usuario autorizado.

El intruso se hace pasar por usuario diferente, normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a un usuario no autorizado acceder a una serie de recursos privilegiados suplantando al usuario que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

2. Repeater o Repetición

El atacante se encuentra en un punto medio entre el emisor y el receptor para poder captar la información, almacenarla y luego volver a transmitirla a su destino original, sin que esta sufra alteraciones. Este es un proceso transparente para los usuarios en los extremos de la comunicación.

Es decir, uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.

3. Fraudulent message o Modificación del mensaje

Es un proceso similar al anterior en el cual el atacante retransmite el mensaje, pero esta vez alterando su contenido.

Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.

4. Men in the middle o Ataque del hombre en el medio

Un atacante emplea un AP de mayor potencia que los existentes en la red, para conseguir que usuarios de ésta, se conecten a él y envíen sus datos.

Este ataque sucede cuando algún usuario malicioso se pone en la mitad del camino entre nuestra host y los servicios de internet que utilizamos, pudiendo esta leer toda la información que recibimos, enviamos e incluso modificarla.

Es uno de los poderosos ataques informáticos de los que podemos llegar a ser víctimas.

Uno de los métodos comunes ocurre cuando usuarios con acceso físico a la misma red a la que nos conectamos, ejecuta una herramienta que primeramente envía información a las tablas ARP[39] del host, estas tablas son las que relacionan la dirección de internet de los equipos con su identidad de hardware.

Ocasionando con esto que el host del usuario asuma que el host del atacante es el equipo que da acceso a internet, una vez que la ruta de tráfico desde y hacia internet tiene como punto intermedio el host del atacante.

Esta herramienta comienza a mostrar en una ventana con un navegador de internet modificado las páginas Web que estamos visitando, además de esto

39 ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones)

ofrece la posibilidad al atacante de modificar las respuestas antes que estas lleguen al host del usuario.

5. Denial of service o Denegación de servicio

Es importante tener en cuenta la seguridad informática, antes de conectarse a internet, ya que cada día crecen las variantes de ataques informáticos que tienen como objetivo tomar el control del host o, simplemente, robar información personal que puede ser utilizada para fines delictivos.

El DoS, es un ataque que se realiza a una red del host que provoca que los usuarios no puedan acceder a un servicio, por lo general esto ocasiona perdida en las conexiones de la red por que el host atacado consume demasiado ancho de banda o sobrecarga los recursos de la red.

Esto se produce cuando una señal de radio frecuencia de potencia considerable, sea intencional o no, interfiere en un sistema inalámbrico dificultando su funcionamiento o inhabilitándolo por completo. Para la detección de fuentes de interferencia, puede valerse de equipos analizadores de espectro.

La denegación de servicio, sobrecarga el equipo informático hasta hacerlo colapsar. Para lograrlo, el atacante envía un flujo de información que sobrepasa la capacidad de procesamiento del equipo, para que no pueda seguir ofreciendo el recurso a los usuarios del sistema. De esta manera, logra que el host (servidor), no pueda seguir dando el servicio, de allí se deriva el nombre de denegación de servicio.

Tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

Por lo general, este tipo de ataques está dirigido a los servidores de una compañía, para que no puedan utilizarse ni consultarse.

La denegación de servicio es una complicación que puede afectar a cualquier servidor de la compañía o usuario conectado a internet.

Su objetivo no reside en recuperar ni alterar datos, sino en dañar la reputación de las compañías con presencia en internet y potencialmente impedir el desarrollo normal de sus actividades en caso de que éstas se basen en un sistema informático.

Esta herramienta también puede ser utilizada de buen modo para comprobar la capacidad de tráfico a la que un computador puede estar soportado sin que se vuelva inestable, afectando a los servicios que provee.

2.5.1.12 Mecanismos de Seguridad Wi-Fi

- **Seguridad Lógica**

Para el buen uso de las redes inalámbricas y para la seguridad de la misma, se debe tomar en cuenta varios aspectos, en los cuales se tiene:

WEP

Es cierto que las redes inalámbricas pueden soportar un espionaje mínimo, se debe estar preparados para algo más grande y prevenirlo de terceros, para ello hay que utilizar la encriptación que proporciona un nivel de seguridad que es parecido al de las LAN cableada pero para la encriptación de las ondas de radio.

Aunque los sistemas WLAN pueden resistir a intrusos ilegales pasivos, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio.

Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN. Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación.

Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

WPA

WPA, es un mecanismo de control de acceso a una red inalámbrica, que fue diseñado con la simple idea de eliminar todas las falencias del WEP.

Este tipo de cifrado utiliza TKIP para gestionar claves dinámicas que mejoran notablemente el cifrado de datos, incluyendo el vector de inicialización, es decir, WPA funciona parecidamente a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4[40] para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

WPA acepta diferentes sistemas de control de acceso que incluye la validación de un usuario y una contraseña, certificado digital u otro sistema o simplemente que utilice una contraseña compartida para identificarse.

Emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP.

WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar

40 RC4 (algoritmo de cifrado de flujo)

caracteres especiales, números, mayúsculas, minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones, que utilizan distintos procesos de autenticación:

- **Para el uso personal doméstico.-** TKIP es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para la red.
- **Para el uso empresarial de negocios.-** El Protocolo de autenticación extensible EAP se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS , esto aporta una seguridad de fuerza industrial para la red.

TKIP.- es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas. WPA es utilizado en redes Wi-Fi para corregir deficiencias en el antiguo estándar de seguridad WEP.

Fue diseñado para reemplazar el WEP sin cambiar el hardware. Esto es necesario, porque la seguridad del WEP fue descifrada, dejando a las redes Wi-Fi sin una buena seguridad en su capa de enlace y la solución a este problema no podía esperar a que se cambie todo el hardware fabricado.

La principal diferencia entre WEP y TKIP, es que WEP utiliza periódicamente la misma clave para cifrar los datos; en cambio TKIP comienza con una clave temporal de 128 bits que comparte entre los host. TKIP combina la clave temporal con la dirección MAC[41] del host. Luego añade un valor de inicialización relativamente largo para producir la clave final con la cual se cifrarán los datos. Tanto WEP como TKIP utilizan el RC4 para hacer el cifrado.

41 MAC (Media Access Control - Control de Acceso al Medio)

Se considera una solución temporal, pues la mayoría de los expertos creen necesaria una mejora en el cifrado.

EAP[42**].-** Es una extensión del PPP[43] que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias.

Se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado. EAP proporciona una arquitectura estándar para aceptar métodos de autenticación adicionales junto con PPP.

Mediante EAP, se pueden admitir esquemas de autenticación adicionales, conocidos como tipos EAP. Entre estos esquemas se incluyen las tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados.

Junto con los tipos de EAP seguros, es un componente tecnológico crítico para las conexiones de red privada virtual VPN seguras, como los basados en certificados, ofrecen mayor seguridad frente a ataques físicos, y de investigación de contraseñas, que otros métodos de autenticación basados en lo mismo.

Es una estructura de soporte framework frecuentemente usada en redes inalámbricas y conexiones PPP. Es definida en el RFC3748[44], aunque el protocolo EAP no está limitado a WLAN y puede ser usado para autenticación en LAN, es frecuentemente usado en WLAN.

Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

---

42 EAP (Extensible Authentication Protocol - Protocolo de Autenticación Extensible)

43 PPP (Point to Point Protocol- Protocolo Punto a Punto)

44 RFC3748 (autenticación que admite múltiples métodos)

Es una estructura de soporte, no un mecanismo específico de autenticación. Provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos EAP, de los cuales se conocen actualmente 40.

Cuando EAP es invocada por un dispositivo NAS[45] capacitado para 802.1X, como por ejemplo un AP 802.11 a/b/g, los métodos modernos de EAP proveen un mecanismo seguro de autenticación y negocian un PMK[46] entre el dispositivo cliente y el NAS.

En esas circunstancias, la PMK puede ser usada para abrir una sesión inalámbrica que usa encriptación TKIP o AES.

WPA2

Nace a partir de su antecesor, que fue WPA, conlleva casi las mismas funciones que provee la WPA, actualmente se incluyen en los dispositivos modernos y es compatible con productos anteriores que tenían WPA.

La diferencia entre estos 2 es que la WPA2 necesita el cifrado AES, en cuanto al WPA emplea TKIP. AES emplea estándares máximo de seguridad utilizadas en entidades del gobierno.

Es de nuevo, una certificación, pero no obliga al dispositivo al uso de ninguna de tecnologías de cifrado específica. Un dispositivo certificado WPA2 puede utilizar tanto el algoritmo de cifrado AES, como RC4. Cuando un dispositivo que soporta WPA2 usa el algoritmo de cifrado AES.

45 NAS (Network Access Server - Servidor de Acceso a la Red).

46 PMK (Pairwise Master Key - Clave Principal de la jerarquía de pares de claves)

Lo hace dentro del protocolo CCMP[47] que es más seguro que TKIP. En la mayoría de dispositivos la denominación es utilizada erróneamente, y se habla de TKIP o AES, cuando en realidad se debería decir TKIP o CCMP.

La confusión procede que el protocolo CCMP utiliza el algoritmo de cifrado AES.

- **Vulnerabilidades de WEP**

La confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre host no sea revelada a personas no autorizadas.

La confidencialidad debe asegurar que ya sea la comunicación entre un grupo de AP en un sistema de distribución inalámbrico WDS, se conserva protegida contra intercepciones. Ha sido asociada tradicionalmente con el término WEP, fue parte del estándar IEEE 802.11 original, de 1999.

La función principal del WEP es brindar a la red inalámbrica, seguridades comparables con las de la red cableada, por el hecho de que una red inalámbrica usa ondas de radio y son más propensas a ser interferidas.

WEP no duro mucho, ya que fue vulnerada su seguridad al poco tiempo de ser publicado.

Uno de las vulnerabilidades de WEP fue la falta de un sistema de manejo de claves que formara parte del protocolo.

El sistema de distribución de claves fue tan simple como teclear manualmente la misma claves en cada host, Fue seguido por varias extensiones de carácter propietario que resultaron también inadecuadas.

47 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Modo de Cifrado de Encadenamiento de Bloques de Codigo de Autenticacion de Protocolo de Mensajes)

- **Reemplazo de WEP**

Luego del deceso del WEP, en 2003 se propone el WPA, luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 en 2004.

WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de claves. Si no se usa un servidor de claves, todas los host de la red usan una PSK. El modo PSK se conoce como WPA o WPA2-Personal.

- **Diferencias entre encriptación WEP, WPA Y WPA2**

Saltarse la protección WEP de un router es cuestión de minutos para un usuario que use el software adecuado: como por ejemplo el packet sniffers y WEP Crackers.

Para llevar a cabo este ataque basta con capturar una cantidad de paquetes necesaria se trata de “romper” el cifrado de la red.

Un WEP cracker es un programa basado en estadísticas que procesa los paquetes capturados para descifrar la clave WEP.

Existen usuario que por desconocimiento o comodidad no cambian la seguridad de las redes de sus casas o pequeños negocios.

Encriptación WEP.- Nace en 1999 como un protocolo para redes wireless que permite la encriptación de la información que se transmite en una red WiFi. Su cifrado está basado en el algoritmo RC4, pudiendo utilizar claves de 64 bits o de 128 bits.

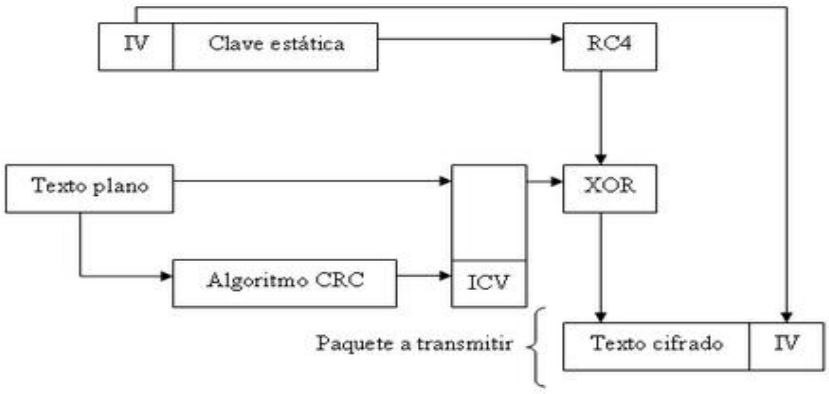

Figura 2.2: Encriptación WEP[48]

Fuente: http://www.formatoweb.com.ar/blog/2007/11/24/el-sistema-de-cifrado-wep/

Por motivos de seguridad, la Alianza Wi-Fi anunció en 2003 que WEP había sido reemplazado por WPA, en 2004 cuando se ratificó el estándar completo 802.11i llamándolo WPA2. A pesar de que su nivel de seguridad se limita a disuadir el uso sin autorización de una red, WEP sigue siendo utilizado, ya que suele ser la primera opción de seguridad que aparece en la configuración de los routers Wi-Fi.

Encriptación WPA.- Es un sistema para proteger las redes inalámbricas creado para corregir las deficiencias del sistema WEP, implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

Posteriormente surgió el WPA2, por otro lado lo mismo, WPA fue definido por la Wi-Fi Alliance y WPA2 es el estándar aprobado por la IEEE.

Adopta la autentificación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Este servidor suele ser del tipo RADIUS[49], orientado principalmente a un uso empresarial.

Para no obligar al uso de un servidor en entornos domésticos, WPA permite la autentificación mediante PSK[50], que requiere introducir la misma clave en todos los host de la red.

La información en WAP también es cifrada utilizando el algoritmo RC4, pero con una clave de 128 bits y un vector de inicialización de 48 bits en lugar de los 104 bits de clave y 24 bits del vector de inicialización usados en WEP.

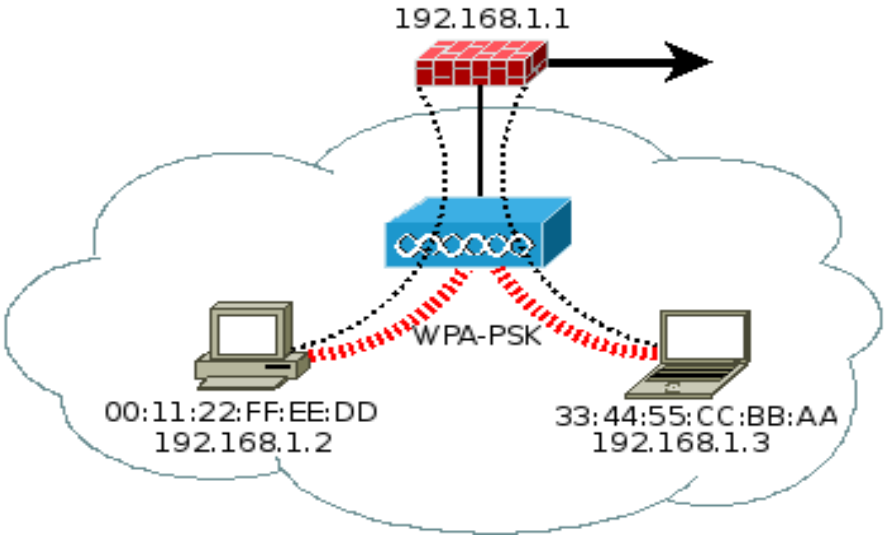

Figura 2.3: Encriptación WPA[51]

Fuente:http://www.ecualug.org/2007/aug/27/comos/implementaci_n_de_una_red_inal_mbrica_segura_usando_gnu_linux_y_wpa

- **Encriptación**

La WEP usa claves secretas que se comparten entre los host, lo que permite que todos los datos enviados y recibidos estén encriptados.

50 PSK (Pre-Shared Key - clave compartida inicial)

La que más se suele usar es la de 128 bits, que ofrece un buen nivel de protección sin ser excesivamente larga y complicada, la encriptación WEP de 256 bits no es soportada por diferentes host.

Una clave de encriptación WEP se puede descifrar, pero para esto es necesario un tráfico ininterrumpido de datos durante un tiempo determinado, evidentemente, cuanto mayor sea el nivel de encriptación y complicada sea la clave es difícil de descifrar.

La mayoría de los programas para descifrar claves están basados en una serie de secuencias lógicas con las que empieza a atacar a la red hasta entrar.

Evitar claves que contengan secuencias relacionadas con fechas, nombres, lugares, así como frases típicas, ya que es lo primero que intentan este tipo de programas. Esto no solo es válido para una clave WEP, sino para cualquier tipo de clave que se utilice. También se debe evitar claves fáciles, como secuencias consecutivas de teclas o números.

Para mayor seguridad se aconseja siempre que sea posible activar el filtrado de direcciones MAC, es un identificador hexadecimal de 48 bits. Esta dirección es única para cada dispositivo, no siendo un parámetro modificable por el usuario, cada tarjeta o interfaz de red tiene su propia dirección MAC, establecida por el fabricante.

- **Autenticación**

Existen dos métodos de autenticación con WEP: la autenticación de sistema abierto y la autenticación de clave compartida, en el caso de la autenticación de sistema abierto, el cliente WLAN no tiene que dar sus datos al AP durante el proceso de autenticación.

Entonces, cualquier usuario, puede autenticarse con el AP y, a continuación, intentar asociarse, realmente, no se realiza ninguna autenticación. Una vez que

se haya autenticado y asociado, se puede utilizar WEP para encriptar los paquetes de datos.

- **Seguridad Física**

Las precauciones se las debe clasificar por el tipo de riesgo al cual estén expuestos ya que todas estas llevarían a detener el funcionamiento de la red inalámbrica.

Si no se dispone de las herramientas adecuadas para proteger los host, se debe tratar en lo posible de minimizar el riesgo de que sufran algún daño, como cubrir los host con una capa blindada para prevenir los golpes de los relámpagos o recubrir el cableado para que en caso de una fuga de liquido, los host no sufran cortocircuitos.

Además se debería negar el acceso al personal no autorizado, colocando los host en áreas seguras y alejadas del tráfico de las personas y asegurando con controles de acceso.

Servidores de autenticación.- En la IEEE 802.11 se habla de estos servidores pero en una forma general, técnicamente un servidor de autenticación trata sobre elementos diseñados según el criterio del marco AAA[52].

Estos elementos hacen referencia a la autenticación de usuarios, a las peticiones de autorización y los movimientos contables del sistema, los servidores deben ser capaces de recibir peticiones y obtener la respuesta a la petición pasando primeramente por una examinación, determinación de las autorizaciones, recuperación de las políticas que necesite y una evaluación de la petición, en caso de no encontrar respuesta el servidor procede al reenvío de la petición hacia otro servidor para realizar el mismo proceso.

52 AAA (Authentication, Authorization and Accounting - Autenticación, Autorización y Contabilidad)

Un servidor de autenticación es un host que controla quién puede acceder a una red informática. Los objetivos son la autorización de autenticación, la privacidad y no repudio.

La autorización determina qué datos de un usuario puede tener acceso a la red, si los hubiere.

Privacidad mantiene la información se divulgue a personas no autorizadas.

No repudio es un requisito legal y se refiere al hecho de que el servidor de autenticación puede registrar todos los accesos a la red junto con los datos de identificación, de manera que un usuario no puede repudiar o negar el hecho de que él ha tenido o modificado el datos en cuestión.

Los servidores de autenticación vienen en formas diferentes. El software de control de la autenticación puede residir en un servidor de acceso a la red, un router u otro tipo de hardware para controlar el acceso a la red, o algún otro AP de la red.

Independientemente del tipo de máquina que aloja el software de autenticación, el término servidor de autenticación sigue siendo generalmente utilizado para referirse a la combinación de hardware y software que cumple la función de autenticación.

Además de las variaciones en el hardware, hay un número de diferentes tipos de algoritmos lógicos que pueden ser utilizados por un servidor de autenticación. El más simple de estos algoritmos de autenticación es generalmente considerado como el uso de contraseñas.

En una aplicación sencilla, el servidor de autenticación sólo puede almacenar una lista de nombres de usuario válido y la contraseña correspondiente, y autenticar todos los usuarios que intentan conectarse a la red de acuerdo a esta lista.

Kerberos es otro tipo de protocolo de autenticación utilizado en muchos sistemas de Windows Server ® de autenticación, y en algunos de seguridad en línea o

sistemas de seguridad de internet. Hay tres aspectos principales para la autenticación Kerberos: la autenticación de la identidad del usuario, el envasado seguro del nombre del usuario, y la transmisión segura de las credenciales del usuario en la red.

Servidores de autenticación Kerberos en los sistemas operativos Windows® están disponibles para Windows XP®, Windows 2000®, Windows 2003® y sistemas operativos.

Un servidor proxy es un servidor que intercepta las peticiones y de una red interna y una red externa, como el internet. Los servidores proxy actúan como servidores de autenticación, además de un número de otras funciones que pueden cumplir.

Hay opciones diferentes que pueden ser utilizados para implementar los servidores de autenticación, incluyendo hardware, sistema operativo, y los requisitos de paquete de software.

Como tal, suele ser importante para una organización a analizar a fondo los requisitos de seguridad antes de implementar un servidor de autenticación en el entorno de red.

Fases de gestión de usuario.- Una vez que se haya analizado todos los elementos que formaran parte de la arquitectura, se ilustrara el diseño de la arquitectura de control de acceso.

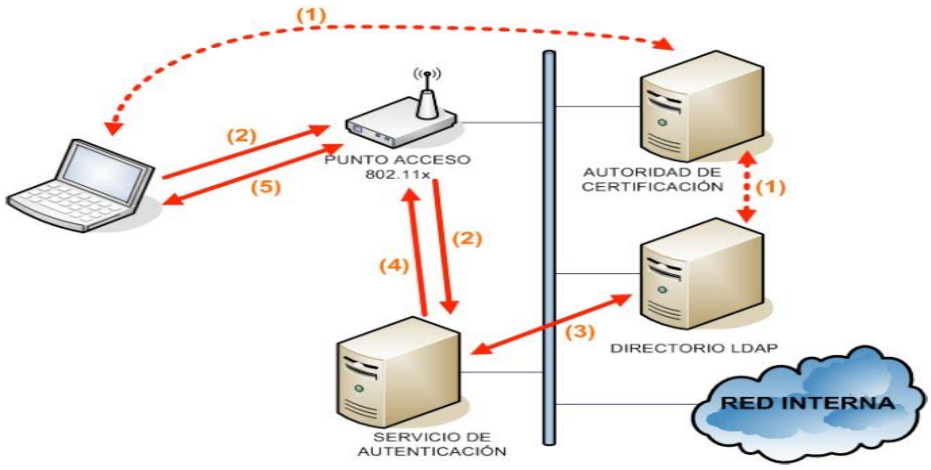

Figura 2.4: Fases Gestión De Usuario[53]

Fuente: http://conocimientoswirelessnetworkdesign.blogspot.com/2010/05/diseno-de-arquitectura-segura-para.html

Como se muestra en la Figura 2.4 un entorno de la arquitectura. En ella se puede ver un AP y un servidor de autenticación conectados mediante un sistema de distribución, también un cliente que cuando intenta ingresar por primera vez a la red inicia el proceso de conexión, es decir, la autenticación, autorización y distribución de la clave de cifrado WEP.

Una vez que se haya conectado el host, el sistema estará periódicamente realizando un proceso de renegociación de la clave WEP.

Fase de autenticación.- Esta es la primera fase y funciona siguiendo el estándar IEEE 802.11, cuando el cliente quiere ingresar a la red por medio de un AP, este le pedirá su identificación y el cliente debe proporcionársela.

Después de esto se realiza el proceso de establecimiento de conexión, en donde el cliente y el servidor de autenticación se autentican mutuamente mediante certificados y negocian los parámetros de configuración necesarios para establecer una ruta de comunicación segura.

Una vez terminada la negociación se establece un canal entre el cliente y el servidor que utilizara para derivar la clave WEP.

Fase de autorización.- En esta segunda fase el cliente indica al servidor cual es el tipo de conexión que desea utilizar en cuanto al ancho de banda y cuál es el tiempo que va a estar conectado, junto con los certificados, que demuestran el usuario está autorizado a utilizar la red que ha solicitado.

Después de esto el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del usuario es el necesario, en caso de haber algún problema, el servidor desautoriza al usuario inmediatamente a acceder a la red.

De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que solo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

Los parámetros del cliente se mandan en una estructura firmada, esto sirve para que el servidor confirme que nadie ha modificado estos parámetros, además, toda la información que hace referencia a la autorización del usuario se manda a través del canal establecido anteriormente, de tal forma que solo se pueden haber enviado por el usuario que inicio la conexión.

Fase de distribución de clave.- En esta tercera fase solo participan el servidor y el AP y consiste en que el servidor le pase al AP un descriptor de la clave WEP que debe utilizar con el usuario, así como el tipo de servicio que el usuario espera que se le ofrezca.

Por otra parte, el AP debe comprobar que en ese momento pueda soportar las necesidades del nuevo usuario, es decir, debe comprobar que lo que el nuevo usuario solicite no sobrepase la capacidad del ancho de banda que actualmente estén usando los demás usuarios y que esté disponible el tiempo que el usuario necesite, informando al servidor sobre la decisión que tome.

Culminado estas 3 fases, el proceso de conexión habrá terminado, y si todo está correctamente establecido, el servidor notificará al AP la autorización de su parte para que el usuario pueda utilizar la red, el AP traslada al usuario esta decisión para que inicie la comunicación, y el usuario puede hacer uso de la red, con la garantía de que sus mensajes serán protegidos por encriptación y serán solo descifrables para el AP.

Fase de renegociación.- Dependiendo del nivel de seguridad que el usuario desee, es posible renegociar la clave WEP que se está utilizando para cifrar la comunicación entre los host.

Para esto el cliente debe iniciar un proceso de renegociación de conexión, no será necesario que el usuario mande sus parámetros, a menos que desee cambiarlos, sino que simplemente se realiza esta fase para indicar al usuario cual es la nueva cadena para generar la clave WEP.

De modo que al terminar el nuevo proceso de conexión, el usuario y el AP tendrán la nueva clave WEP, que podrán utilizar para cifrar sus comunicaciones.

Fase de movilidad.- Esta fase está fundamentada y complementada con la anterior, ya que cuando un usuario se ubica en el área de cobertura de un nuevo AP, en lugar de iniciar el proceso de conexión descrito en el principio, simplemente inicia un proceso de renegociación de conexión.

Al tener los mismos parámetros de la conexión anterior, se puede realizar de manera sencilla y además evita que el servidor tenga que validar nuevamente al usuario.

- **Mecanismos de Autentificación**

Osa[54]

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. No realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

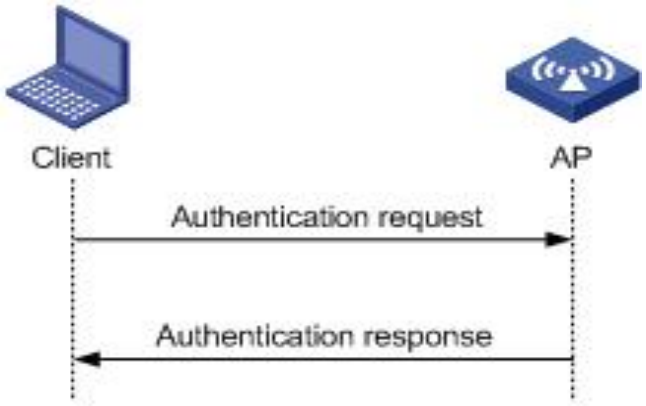

Figura 2.5: Esquema de OSA[55]

Fuente:http://www.h3c.com/portal/ProductsSolutions/Technology/WLAN/Technology_Introduction/200812/624019_57_0.htm

ACL

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

54 OSA (Open System Authentication - Autenticación de Sistema Abierto)

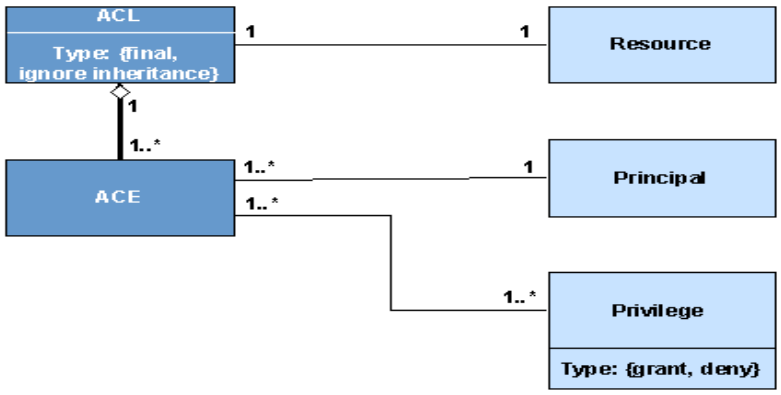

Figura 2.6: Esquema de ACL[56]

Fuente:http://help.sap.com/saphelp_nw04/helpdata/en/21/53882f3fee0243b6c774e26ebed880/content.htm

ACL Estándar .- El objetivo de las ACL estándar es filtrar el trafico de la red en base a las direcciones de los paquetes que entran y salen, en la que se instale la ACL, lo que implica un nivel básico de filtrado.

Lo primordial de las ACL estándar es que la dirección de origen coincida con la dirección de referencia, entonces cada vez que llegue un paquete se compararán las direcciones IP de cada una de las reglas de la lista de acceso, si alguna cumple entonces se dará acceso o se la negara y no se comparar con ninguna otra regla.

ACL Extendida.- La ACL extendida permite especificar hacia donde se dirige el tráfico y de esta manera puedo bloquear o permitir un tráfico mas especifico, ya sea el que proviene del host pero se dirige a una red en particular o solo el de una red que se dirige a otra red en particular, esto se logra con el simple hecho de permitir comparar las direcciones de destino de los paquetes, entonces con esto solo se permite un host, el resto de la red se bloquea y otras redes se va a permitir.

CAPÍTULO 3

3 ANÁLISIS DEL DISEÑO DE LINEAMIENTOS PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD A LOS USUARIOS Y GESTIÓN

3.1 ANÁLISIS

3.1.1 ESTADO SITUACIÓN INICIAL[57]

Actualmente se tiene trece antenas para conexión inalámbrica las cuales fueron puestas con otro propósito que era el de conectar las PDA's para cuando descarguen los contenedores de los productos de PRONACA, como el proyecto se pospuso de decidió optar por utilizar estas antenas para la conexión de los usuarios del centro de operaciones.

Por lo cual se reutiliza la infraestructura ya instalada y se aprovecha la misma, las características de estas antenas son direcciones por ende pueden existir usuarios que no se conecten una vez salido del área de cobertura donde este apuntando la antena.

La empresa, cuenta en su mayor parte con infraestructura de equipos CISCO que son considerados, mundialmente, entre los mejores para comunicaciones en la red, entre los que se utilizan tenemos:

57 Fuente: DBA Networking Ing. Omar González .

CISCO Wirelles LAN Controller 4402 AIR-WLC4402-25-K9

Descripción del producto	Cisco Wireless LAN Controller 4402 - dispositivo de gestión de la red
Tipo de dispositivo	Dispositivo de gestión de la red
Tipo incluido	Montable en bastidor - 1U
Dimensiones (Ancho x Profundidad x Altura)	44.3 cm x 40 cm x 4.5 cm
Cantidad de puertos	2
Protocolo de interconexión de datos	Gigabit Ethernet
Red / Protocolo de transporte	TCP/IP, UDP/IP, ICMP/IP, IPSec
Protocolo de gestión remota	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH
Capacidad	Puntos de acceso gestionables : 25
Características	Soporte de DHCP, soporte BOOTP, soporte ARP, soporte VLAN, soporte para Syslog, Quality of Service (QoS)

Figura 3.1: CISCO Wirelles LAN Controller AIR-WLC4402-25-K9[58]

Fuente: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0_ps6366_Products_Data_Sheet.html

CISCO Router 2801

Tipo de Producto	Router de servicios integrados
Part Number Fabricante	CISCO2801-V/K9
Fabricante	Cisco Systems, Inc
Modelo de Producto	Router de servicios integrados 2801 con bundle de voz
Gama de Producto	2800
Interfaces/Puertos	2 x 10/100Base-TX LAN
Detalles de Interfaces/Puertos	2 x RJ-45 10/100Base-TX LAN 1 x RJ-45 Consola Gestión 1 x RJ-45 Auxiliar Gestion 1 x USB 1.1

Ratio de Transferencia de Datos	10Mbps Ethernet 100Mbps Fast Ethernet 115,2Kbps Consola 115,2Kbps Auxiliar
Tipo de Conexión	Par Trenzado 10/100Base-TX
Ranuras Expansión	8 x Ranura de expansion
Módulos	1 x PVDM2-8 modulo DSP voz/fax
Detalles de la Ranura	2 x AIM Interno 2 x PVDM Interno 4 x Ranura de expansion Interno
Protocolos	TCP/IP SNMP v3 SSH v2 SRTP VoIP H.323 MGCP VoFR ATM VoATM
Memoria	256MB DRAM Instalado 384MB DRAM Max. 64MB Flash Instalado 128MB Flash Max.
Voltaje de Entrada	100 V AC a 240 V AC Auto Rango
Dimensiones	4,37cm Altura x 44,45cm Anchura x 41,91cm Profundidad
Peso	6,21 kg Max.
Formato	1U 19" Montable en rack Sobremesa

Figura 3.2: Router de Servicios Integrados CISCO 2801[59**]**

Fuente: http://www.cisco.com/en/US/products/ps6018/index.html

CISCO Acces Point AIR-LAP1242G-A-K9

Access Point autónomo
Diseñado para entornos menos decorativos como fábricas, almacenes o áreas de comercio minorista
Hasta 108 Mbps de capacidad
Conectores para antenas externas
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

Figura 3.3: Acces Point AIR-LAP1242G-A-K9[60]

Fuente:http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd80635208.html

CISCO Switch POE WS-C2960-24PC-L

Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.
Función Power over Ethernet que le permite implementar fácilmente nuevas funciones como comunicaciones por voz e inalámbricas sin necesidad de realizar nuevas conexiones.
Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de 1000 megabits por segundo), en función del precio y sus necesidades de rendimiento.
Varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
Capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
Seguridad integrada
Funciones de supervisión de red y solución de problemas de conectividad mejoradas.
Actualizaciones de software sin gastos adicionales.
Garantía limitada de hardware por vida

Figura 3.4: Switch POE CISCO WS-C2960-24PC-L[61]

Fuente:http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_at_a_glance0900aecd8047794c.pdf

3com Switch no Administrable baseline

Transmisión de datos	0.1 Gbit/s, 10/100 Mbit/s.
Red	IEEE 802.1d, IEEE 802.3, IEEE 802.3u, IEEE 802.3x, ISO 8802-3.
Características de manejo	No administrado, L2.
Conectividad	10BASE-T/100BASE-TX.
Peso y dimensiones	1U, 440 x 173 x 44 mm, 1500 g.
Control de energía	10 W, 100-240 VAC, 50/60 Hz.
Aprobaciones reguladoras	FCC, CE, UL 60950-1, CSA 22.2 60950, EN 60950, IEC 60950, EN 55022 Class A, FCC Part 15 Subpart.
Condiciones ambientales	32 - 104 °F, 0 - 40 °C.
Iluminación/Alarmas	Link, Act.

Figura 3.5: Switch no Administrable 3com baseline[62**]**

Fuente:http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&taskId=120&prodSeriesId=4237308&prodTypeId=12883&objectID=c02631865

Todos estos host conforman la infraestructura de la red wireless que la empresa tiene, la cual está estructurada de la siguiente manera:

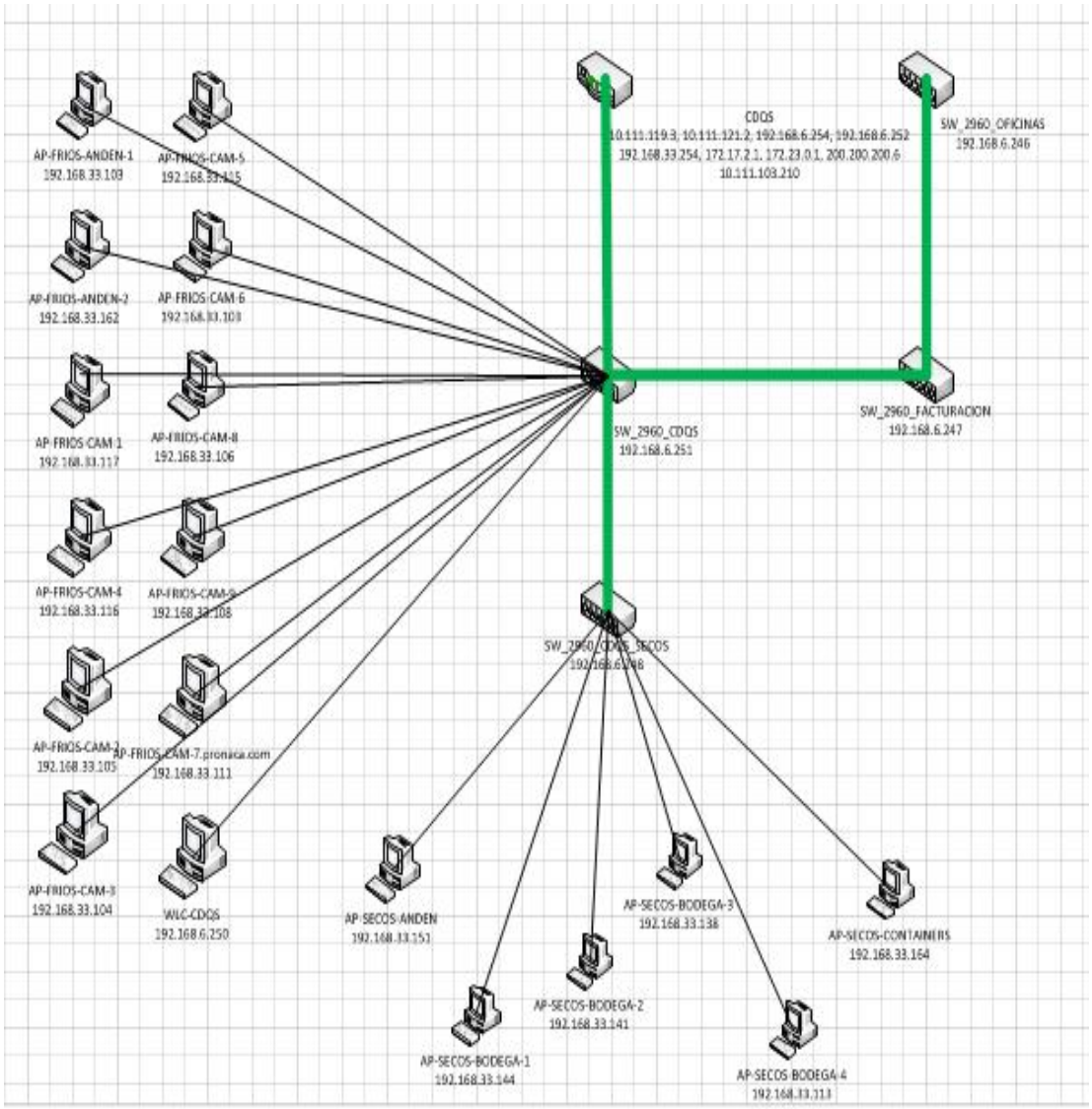

Figura 3.76: Estructura de la Red Centro de Distribución PRONACA CD SUR[65]

Fuente: DBA Networking Ing. Omar González

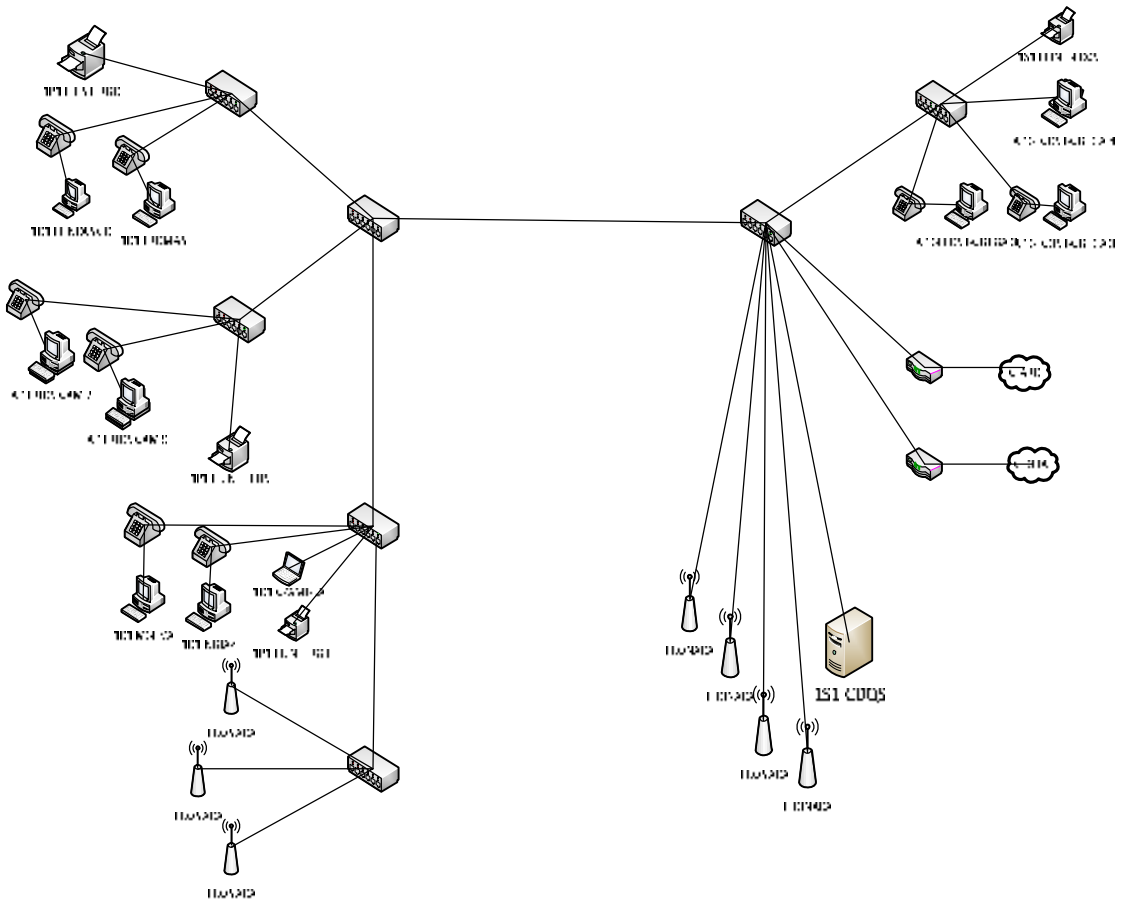

Figura 3.77: Estructura de la Red Centro de Distribución PRONACA CD SUR[63]

Fuente: DBA Networking Ing. Omar González

3.1.2 CONCEPTOS DE SEGURIDAD

Las políticas de seguridad nacen como una herramienta para las organizaciones que sirven para dar a conocer a cada uno de los usuarios que conforman la organización, sobre la importancia de tratar la información y los servicios que favorecen al desarrollo y buen funcionamiento de la organización.

3.1.2.1 Definiciones

- La seguridad puede ser confidencial para algunos usuarios o para instituciones completas.
- La información se almacena y se procesa en host, que pueden ser independientes o estar conectados a sistemas de redes.
- Una red es un conjunto sistemático de canales conductores que comunican los servicios o recursos para un fin determinado.
- La seguridad es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Al unir todas estas definiciones podemos dar un concepto concreto a lo que es la seguridad en una red.

La seguridad en una red tiene como objetivo resguardar y proteger a todos los recursos y la información que la red cuenta, basándose en una política de seguridad que permitan el control de lo que se va a hacer.

3.1.2.2 Impacto

La implementación de un sistema de seguridad conlleva a dificultar las operaciones en la empresa, tanto técnica como administrativa.

Es una tarea que no tendría complicación si solo un usuario tiene acceso a la información, debido a que solo se revisará el contenido habilitado en el servidor, pero cuando varios usuarios tienden a actualizar la información simultáneamente, en ese caso deberán establecer reglas estrictas, asignando responsabilidades a cada usuario.

Las WLAN son inseguras por naturaleza ya que son fáciles de vulnerar que una LAN y que un hacker puede violar la seguridad de una empresa desde cualquier host. A esto se puede decir que si bien es cierto que esto puede suceder, la

vulnerabilidad no está en la tecnología como tal, sino en las políticas de seguridad que tenga la empresa. Una WLAN puede ser tan o más segura que una LAN si se posee la preparación necesaria. Existen firewalls especialmente diseñados para las WLAN, los cuales han probado ser efectivos y poderosos.

Las empresas se han demorado en adoptar la tecnología de uso y soporte general, y ha delimitado frecuentemente su aplicación a la administración de bodegas y transporte de carga. Las WLAN primero ingresaron al mercado residencial y ahora están apareciendo en las oficinas.

Las organizaciones no pueden adoptar más la postura de "esperar a ver qué pasa" ante la tecnología inalámbrica. Ésta es la realidad actual: sin orientación ni dirección, los colaboradores y socios están comprando, instalando y ejecutando su propia tecnología móvil para usarla en el trabajo. Los usuarios tienen control sobre el proceso de compra, el flujo de información y cada vez más sobre la seguridad de la organización.

Es apropiado desarrollar una amplia estrategia sobre el uso que se le dará a la tecnología inalámbrica. Se deben entender las consecuencias de esta tecnología para la seguridad si se quiere cumplir con un estándar de cuidado. Las políticas de seguridad se deben actualizar para que abarquen las aplicaciones que están planeadas y aquellas que ya utilizan los colaboradores y grupos de trabajo.

Las empresas deben considerar los siguientes pasos cuando comiencen a aceptar la tecnología inalámbrica y desarrollar sus propias estrategias inalámbricas.

El departamento de IT debe desarrollar y tener conocimientos sobre los sistemas operativos y host utilizados por la organización. Si el personal de sistemas limita la cantidad de alternativas podrá comprender muy bien las fortalezas y debilidades de cada solución y reducir el costo total de propiedad al minimizar el desarrollo de las aplicaciones, soporte y capacitación.

Los usuarios hasta ahora han tomado decisiones sobre la tecnología que utilizan y cómo la utilizan. La administración y mantenimiento de los host y servicios necesita el costo de propiedad y requerirán el hacer cumplir la política. Si el negocio de la compañía se realiza en éstos sistemas, a través de o por parte de ellos, se debe tener en cuenta la seguridad.

El riesgo debe equilibrarse con la función de la administración básica de la información personal, como la libreta de direcciones y programa cronológico, se deben asumir de manera diferente a las actividades de administración de las relaciones comerciales móviles auténticas. El personal de sistemas y los host de seguridad deben determinar los riesgos que son permisibles y los métodos que se deben utilizar para reducir o mitigarlos. Los servicios de las empresas de telecomunicaciones jugarán un papel cada vez más importante en la prestación del servicio de conectividad entre el usuario remoto y la oficina.

Las políticas de seguridad se deben actualizar con frecuencia para reflejar el impacto que pueden tener las características y la función del host inalámbricos en los sistemas existentes, un entorno que aparentemente fue seguro alguna vez puede necesitar una actualización de las políticas y configuración.

Los estándares, políticas y diseño por sí mismos no protegerán a la organización, es fundamental capacitar a los colaboradores sobre su función de respaldar las políticas de seguridad y determinar las precauciones que deben tomar para mitigar los riesgos.

3.1.2.3 Implementación

La implementación de técnicas de seguridad es un proceso técnico y administrativo, este proceso debe estar totalmente apoyado por el sector gerencial ya que toda la organización la va a abarcar y si no se lo hace, las medidas que se tomen no tendrán validez alguna.

Tomar en cuenta que la implementación de estas medidas, aumentara la complejidad en las operaciones de la organización, y las ganancias en seguridad con respecto a los costos administrativos y técnicos que se genere.

Para que el usuario pueda establecer una conexión de acuerdo a la seguridad dada tendrá que realizar lo siguiente:

- Ser usuario registrado y activo en la organización.
- Poseer un host con tarjeta inalámbrica integrada.
- Acudir al administrador o encargado de la red para que le ingrese la clave de acceso.
- Ingreso de la clave de acceso.
- Una vez validado, estará conectado a la red de la empresa y podrá navegar o acceder a aquellos recursos de la misma a los que esté autorizado.

3.1.3 POLÍTICAS DE SEGURIDAD

3.1.3.1 Políticas de Seguridad Informática

No se pueden establecer sistemas totalmente seguros al 100%, por motivos de que al implementar un sistema de seguridad conllevaría a incrementar las operaciones de la empresa tanto técnica como administrativa, y se debería destacar que la seguridad debe ser considerada desde la fase de diseño.

Porque si la seguridad se contempla luego de la implementación, todo el personal puede enfrentarse a problemas técnicos, humanos y administrativos de gran magnitud que implicaría mayores costos para lograr un menor grado de seguridad, por esa razón las empresas se arriesgan a perder su establecimiento o simplemente a sufrir un hackeo repentino.

Para estos casos surgen las políticas de seguridad informática, que no son más una herramienta que sirve para hacer conciencia a cada uno de los usuarios de la

empresa sobre lo importante y lo sensible que es la información y sus servicios, ya que esto es lo que permite que la empresa crezca y se desarrolle.

3.1.3.2 Elementos de una Política de Seguridad Informática

Para establecer una política de seguridad informática se deben considerar los siguientes elementos:

- El alcance de las políticas, que incluye las facilidades, sistemas y el usuario sobre lo cual vamos a aplicar. La organización capacita a cada uno de sus miembros, que la información es uno de sus activos principales y permite el desarrollo en sus negocios.
- Los objetivos de la política y una descripción clara de los elementos involucrados en su definición.
- Las responsabilidades a cada uno de los niveles de la organización en cuanto a los servicios y recursos informáticos.
- Los requerimientos mínimos que se debe tomar en cuenta para la configuración de la seguridad de los sistemas que cubre al alcance de la política.
- Las definiciones de las consecuencias y violaciones que se cometerían al no cumplir la política.
- Las responsabilidades que tienen los usuarios con el tratamiento de la información a la que ellos tienen acceso.

Las políticas de seguridad informática deben explicar claramente acerca de las decisiones que se deben tomar, y transmitir la importancia de estos recursos y servicios.

Deber redactarse en un lenguaje fácil de entender, en el cual no contenga términos técnicos para así no impedir la comprensión de las mismas, tratando en lo posible de no quitar su precisión.

3.1.3.3 Parámetros para Establecer Políticas de Seguridad Informática

- Realiza un análisis de los riesgos informáticos y valorar lo más importantes, lo cual permitirá estructurar de mejor manera las políticas de seguridad de la organización.
- Incluya al personal de los recursos y servicios informáticos, ya que ellos son los que tienen experiencia y son la fuente principal para establecer los alcances y las violaciones que se cometen en las políticas de seguridad.
- Informar a todo el personal que esté involucrado en el desarrollo de las políticas de seguridad, sobre los beneficios y riegos que estén relacionados con los recursos, bienes y sus elementos de seguridad.
- Identificar a la persona que tiene la autoridad en la toma de decisiones, ya que son ellos quienes resguardan la información de la funcionalidad de su área.
- Desarrollar un procedimiento en el que se monitoree periódicamente las actividades de la organización, para poder actualizarlas oportunamente.
- Ser explicito y claro al momento de definir los alcances y las propuestas de seguridad, esto para evitar malos entendidos al momento de establecer los mecanismos de seguridad que respondan a las políticas de seguridad informática establecidas.

3.1.3.4 Factores a tomar en cuenta para realizar un Sistema de Seguridad

Realizar una evaluación del factor humano que interviene, ya que es el punto más vulnerable en todo el aspecto de seguridad, los mecanismos con los que contamos para realizar los procesos, el medio ambiente en que se estructura el sistema, las consecuencias que se podría tener y cuales serian las posibles amenazas.

Una vez que se haya evaluado todo lo mencionado, se lleva a cabo un programa de seguridad, que involucra los pasos para asegurar los datos que se desee, luego, pasamos al plan de acción que define como se va a llevar a cabo el

programa de seguridad, finalmente se describen los procedimientos y normas que permiten tener una seguridad mejor estructurada.

Establecer políticas de seguridad es un proceso dinámico sobre el cual se debe estar actuando constante y permanentemente, de tal manera que no se desactualicen y permita que, al momento de descubrir alguna debilidad, se la pueda corregir inmediatamente para que así la red este operativa.

3.1.3.5 Procedimientos para Determinar Passwords

"Una contraseña es una secuencia de caracteres que se pueden utilizar para varios propósitos de autenticación. Las contraseñas se utilizan a menudo para autenticar la identidad de un sistema automatizado de datos de usuario del sistema de procesamiento" **[**64**]**

A pesar de que un password es un juego de caracteres, la mayoría de organizaciones no valoran establecer una clave efectiva, para elegir un password eficaz se debe seguir las siguientes normas:

- Se debe definir los caracteres mínimo que establece el password.
- No debe tener ninguna relación directa con datos personales del usuario.
- Debe contener entre números, letras mayúsculas y minúsculas, símbolos de puntuación.
- Si es posible, se debe llevar un registro de todas las contraseñas que anteriormente haya tenido.

Una vez que el usuario haya elegido su password, debe pasar por un proceso de evaluación mediante un programa crackeador, para verificar el tiempo en el que tarda en romper la contraseña.

Este procedimiento está basado en la norma de "Contraseñas de Uso", utilizado en la categoría estándar para la seguridad informática

3.1.3.6 Procedimientos de Verificación de Acceso

Se debe detallar la forma de realizar las auditorias de los archivos logs de ingreso con el fin de detectar actividades ilícitas, así mismo como el tiempo entre la auditoria y que hacer en caso de detectar intrusiones.

Por lo general todo este procedimiento se lo puede hacer con el uso de un programa al que se le asigna las normativas para que pueda comparar, escanea todos los archivos log[65] con diferentes fechas tomando en cuenta todos los datos que se le ha dado, si llega a detectar algún problema, el programa genera un reporte en donde detalla el mismo.

En este proceso se debe indicar quien es el responsable del mantenimiento del programa que escanea el log y que es lo que se hace cuando surge un problema.

3.1.3.7 Riesgos

La autenticación se realiza por lo general mediante una contraseña, cuando lo más lógico sería la posibilidad de combinar con sensores biométricos para impedir la suplantación del usuario, entre las cuales podrían estar: firmas digitales con reconocimiento en el servidor, análisis de iris del ojo, la huella digital u otras.

Aunque se haya implementado el máximo en seguridad, el mayor riesgo que puede existir es que la informática y la tecnología de la información en general no cubran las necesidades de la entidad, o que simplemente no se ajusten a las finalidades de la organización.

En caso de no tener seguridad, los riesgos serian muchos, lo primero conocerlos y segundo será tomar decisiones al respecto, porque conocerlos y no tomar decisiones no tendría ningún sentido.

---

65 LOG (Archivo que registra movimientos y actividades de un determinado programa)

Existen daños con pocas consecuencias, siendo los errores y omisiones la causa más frecuente normalmente de poco impacto pero frecuencia muy alta y otros, como por ejemplo:

- El acceso ilegal a los datos.
- Los daños por fuego y por agua, sea esta por lluvia o por una tubería mal instalada.
- La configuración no autorizada de programas, su copia indebida y otros, con el único propósito de causar daño, beneficio propio o simplemente por venganza.

Otro riesgo es el hacker, que intenta acceder a los sistemas para demostrar o simplemente presumir que es capaz de romper las seguridades que se hayan establecido.

El hacker puede ser externo como puede ser un usuario mal intencionado, es más, el riesgo seria si ese usuario perteneciere a la empresa, porque tendría acceso rápido y fácil a todo lo que este a su alcance, comprometiendo la seguridad de la información importante.

RIESGO	IMPACTO
Acceso de usuarios que no tienen nada que ver con la información requerida	Se pierde la información
Acceso no autorizado de personas que no pertenezcan a la empresa	Terceros pueden tener acceso a la información y cometer el delito de robo.
Acceso a los archivos que no pertenezcan a los usuarios.	La información puede ser manipulada o podría quedar incompleta
Mala administración en cuanto a autenticación	Cualquier persona podría tener acceso a los archivos internos de la empresa, tomando el control de su contenido

Diseño o ubicación de los equipos en una infraestructura no adecuada.	Los equipos podrían sufrir daño por filtro de agua o exceso de calor que podrían incendiarlos.

3.1.3.8 Niveles De Seguridad

- **Confidencialidad**

Consiste en proteger la información contra la lectura no autorizada, y no solo la protección de la información sino también las herramientas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

- **Integridad**

Siempre es necesario proteger la información contra la modificación sin la previa autorización del propietario.

La información que quiera ser protegida no solo debería estar almacenado en los host sino también considerar otros lugares como respaldos, documentación, registros de contabilidad del sistema.

Esto debido a que pueda existir alguna modificación causadas por estos factores:

- Causadas por errores de hardware o de software
- Causadas de forma intencional
- Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar si los datos fueron modificados durante su transferencia.

- **Autenticidad**

En las telecomunicaciones se refiere a que la autenticidad garantice que el usuario sea realmente quien dice ser, es decir, que deben implementar mecanismos para verificar quien está enviando la información.

- **No Repudio**

No se debe negar la transmisión de un mensaje tanto el origen como el destino, quien envía el mensaje puede comprobar que, realmente, el mensaje fue enviado y viceversa.

- **Disponibilidad de los Recursos y de la Información**

No serviría de nada que la información esté en un sistema y los usuarios no puedan acceder a ella, por lo tanto se debe proteger los servicios de manera que no se privaticen o no estén disponibles a los usuarios de forma no autorizada.

La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

- **Consistencia**

Se debe asegurar de que el sistema funcione siempre de manera correcta y en la forma que se espera, de tal manera que los usuarios no tengan problemas ni variantes inesperadas.

- **Control de Acceso a los Recursos**

Se debe controlar quien utiliza el sistema o cualquiera de los recursos que ofrece y como lo hace.

- **Auditoria**

En esta fase consiste en tener los mecanismos para determinar qué es lo que sucede en el red, que es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

Tener en cuenta los 2 últimos puntos que son de importancia, en cuanto a los derechos de los usuarios, se debe diferenciar entre espiar y monitorear. La ética es algo muy importante que todo buen administrador debe conocer y poseer.

Todos estos servicios de seguridad se debe tomar en cuenta al momento de elaborar las políticas de seguridad en una organización para evitar pasar por alto detalles importantes. De esta manera, es posible describir y dejar en claro los derechos y limites de un usuario y del administrador.

Sin embargo, antes de realizar cualquier acción para lograr garantizar estos servicios es necesario que los usuarios conozcan sus derechos y obligaciones de tal forma que no se sientan ofendidos por los procedimientos de la organización.

3.2 DISEÑO DE LINEAMIENTOS PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD

3.2.1 RECOMENDACIÓN PARA EL DISEÑO

Se podrían hacer varias recomendaciones para diseñar los lineamientos para la definición de políticas de seguridad e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización en un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden ser tratados como cualquier usuario de internet (externo a la organización).

Cuando algunos host de la red interna deben ser accesibles desde una red externa, como servidores de correo y servidores web, es necesario crear una nueva dirección hacia una red que está separado, en la que se pueda tener acceso tanto interna como externamente sin correr el riesgo de que la seguridad de la empresa se vea comprometida, el DMZ o zona desmilitarizada hace referencia a esta red separada que posee aplicaciones públicas. La DMZ actúa como escudo entre la red interna y la externa.

Así mismo, instalar firewall y mecanismos de autentificación entre la WLAN y LAN, situando los AP delante del firewall y utilizando VPN[66] a nivel de firewall para la encriptación del tráfico en la WLAN.

Los usuarios de la WLAN deben acceder a la red utilizando SSH[67], VPN o IPSec[68] y mecanismos de autorización, autenticación y encriptación del tráfico SSL[69]. Lo ideal sería aplicar un nivel de seguridad distinto según que usuario accede a una determinada aplicación.

Como contradicción, es recomendable no utilizar excesivas normas de seguridad por que podría reducir la rapidez y la utilidad de la red inalámbrica.

La conectividad entre host y AP es FCFS[70], es decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual nos tenemos que asegurar un número adecuado de AP para atender a los usuarios..

3.2.2 RECOMENDACIONES DE SEGURIDAD

La seguridad de las comunicaciones inalámbricas se basa principalmente en tres funciones:

- Cifrar de forma eficaz la comunicación, para lo cual se debe usar WPA2 con Radius.
- Limitar el acceso, estableciendo un control de acceso eficaz, basado en los controles de autenticación comentados anteriormente, sea biométrico o firmas digitales.

---

66 VPN (Virtual Private Network - Red Privada Virtual)

67 SSH (Secure SHell - Intérprete de órdenes Segura)

68 IPsec (Internet Protocol Security - Seguridad de Protocolo de Internet)

69 SSL (Secure Sockets Layer - Protocolo de Capa de Conexión Segura)

70 FCFS (First Come First Served - Primero en Llegar Primero Servido)

- Proteger con contraseñas seguras y robustas, que combinen números, letras mayúsculas, letras minúsculas y símbolos, basados en la norma de contraseñas de uso, y en el sistema de protección automática (ADP)

Una vez se dispone del conocimiento de la tecnología disponible para alcanzar estos objetivos, las recomendaciones son las siguientes:

- Filtrado de direcciones MAC.
- Uso de WPA2 bien configurado.
- Ocultación de SSID[71].
- Diseño de red.

3.2.2.1 Filtrado de Direcciones Mac

Los AP tendrán una relación de las direcciones MAC que pueden conectarse a ellos.

La dirección MAC es un identificador único que se asigna a todas y cada una de las tarjetas de red existentes y que se graba en ellas en una memoria especial. Lo hace el propio fabricante de la tarjeta o dispositivo, y consiste en una serie de números que identifican unívocamente a esa tarjeta de red.

De esta secuencia de números se pueden deducir una serie de datos como por ejemplo el fabricante, también es conocida como la dirección física o dirección hardware.

No es un método que ofrezca un alto grado de seguridad, puesto que un atacante puede falsear su dirección y hacer que coincida con una de las permitidas, pero es una medida básica para evitar que cualquiera pueda acceder a la red de forma trivial.

71 SSID (Service Set Identification - Identificar y Nombrar a la Red)

Para conocer cuáles son las direcciones MAC permitidas, el atacante solo tiene que obtener algún tráfico de red, puesto que esta dirección, por definición y obligatoriamente, viaja sin cifrar en cada paquete de información que se transmite.

3.2.2.2 Uso de WPA2

WPA2 es la certificación más robusta que se conoce para Wi-Fi hasta el momento. Es importante que se utilicen, dentro de ella, las tecnologías adecuadas para proteger la información. En este momento esto se consigue con el protocolo CCMP, que incluye el cifrado AES, puesto que en TKIP se han encontrado ya ciertos vulnerabilidades de seguridad.

Otra medida básica es utilizar contraseñas largas, robustas, complejas y que estén almacenadas en un lugar seguro. Si no es posible utilizar un servidor Radius, se puede utilizar PSK.

La ventaja de utilizar un servidor estándar Radius es que, en este caso, cada usuario contará con una contraseña, en vez compartir una misma contraseña entre todos los que se conecten con el AP.

Así, si una clave de usuario quedase comprometida, el atacante solo tendría acceso a la información transmitida entre ese usuario y el AP.

3.2.2.3 Ocultación de SSID

El SSID es una cadena usada por los nodos de acceso de redes inalámbricas por el que los usuarios son capaces de iniciar conexiones.

Es necesario elegir un SSID único en cada AP y, si es posible, que no se publique, de forma que los usuarios que lo necesiten deban introducir este valor de forma manual para encontrar la red inalámbrica.

Al igual que ocurre con el filtrado MAC, un atacante podría llegar a descubrir el SSID aunque no esté publicado.

3.2.3 CONEXIÓN WLAN

En la Figura 3.7 se muestra los pasos a realizar para asociarse con un AP:

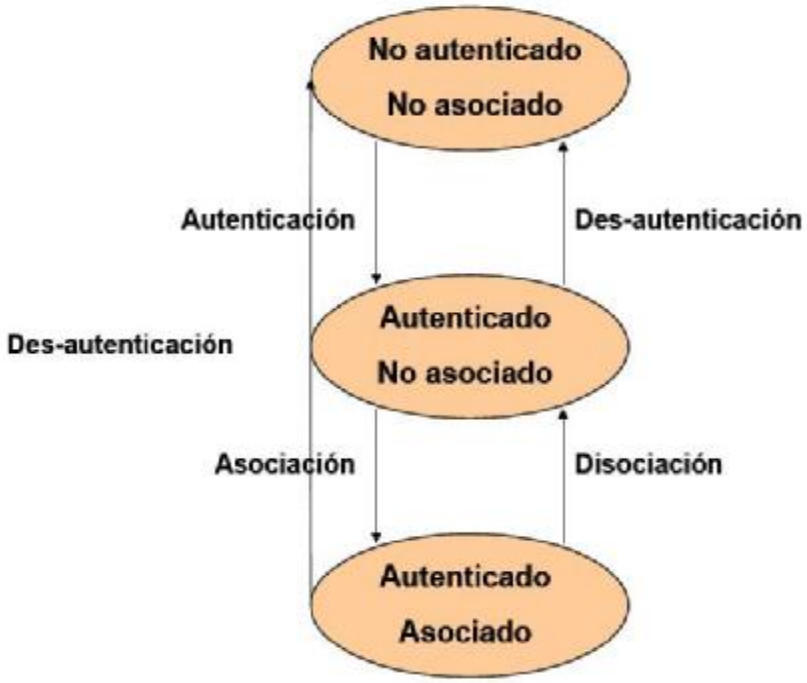

Figura 3.8: Asociar AP[72]

Fuente:http://foro.elhacker.net/hacking_wireless/taller_de_victhor_protocolo_80211_taller_wifi-t261453.0.html

Como se observa en la Figura 3.7, existen 3 estados:

- No autenticado
- Autenticado y no asociado
- Autenticado y Asociado

En el transcurso de los 3 estados, el cliente y el AP intercambian mensajes, en el cual realizan el siguiente proceso:

Los AP transmiten estructura de la trama cada cierto tiempo fijo, para que un cliente pueda asociarse al AP debe introducirse en la red en busca de una estructura de la trama para identificar puntos de acceso.

El cliente también puede enviar una trama de respuesta que contenga un ESSID[73], para ver si le responde un AP que tenga el mismo ESSID.

Una vez identificado el AP, el cliente y el AP realizan una autentificación mutua, intercambiando varios paquetes como parte del proceso, después de realizar la autenticación con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado), el cliente debe enviar un paquete de petición de asociación, y el AP debe enviar un paquete de respuesta de asociación, entonces el cliente llega a formar parte de un host más de la red wireless y está listo para enviar y recibir datos.

3.2.4 LA NECESIDAD DE DEFINIR POLÍTICAS DE SEGURIDAD

La necesidad nace por el motivo de la existencia de un fallo o deficiencia en la seguridad de la información, lo cual la pone en riesgo a la hora de proteger los datos, lo que implica dinero y tiempo invertido.

Con buenas políticas y mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

Elementos que ayudan a la colaboración de las políticas de seguridad:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

---

73 ESSID (Extended Service Set ID - Servicio de Identificación Extendida)

- Responsabilidades por cada uno de los servicios y recursos informáticos aplicados a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Es muy importante que las políticas de seguridad deben estar en un proceso de actualización y revisión constante.

3.2.5 ESTRUCTURA DE UN MODELO DE POLÍTICA DE SEGURIDAD

3.2.5.1 Organización de la Seguridad

Administrar la seguridad de la información dentro de la organización y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la organización.

3.2.5.2 Clasificación y Control de Activos

Garantizar que los activos de información reciban un apropiado nivel de protección.

Designar a los propietarios de la información existente en la Organización.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

3.2.5.3 Seguridad del Personal

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y manejo no autorizado de la información.

Las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal, incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del colaborador.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer acuerdos de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas necesarias para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

3.2.5.4 Gestión de Operaciones y Comunicaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

3.2.5.5 Control de Accesos

Es importante impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información, también se debe implementar seguridad en los accesos de usuarios por medio de técnicas de identificación y autenticación.

Se debe controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas, registrar, revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Hay que tomar en cuenta el hecho de concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos con el propósito de garantizar la seguridad de la información cuando se utiliza host móvil e instalaciones de trabajo remoto.

3.2.5.6 Desarrollo y Mantenimiento de Sistemas

Como parte del mantenimiento se debe asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Concluida la actividad se puede definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base de los cuales éstos se apoyan para definir los métodos de protección de información crítica.

3.2.5.7 Administración de la Continuidad de las Actividades de la Organización

- **Notificación y Activación**: Consistente en la detección y determinación del daño y la activación del plan.
- **Reanudación:** Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- **Recuperación:** Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la organización y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar responsabilidades para cada actividad definida.

3.2.5.8 Cumplimiento

Hay que tomar en cuenta el cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas y legales a la organización y usuario, para garantizar que los sistemas cumplan con las políticas y estándares de seguridad de la Organización.

Como prevención revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de las soluciones y estándares de seguridad, sobre las plataformas tecnológicas y los sistemas de información para de esta manera optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Se debe garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas y determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Organización.

La tendencia en estos últimos años es escuchar la frase “hay que educar al consumidor”, pero en este caso sería, “hay que educar a los usuarios” y en esta frase “usuario” va más allá de la persona que se sienta frente a un host y se limita a hacer su trabajo diario, sino que abarca a todos los que trabajan en la organización desde la cabeza hasta el último.

Las políticas bien elaboradas y aplicadas, si bien implican tal vez mucho dinero hay que entender que ese dinero es bien invertido y en el futuro a la hora de actualizar o implementar nuevos cambios en las políticas ya establecidas puede ahorrar mucho dinero.

También sería bueno y útil que a las políticas acompañen capacitaciones continuas del personal, si se cree necesario crear un calendario donde se fijen horarios, días y períodos de capacitación y una vez que éstos se ponen en práctica realizar un control o seguimiento para que una vez llegado, por ejemplo al

año realizar una evaluación y ver cuáles fueron los resultados arrojados de dicha implementación.

3.3 DEFINICIÓN DE POLÍTICAS

3.3.1 POLÍTICAS DE SEGURIDAD Y GESTIÓN DE USUARIO EN EL SEGMENTO WLAN

Para construir medidas de protección efectivas, se desarrolla un análisis que pretende recomendar procedimientos y planes, que salvaguarden los recursos de la red Inalámbrica del Centro de Distribución PRONACA CD Sur contra pérdidas y daños.

Estas políticas de seguridad de la red inalámbrica de Centro de Distribución contemplaron diversos aspectos, desde la administración de seguridad de la red hasta la conducta de los usuarios que la utilizan y de esta manera, establecer formalmente la definición de los criterios y lineamientos a seguir en esta materia.

Para ello, se tomaran en cuenta gran variedad de factores técnicos, humanos y culturales relacionados con las características propias de la administración interna de la empresa.

Inicialmente, para crear la política de seguridad, se llevaron a cabo las pautas expuestas en el Capítulo II, acerca de cómo idear y establecer un plan para crear una política de seguridad.

Con esta documentación, y luego de analizar tanto la situación actual del Centro de Distribución como los resultados obtenidos del análisis de riesgos, se contaran con los siguientes aspectos iniciales para desarrollar la política de seguridad de la empresa:

- Activos y recursos a proteger.
- Ataques de los cuales es necesario proteger los recursos.
- Factibilidad de las amenazas.
- Importancia de los recursos y activos.

- Medidas a implantar para proteger los bienes de una manera económica y factible.

Estos aspectos permiten identificar todos los recursos a los cuales su seguridad está en riesgo de ser violentada, las posibles amenazas a estos recursos y la factibilidad de su puesta en marcha.

Se determinará la prioridad de los activos a proteger y algunas de las medidas de protección en contra de los eventos adversos, elementos que sirvieron como inicio para determinar los asuntos que deberían ser contemplados en cuanto al uso de la red y sus responsabilidades, para establecer dentro de las políticas lo siguiente:

- Usuarios con permiso de utilizar los recursos.
- Uso correcto de los recursos.
- Personal autorizado para garantizar acceso y aprobar el uso.
- Privilegios de administración del sistema.
- Derechos y responsabilidades del usuario.
- Derechos y responsabilidades del administrador del sistema frente a los usuarios.
- Derechos y responsabilidades de la alta gerencia Después de establecer a qué usuarios se les permite ingresar a los recursos de la red, se deben documentar las guías para el uso aceptable de los mismos. Estas guías dependen de la clase de usuario: usuario interno o externo. Por esto, en la política se establecerá qué tipo de uso de red es aceptable e inaceptable y qué tipo de uso será restringido.

En las políticas de seguridad, la responsabilidad de cada usuario influye en los mecanismos de seguridad implantados.

En muchos casos, dentro de la política recomendada, se plantea claramente cómo debe ser la conducta a seguir por los usuarios, para evitar consecuencias legales a la organización, relacionadas con usuarios que indiquen que no se les informó o entrenó acerca de la política de red.

La siguiente es una lista de restricciones que deberán ser incluidas:

- No entrar a las cuentas de otros usuarios.
- No violar las contraseñas.
- No está permitido interrumpir servicios.
- No se puede compartir el acceso a las cuentas entre los usuarios.

En la política de red recomendada, se determinara que exclusivamente el personal con la cuenta de administrador de red y autorizados por los Directores de cada área, está autorizado a otorgar el acceso a ciertos servicios.

Es por esto que se deberá establecer el permitir el acceso desde un punto central, que otorgue sólo privilegios especiales a usuarios que les permitan llevar a cabo las tareas necesarias para hacer su trabajo.

En cuanto a la creación de cuentas de usuario y la asignación de permisos, se recomiendan procedimientos específicos, para evitar confusiones y minimizar posibles errores cometidos por los administradores del sistema.

En la política de seguridad desarrollada, se definirán aspectos como los derechos y responsabilidades de los usuarios, y los administradores del sistema al utilizar los recursos y servicios de la red.

3.3.1.1 Políticas en Cuanto al Usuario

- Restricciones en cuanto al uso de recursos.
- Cuáles situaciones constituyen abuso en los términos del uso de recursos.
- Política de contraseña del usuario.
- Acciones legales u otro castigo a implantarse en caso de divulgar información confidencial.
- Políticas de uso y acceso de cuentas.
- Privacidad.

3.3.1.2 Políticas en Cuanto al Administrador

- Límites para revisar los directorios o archivos privados del usuario para el diagnóstico de problemas de seguridad.
- Derecho de examinar el tráfico de la red.

Por último, otro punto tomado en cuenta en el desarrollo de la política de seguridad, es el plan de acción cuando la política de seguridad es violada, el cual sirve para proporcionar una guía con respecto a la acción correctiva en una brecha de seguridad. Para definirla se deben ofrecer guías sobre las medidas a tomar, en base al tipo de violación del usuario de la política de seguridad en cuanto a:

- Negligencia personal.
- Accidente o error.
- Ignorancia de la política actual.
- Ignorancia deliberada de la política.

3.3.2 POLÍTICAS DE ADMINISTRACIÓN Y CONTROL DE SEGURIDAD

Las siguientes políticas se deberán diseñar con el fin de cubrir las necesidades y de reforzar ciertas debilidades, identificadas en el diseño de seguridad actual de la organización.

Además proveen los lineamientos fundamentales que permitirán garantizar la seguridad, disponibilidad, e integridad de la información en el Centro de Distribución, la cual abarca todos los datos e información que se manejaran, mantenidas y procesadas por los sistemas del Centro de Distribución, hasta su transferencia segura a entes externos. Estas proporcionan un marco referencial de actuación a todos los usuarios de la red de la institución, en materia de seguridad de activos de información.

Las políticas de seguridad definen los recursos y procedimientos sujetos al nuevo ambiente de seguridad y acceso, sobre los cuales se fundamentarán los parámetros para la configuración de los mecanismos de protección. Así mismo,

ayudan a prever inconsistencias que puedan introducir riesgos, y funcionan como una base para reforzar aún más los procedimientos y reglas detalladas.

Estas políticas proveerán un marco de actuación a todos los empleados del Centro de Distribución en materia de seguridad de información.

No obstante, todos ellos son responsables de implementar los mecanismos de seguridad necesarios para controlar el acceso a la información que manejan. La estructura de las políticas, cuyo contenido se indica a continuación, se presenta de acuerdo a las siguientes divisiones:

3.3.2.1 Organización de la Seguridad

El objetivo fundamental es establecer una estructura organizativa responsable de definir y mantener los requerimientos de seguridad de información de los usuarios de la red de la empresa.

Este comité estará integrado por personal de la Gerencia de Servicios de Información, para garantizar de una manera eficiente y eficaz la protección de toda información referente a cualquier actividad de la empresa.

En dicha estructura se pueden identificar tres funciones básicas.

Una función principal, es la de establecer y definir los requerimientos de seguridad de cada usuario, la segunda, es la de identificar y coordinar la implantación de los mecanismos más eficientes para proveer los niveles de seguridad requeridos por los usuarios y, la tercera, es la de hacer seguimiento y dar soporte a cada una de las necesidades individuales de seguridad.

Para llevar a cabo la función de seguridad de la información, deben formarse:

- **Comité de Seguridad de la Red**

Representa el aspecto direccional, se encarga de formular directrices y políticas en esta materia.

- **Coordinador de Seguridad de la red**

Representa el aspecto técnico, llevará a cabo el monitoreo técnico de la seguridad y ejecutará las directrices del comité.

- **Coordinador de Seguridad de Recursos Humanos**

Representa el aspecto humano, será el responsable por el desarrollo de la cultura de seguridad en la empresa, de acuerdo con los lineamientos del mencionado comité.

Cada uno de los integrantes de la estructura organizativa, así como las otras personas involucradas en el cumplimiento de los mecanismos de seguridad, deberán cumplir con unos roles de seguridad.

3.3.3 GESTIÓN DE USUARIOS

El objetivo principal es mantener la operatividad de los procesos en la empresa, contemplando los aspectos relacionados con la definición y control del esquema de acceso y seguridad a los datos y las aplicaciones que se encuentren en los sistemas operativos. El mecanismo principal que debe ser tomado en cuenta es la identificación y autenticación del usuario y la validación de los derechos y privilegios de éstos sobre los recursos de la red.

Este esquema de acceso debe ser definido de acuerdo a los requerimientos de información de cada usuario y las características operativas de cada área. En la gestión de usuarios se contempla todo aquello que tenga que ver con la administración de usuarios (niveles de acceso, perfiles expuesta en el Capítulo I, administración de claves de acceso), así como el control de aplicaciones, entre otros.

3.3.3.1 Creación de Usuarios

Cada usuario identificado en el sistema va a tener ciertas cualidades y características que van a definir sus posibilidades de acceso y utilización de los recursos disponibles en la red de la empresa. Estos permisos de acceso a la red

deben ser otorgados por la estructura organizativa de seguridad, según las necesidades específicas de cada caso y tomando en cuenta lo siguiente:

- Por regla general, las aplicaciones estándares están disponibles para que todos los usuarios las puedan ejecutar en cualquier momento; sin embargo, existen aplicaciones especiales que sólo algunos usuarios podrán acceder. Si el usuario necesita alguna de estas aplicaciones hay que otorgarle los accesos correspondientes.
- Si el usuario solicita acceso a directorios comunes en un grupo, (una vez confirmada su autorización), según lo especificado en el grupo correspondiente, le autorizarán los derechos necesarios sobre dicho directorio. Este procedimiento se inicia cuando un colaborador de la empresa, fijo o contratado, requiera integrarse en calidad de usuario para trabajar en la red corporativa.

  Consta de los siguientes pasos, por parte del analista de red:

  - Definir el perfil del usuario y proceder a crearlo, según los requerimientos de éste.
  - Habilitar la cuenta para el acceso a la red, asignando el usuario, al grupo necesario, para que pueda hacer uso de los recursos que necesita.
  - Si se trata de un usuario de aplicaciones de Bases de Datos, se deberá enviar copia del reporte a la División de Base de Datos de la Coordinación de Informática, para que éste asigne los permisos requeridos por dicho usuario para las bases de datos.

3.3.3.2 Definición de Perfiles

Dependiendo de las actividades y de las operaciones que deban realizar los usuarios en la red y para mantener la seguridad y la integridad de los datos y aplicaciones, se deben establecer perfiles de usuarios que regulen el acceso a la red y la utilización de los recursos de ésta.

Las Consideraciones Generales en este aspecto son:

- El acceso de los usuarios a los servicios de la red se hará a través del mecanismo de autenticación mediante la identificación del usuario y una clave.
- Sólo tendrán acceso a la red los usuarios a quienes les sean asignados su identificación de usuarios. Esta asignación se hará a aquellos usuarios que, dependiendo de sus actividades laborales, deben hacer uso de los servicios de red.
- Es imprescindible que todos los usuarios cuando sean definidos les sea colocado su nombre completo, es decir, registrar el funcionario a quien ha sido asignado dicha cuenta de usuario y la unidad en la cual presta sus servicios.
- Sólo será permitida una clave de acceso a la red por usuario. Los únicos usuarios exentos a esta regla son los Administradores y el Supervisor, quienes, además de conocer estas claves, tendrán asignadas cuentas de usuarios ordinarios.
- Los nombres de usuarios están conformados por la primera letra del nombre y el primer apellido.
- Los nombres de usuarios definirán los derechos y privilegios que tendrán los usuarios en la red, así como los recursos y servicios que podrán utilizar.
- Los privilegios de los usuarios sobre los directorios y archivos del sistema operativo y de las aplicaciones deberán ser mínimos para evitar que éstos puedan modificar o borrar algún archivo, sólo tendrán acceso a los directorios de sistemas de las aplicaciones existentes en los servidores para lectura y así poder ejecutar las aplicaciones.
- Una vez realizado con éxito el proceso de entrada a la red, el usuario deberá ser ubicado automáticamente en su directorio de trabajo, en el cual se encontrarán todos sus archivos de datos personales.
- Para los usuarios que no tengan equipo asignado, éstos podrán hacer uso de cualquiera de los equipos de su unidad, pero respetando el número máximo de conexiones simultáneas a la red permitidas por usuario que es de una, es decir, que antes de conectarse con su usuario, el otro usuario

deberá cerrar sesión en su computador, de esta forma, ninguna clave podrá estar activa desde dos lugares distintos al mismo tiempo.

- Debe existir un directorio público, sobre el cual todos los usuarios tienen todos los derechos y donde estos usuarios podrán colocar archivos de datos que deseen compartir con otros usuarios.
- Los Administradores serán responsables de cualquier situación ocurrida que tuviese relación con el área a la que estén asignados.

3.3.3.3 Definición de Usuarios

- Los permisos de cada uno de los usuarios se realizará mediante la asignación de los usuarios a los grupos correspondientes, evitando así la asignación individual de derechos a cada uno de los usuarios.
- Existirá un usuario Administrador del Manejador de Bases de Datos para cada servidor de la institución. Este usuario será el encargado de administrar los parámetros del manejador de base de datos asociados con el sistema operativo del servidor.
- Existirá un usuario Administrador de Bases de datos por cada aplicación instalada en el servidor. Este usuario estará encargado de otorgar los permisos a los usuarios para acceder a las bases de datos asociadas con la aplicación.

3.3.3.4 Autenticación y Control de Acceso

Entre los aspectos que proporciona el firewall, se encuentra la autenticación y control de acceso, a través del establecimiento de reglas, tanto de origen como de destino, que permiten comprobar el acceso a la red. Estas reglas deben ser especificadas en orden de precedencia, de las más restrictivas a las generales, y expresamente permitir el acceso, ya que, de lo contrario, todo el acceso será negado.

Para este fin, el perímetro del firewall debe ser definido, especificando de quién y de qué la red debe ser protegida.

El acceso a los servicios se puede restringir basándose en:

- Nombres de Usuarios.
- Origen y Destino.

♣ **Nombres de Usuarios**

El proceso de autenticación puede ser diseñado para actuar sobre grupos de servicios, en los cuales se especifica que para disponer de ese servicio es necesario ser un usuario autorizado. Para utilizar las reglas de restricción de usuarios es necesario crear un nombre de usuario, en la base de datos internas del servidor, es decir, del Active Directory, creada para la autenticación de nombres de usuarios. Esta base de datos mantiene un registro para cada usuario, incluyendo el mecanismo de autenticación que se utiliza para cada uno de ellos y el tipo de protocolo de autenticación que va a ser aplicado a dicho usuario.
A su vez, también se establece el status de autenticación del usuario, que puede ser:

- Habilitado cuando el usuario puede acceder al firewall repetidas veces.
- Habilitado una sola vez cuando el usuario puede acceder al firewall una vez.
- Deshabilitado cuando el usuario no puede acceder al firewall.
- Temporalmente deshabilitado cuando por cierto período de tiempo no puede acceder al firewall.

♣ **Origen y Destino**

La autenticación también puede ser realizada a través del establecimiento de reglas de permiso, por cada servicio, que reflejen exactamente el modelo de seguridad que se ha diseñado, como por ejemplo:

- Direcciones origen.
- Direcciones destino.
- Usuarios.
- Si requiere autenticación para poder ser utilizado

Cuando se utiliza un firewall de filtrado de paquetes, la autenticación y control de acceso no es posible, ya que ésta se realiza a través de las aplicaciones mediante el proxy.

3.3.3.5 Mecanismos de Detección y Clasificación

El firewall por medio de la verificación de los controles de acceso, establecidos en la configuración de cada uno de los proxys de aplicaciones de los servicios, provee reportes detallados del tráfico que circula entre las redes y hace un seguimiento exhaustivo de la información que circula a través de él, para facilitar al administrador de la red la detección y clasificación de intrusos.

Para este fin, es necesario especificar quiénes pueden acceder a los servicios de la red y qué servicios están disponibles según los requerimientos de la empresa.

Los reportes detallados de seguridad, para detectar y clasificar los usuarios, proveen información de los servicios que están en uso y de la configuración actual del firewall referentes a los siguientes:

- Usuarios autorizados a utilizar los servicios.
- Usuarios que envían mensajes y la fecha de emisión.
- Usuarios que iniciaron sesión.
- Usuarios a los cuales se les negó algún servicio.
- Servicios que fueron negados.

Estos reportes pueden ser emitidos diariamente, brindando una estadística del tráfico y el uso de los registros de ese día, o semanales, mostrando un resumen del tráfico manejado durante la semana. Pueden ser ejecutados con la frecuencia que se requieran y su salida es enviada automáticamente al administrador del firewall por medio de correo electrónico.

También el firewall cuenta con el sistema de registros, el cual contribuye a la detección y clasificación de intrusos, permitiendo establecer una expresión regular en el archivo de configuración e invocando programas específicos cuando un

registro de entrada cualquiera es recibido. Esto permite al administrador provocar la suspensión de un proceso o dirigir un mensaje de alerta cuando un evento adverso ha sido detectado.

Estos sistemas de registro son almacenados una vez a la semana y después de 14 días pasan a un formato comprimido de almacenamiento. El sistema de registro puede ser utilizado como un mecanismo primario de alerta, que indique al administrador la existencia de problemas de configuración, errores en el sistema o condiciones de peligro.

- **Sistema de detección de intrusos (IDS)**

Este mecanismo permite detectar el acceso no autorizado a una red o a un host, estos accesos pueden ser realizados por los hackers o simplemente de algún virus que haya sido programado automáticamente.

El IDS, generalmente, posee sensores virtuales con los que puede obtener datos externos que casi siempre son sobre el trafico de la red, usando estos sensores, el IDS es capaz de detectar anomalías que pueden dar inicio a la presencia de ataques.

Por lo general el IDS suele integrarse con un firewall, porque es incapaz de detener ataques por sí solo, excepto los que utilizan dispositivos que actúen como puerta de enlace incluida la funcionalidad de firewall, lo que lo convertiría en una herramienta sumamente potente ya que combina la inteligencia del IDS y el bloqueo del firewall en donde los paquetes puedan ser bloqueados antes de ingresar a la red.

En ocasiones los IDS poseen una base de datos de firmas de ataques conocidos, para alimentarse y saber sobre problemas que anteriormente hayan sucedido y así estar prevenido con anticipación

- **Sistema de Prevención de Intrusos (IPS)**

Este mecanismo ejerce el control de acceso en una red de información y su función principal es proteger los sistemas de computación de ataques y daños, esta tecnología se considera una extensión del IDS (Sistema de detección de intrusos) pero no lo es, por que este maneja otro tipo de control de acceso, parecidos a la acción que realiza el firewall.

Los IPS mejoran de manera aceptable a la tecnología de los firewall tradicionales, tomando decisiones de control de acceso basados en los contenidos, en lugar de basarse en direcciones IP o puertos.

Es importante destacar también que los IPS pueden actuar a nivel de los host, para contrarrestar actividades que sean potencialmente maliciosas.

Otro mecanismo de prevención de intrusos es el sistema de alarma, que permite alertar al administrador de problemas potenciales que puedan existir. Periódicamente, el sistema de alarma ejecuta un chequeo de la información que haya accedido al sistema de registro.

En este sistema se define una lista de los sucesos que no son importantes para que sean ignorados, mientras que los demás sucesos son traídos al administrador del sistema para su atención. El sistema de alerta es chequeado constantemente y cualquier salida generada por él es enviada electrónicamente al administrador del firewall inmediatamente.

Los resultados de esta investigación pretenden sentar las bases para guiar la implementación de la “tecnología” de seguridad, la cual tiene como finalidad establecer la dependencia entre las políticas de seguridad sugeridas y las medidas de protección tecnológicas seleccionadas. Logrando así unificar esfuerzos que permitirán elevar el nivel de seguridad actual.

Los Sistemas de Prevención de Intrusos tienen varias formas de detectar el tráfico malicioso:

- Detección Basada en Firmas, como lo hace un antivirus,
- Detección Basada en Políticas: el IPS requiere que se declaren muy específicamente las políticas de seguridad,
- Detección Basada en Anomalías: funciona con el patrón de comportamiento normal de tráfico (el cual se obtiene de mediciones reales de tráfico o es predeterminado por el administrador de la red), el cual es comparado permanentemente con el tráfico en línea, enviando una alarma cuando el tráfico real varía mucho con respecto del patrón normal, y
- Detección Honey Pot (Jarra de Miel): funciona usando un equipo que se configura para que llame la atención de los hackers, de forma que estos ataquen el equipo y dejen evidencia de sus formas de acción, con lo cual posteriormente se pueden implementar políticas de seguridad.

♣ **Dispositivo de Seguridad Adaptivo (ASA)**

Todas las empresas están destinadas a tener una red y por ende a depender de ellas, por lo tanto necesitan una seguridad solida, eso es lo que ofrecen los dispositivos de seguridad adaptivo de Cisco, con su seguridad de última generación y la flexibilidad necesaria para satisfacer las necesidades de una empresa a medida que se va desarrollando y creciendo.

Estos dispositivos soportan:

- Personalización: Puede personalizar la seguridad dependiendo de las necesidades de acceso especifico y políticas comerciales.
- Flexibilidad: A medida que la empresa vaya creciendo y necesite realizar cambios, los podrá hacer fácilmente o actualizar de un dispositivo a otro.

- Seguridad avanzada: Cuenta con los últimos avances en seguridad de contenidos, cifrado, autenticación de identidad, autorización y prevención de intrusiones.
- Simplicidad: Cada dispositivo está diseñado para ser fácil de instalar, gestionar y supervisar.
    - Redes Avanzadas: Puede configurar redes privadas virtuales (VPN) que proporcionen a los usuarios un acceso seguro a los datos de la empresa o puede establecer VPN entre patrocinadores, otras oficinas o empleados que cumplan roles.

CAPITULO 4

4 PROPUESTA

4.1 POLÍTICAS DE SEGURIDAD

4.1.1 POLÍTICAS GENERALES

Se debe proveer políticas de actuación al colaborador de la organización en materia de seguridad de la información y dar a conocer la filosofía que en estas políticas se establece. Estas instrucciones están dirigidas a todos los usuarios del Centro de Distribución CD Sur de PRONACA, con el propósito de incorporar las mismas en sus rutinas de trabajo, las cuales se detallan a continuación:

- Todos los activos de información, manejados a través de la red del Centro de Distribución de PRONACA CD Quito Sur, deberán ser protegidos de manipulación, alteración, revelación, destrucción y de cualquier hecho, accidental o no, que altere la integridad de los mismos.
- Todos los colaboradores de la organización serán responsables de administrar la seguridad, según los lineamientos internos establecidos, y de crear los mecanismos de control de acceso a la información por ellos manejada. El personal gerencial y el área de recursos humanos son los responsables de desarrollar la conciencia de seguridad en la organización.
- El personal gerencial de la organización será responsable de identificar y proteger todos los activos de información que están dentro del área asignada a ellos, para su control, administración, y de implantar las prácticas de seguridad en su área asignada.
- Todos los usuarios de la red deberán considerar las prácticas de seguridad al momento de generar los activos de información, así como también al momento de manipular los mismos, a fin de resguardarlos y garantizar su confidencialidad e integridad.
- El comité de seguridad de la red, la Coordinación de Informática y el área de Recursos Humanos, serán los responsables de desarrollar los criterios de actuación del personal en materia de seguridad, así como también de

diseñar los mecanismos o procedimientos de control que garanticen la protección de los activos de información, a los fines de llevar a cabo las políticas recomendadas y poder monitorear el cumplimiento de las mismas.

4.1.1.1 Usuarios de la Red

Como fundamento principal se provee las políticas para los Usuarios de la Red en materia de seguridad de la información, a fines de incorporar las mismas en sus rutinas de trabajo. Con el fin de no comprometer la seguridad de la red, todos los usuarios deben cumplir con las siguientes responsabilidades:

- Modificar periódicamente las claves personales de acceso a la red.
- Acatar todos los criterios, lineamientos de almacenamiento y respaldo de datos.
- Velar por el buen funcionamiento de los equipos que le sean asignados.
- Mantener respaldada y guardada, en un lugar seguro, la información que haya sido clasificada como de alto riesgo o confidencial y que se encuentre bajo su responsabilidad, así como los medios de almacenamiento, manuales y listados de información.
- Apagar el equipo una vez finalizada la jornada de trabajo.
- Destruir, previa autorización correspondiente, cualquier documento que contenga información importante y vaya a ser desechado.
- Efectuar respaldo y borrar del disco duro la información almacenada en él, cuando el área de operaciones y mantenimiento técnico deba movilizar el computador fuera de su área asignada, bien sea por reasignación, por reparación o cualquier otro motivo.
- Notificar de inmediato al Comité de Seguridad y Coordinación de Informática cuando exista la sospecha o se descubra que su información ha sido manipulada sin autorización.
- No dejar información en pantallas, ni listados en la impresora, cuando deba alejarse de su puesto de trabajo.
- Realizar periódicamente pruebas de recuperación de la información respaldada.

- Informar a la Coordinación de Informática cualquier traslado, ingreso o retiro del personal o de equipos.
- Reportar al departamento de soporte usuario sobre cualquier desperfecto, modificación de la configuración o instalación de programas que afecten al equipo.
- Solicitar al departamento de soporte usuario las reubicaciones de equipo que se consideren necesarias y esperar al personal del departamento de operaciones y mantenimiento técnico para que éste realice el traslado.
- Seguir las instrucciones emitidas por el departamento de soporte usuario sobre la estructura de directorios en los discos fijos.

♣ **Prohibiciones para el Usuario**

Para evitar situaciones que comprometan la seguridad de la red, los usuarios no deben:

- Divulgar la clave personal de la red, que le esté asignada para el acceso a la información.
- Realizar la instalación de cualquier programa o aplicación en los host, sin la autorización de la Coordinación de Informática.
- Instalar programas ilegales (sin licencia) en los host de la institución.
- Acceder a la red con las claves de acceso y equipos asignados a otros usuarios sin su previa autorización.
- Trabajar en la red fuera del horario establecido.
- Comer, beber o fumar mientras esté utilizando los host de la organización.
- Usar los host de la organización para la ejecución de juegos informáticos.
- Realizar copias no autorizadas de programas instalados en su host.
- Utilizar los host e información de la organización para fines distintos a los cuales están destinados.
- Instalar programas o aplicaciones en los directorios de datos de los servidores.
- Extraer cualquier tipo de información de la institución sin previa autorización.

4.1.1.2 Administradores de la Red

♣ **Deberes del Administrador**

Con el fin de no comprometer la seguridad de la red, todos los administradores de red deben cumplir con las siguientes responsabilidades:

- Realizar periódicamente respaldos de la información contenida en los directorios de datos de los servidores, con las aplicaciones seleccionadas y bajo los criterios establecidos, y realizar continuamente pruebas de recuperación de la información.
- Guardar los medios de almacenamiento y respaldo de los datos de los usuarios, manuales y listados de información en un lugar seguro, y definir un esquema de respaldo de la información así como los lugares alternativos donde se realizarán los respaldos.
- Mantener en estricto grado de confidencialidad las cuentas y las claves de acceso de los administradores y de los usuarios.
- Documentar las configuraciones de los equipos servidores, dispositivos, programas, aplicaciones, así como también cualquier cambio efectuado en las mismas.
- Mantener actualizada la bitácora con las actividades diarias de cada servidor de la red, reflejando la operación realizada y la persona responsable.
- Notificar por escrito al Coordinador de seguridad de la red, sobre cualquier cambio, problema o incidente de seguridad que ocurra en la red.
- Definir los perfiles de usuario de acuerdo con los requerimientos de éstos y asegurarse de que puedan acceder a todas las aplicaciones solicitadas y a sus datos.
- Verificar que no queden usuarios trabajando en los servidores de la red e indicar en la bitácora los usuarios, que con previa autorización, permanecerán trabajando, luego de finalizar la jornada de trabajo.

- Realizar inducción a todos los colaboradores de la organización acerca de las nuevas medidas adoptadas para garantizar la seguridad de activos de información.
- Asegurar que todos los programas, aplicaciones, sistemas operativos, equipos y dispositivos instalados o conectados a la red, posean funciones de seguridad acordes con los requerimientos de los usuarios.

♣ **Prohibiciones del Administrador**

Para evitar situaciones que comprometan la seguridad de la red los administradores de red no deben:

- Copiar archivos de datos en los directorios de aplicaciones del servidor.
- Copiar o instalar programas o aplicaciones en los discos de datos de los usuarios del Centro de Distribución Cd Quito Sur PRONACA.
- Facilitar la información o el acceso a ella a alguna persona, ajena o interna a la institución, que no esté autorizada para conocer o utilizar dicha información.
- Instalar o copiar programas o aplicaciones ilegales (sin licencia) en los servidores de la red.
- Acceder a la información de los usuarios almacenada en los discos de los servidores de la red.

4.1.1.3 Supervisores y Gerentes

Se presenta fundamentos de políticas para nivel de Supervisores y Gerentes de la Red en materia de seguridad de la información, a los fines de incorporar las mismas en sus rutinas de trabajo.

- Divulgar y asesorar, a nivel de su ámbito laboral, las normas y políticas existentes sobre el uso y manejo de los recursos, desde el más alto nivel operativo, y apoyar en la concientización del personal para que actúe con conocimiento de causa en el tratamiento que debe darse a dichos recursos.

- Mantener un programa de motivación y adiestramiento para la difusión de las normas y políticas existentes relacionadas con la seguridad de la información, hardware, software y cualquier documento considerado propiedad de la organización.
- Ejecutar y hacer cumplir los procedimientos generados y aprobados para el área, los cuales regularán los aspectos relacionados con el manejo de la información.
- Velar porque el personal bajo su cargo designado cumpla, en forma optima, los procedimientos y normativas establecidos para la seguridad de activos de información.
- Velar porque, al finalizar la jornada de trabajo, todos los equipos sean apagados, las estaciones de trabajo desconectadas de la red y que no quede ninguna información olvidada en lugar visible.
- Canalizar las acciones necesarias, en caso de que los colaboradores fijos, temporales o cualquier otra persona que está bajo convenio de asistencia tecnológica, infrinja las normas y políticas existentes.

4.1.2 MEDIDAS DE SEGURIDAD A TOMAR EN CASO DE NO CUMPLIR LAS POLÍTICAS DE SEGURIDAD

Se propone las siguientes políticas para las medidas a tomar en caso de que los usuarios, sean colaboradores o no, violen o incumplan con las normas, políticas y procedimientos de seguridad estipulados.

- Determinar la identidad del infractor o de los infractores.
- Determinar si el infractor es de origen interno o externo a la organización.
- Identificar si la violación ocurrió por negligencia personal, accidente o error, ignorancia de la política actual o ignorancia deliberada de la política.
- En caso de no disponer de las pruebas necesarias para inculpar al transgresor se le permitirá continuar con su conducta hasta obtener la información suficiente y así aplicar las sanciones establecidas.
- En caso de contar con las pruebas necesarias, se procederá a detener las acciones del transgresor y aplicar las sanciones establecidas.

- Los usuarios, sean colaboradores de la organización o no, que violen o incumplan las normas o políticas y procedimientos establecidos serán sometidos a las sanciones administrativas contempladas por el Comité de Seguridad, la Gerencia de servicios de Información y el departamento al que pertenezca el usuario.

4.1.3 RESTRICCIONES POR DEFECTO PARA LOS USUARIOS

- Las cuentas de usuario regular de la red no tendrán fecha de expiración.
- Para cada usuario nuevo que sea definido deberá crearse un directorio raíz, donde el usuario podrá colocar sus datos personales.
- Es obligatorio que todo usuario en la red tenga asignado una clave como medida de seguridad para el acceso a la red.
- Es obligatorio el cambio periódico de las claves.
- Se permitirán sólo tres intentos no exitosos de conexión a la red.
- El cambio periódico de las contraseñas de los usuarios deberá hacerse por claves únicas. Esto quiere decir que cuando un usuario debe cambiar su clave, no podrá usar las anteriormente empleadas.

4.2 PROPUESTA DE IMPLEMENTACIÓN DEL PROYECTO DE GESTIÓN DE POLITICAS DE SEGURIDAD

4.2.1 PROCEDIMIENTO PARA LA IMPLEMENTACIÓN DE LAS POLÍTICAS

El proceso para implementar políticas de seguridad en una empresa, es orientado a lo técnico-administrativo, por el hecho que debe abarcar toda la organización, sin excepciones, y apoyado por la gerencia ya que sin su apoyo no se tendrá fuerza para tomar las medidas del caso.

Hay que tener en cuenta que implementar políticas de seguridad conlleva a ciertos problemas que afectan el desempeño de la empresa, por motivos de complejidad en sus operaciones, tanto técnica como administrativa.

Por esta razón será indispensable analizar la ganancia en seguridad con relación a los costos administrativos y que técnicos que surjan.

Es indispensable notificar a todos los miembros de la empresa sobre las nuevas disposiciones y dar a conocer al resto de la empresa para que así nadie sea excluido y comprendan los actos de la administración

Una Política de seguridad deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porqué de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una proposición de una forma de realizar una política de seguridad adecuada puede apreciarse en la siguiente figura:

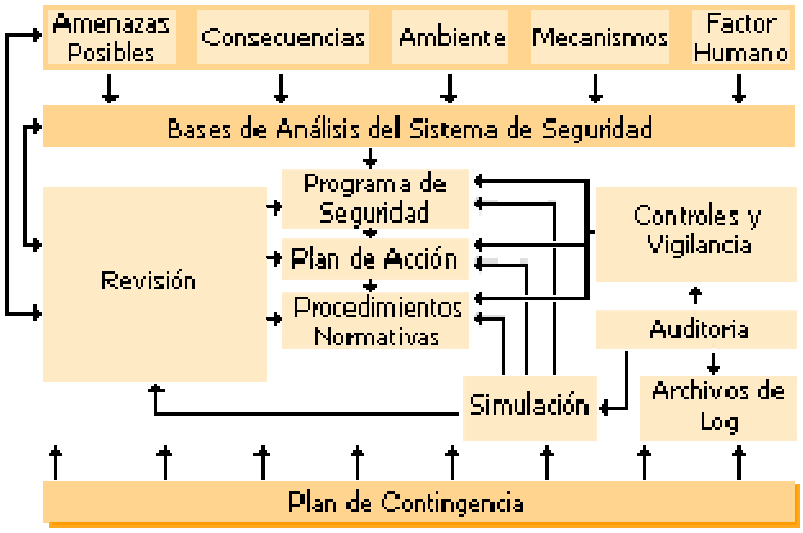

Figura 4.1: Política de seguridad[74]

Fuente: Autor Tesis

Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoría a los archivos Logs de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los casos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por último el Plan de Contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

4.3 GESTIÓN DE USUARIOS

4.3.1 PERFIL DE USUARIO

Los perfiles de usuario son una de las herramientas importantes de Windows para la configuración del entorno de trabajo. Definen un entorno de escritorio personalizado, en el que se incluye la configuración individual de la pantalla, así como las conexiones de red, las impresoras y las aplicaciones a las que tiene acceso.

Cada usuario puede tener un perfil asociado a su nombre de usuario que se guarda en su host, o dependiendo del tipo de perfil, puede residir en un recurso de red (como por ejemplo un servidor Windows 2003 Server) y el usuario o el administrador de sistema pueden definir el entorno de escritorio.

Existen tres tipos de perfiles de usuarios en los sistemas operativos de Microsoft, a partir del Windows 2000Profesional o Server, los cuales son:

Perfil de usuario local.- Es el más conocido, se crea la primera vez que un usuario inicia sesión en un host y se almacena en el disco duro local. Todas las

modificaciones efectuadas en un perfil de usuario local son específicas del equipo concreto en el que se hayan realizado.

Perfil de usuario móvil.- Orientado a redes, lo crea el administrador de sistema y se almacena en un recurso de red una carpeta compartida que puede residir en un servidor, pero que también puede encontrarse en una estación de trabajo. Se descarga al equipo local cuando un usuario inicia sesión y se actualiza tanto localmente como en el servidor cuando el usuario cierra sesión.

Perfil de usuario mandatorio u obligatorio.- Al igual que el anterior, es orientado a redes, pero se diferencia en que no se actualiza cuando el usuario cierra la sesión. Se descarga en el escritorio del usuario cada vez que inicia sesión.

Además de los tres anteriores, algunos expertos hablan de un cuarto perfil de usuario el cual se conoce como:

Perfil de usuario temporal.- se elimina al final de cada sesión. Los cambios realizados por el usuario en la configuración del escritorio y los archivos se pierden cuando cierra sesión.

En este caso gestionaremos los perfiles móviles, que son los que irán dentro de la red.

4.3.2 CREANDO USUARIO

Para crear un usuario en Windows 2003, se debe seguir los siguientes pasos:

“Administre su servidor” -> “Controlador de dominio (Active Directory)” -> “Administrar usuarios y equipos en Active Directory” o “Inicio -> Herramientas Administrativas –> Usuarios y equipos en Active Directory”.

Se ubica sobre el dominio, botón derecho y escoger la opción “Nuevo -> Usuario”.

En la ventana que aparece se coloca los siguientes datos: “Nombre, Apellidos y Nombre de inicio de sesión de usuario”

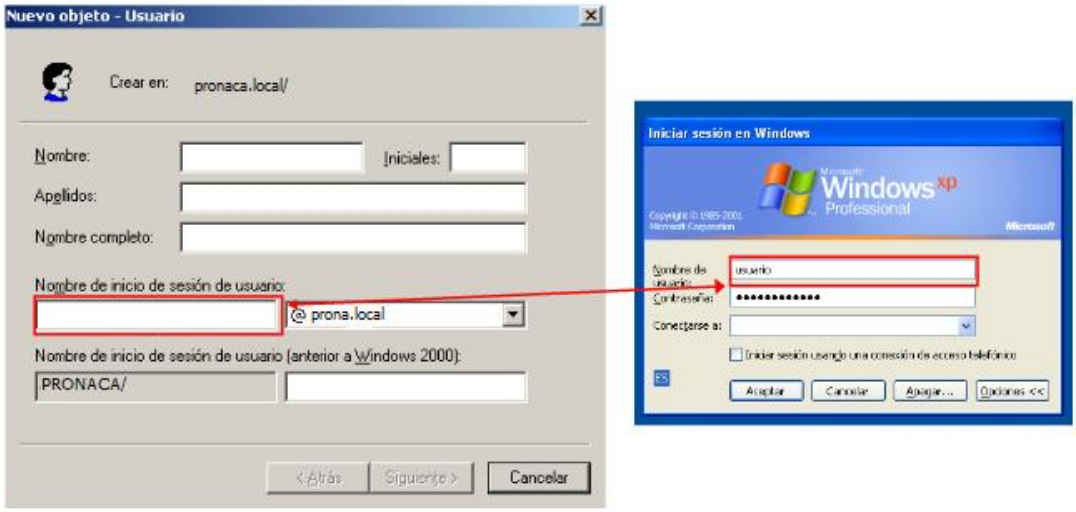

Figura 4.2: Creando usuario [75]

Fuente: Autor Tesis

En la siguiente ventana, se debe colocar la “Contraseña” y “Confirmar Contraseña”. Dependiendo de la configuración que se desea se marca una opción u otra:

- El usuario debe cambiar la contraseña al iniciar una sesión de nuevo.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca caduca.
- La cuenta está deshabilitada.

Algunas opciones son excluyentes entre sí, por ejemplo, marcar a la vez la primera y segunda opción.

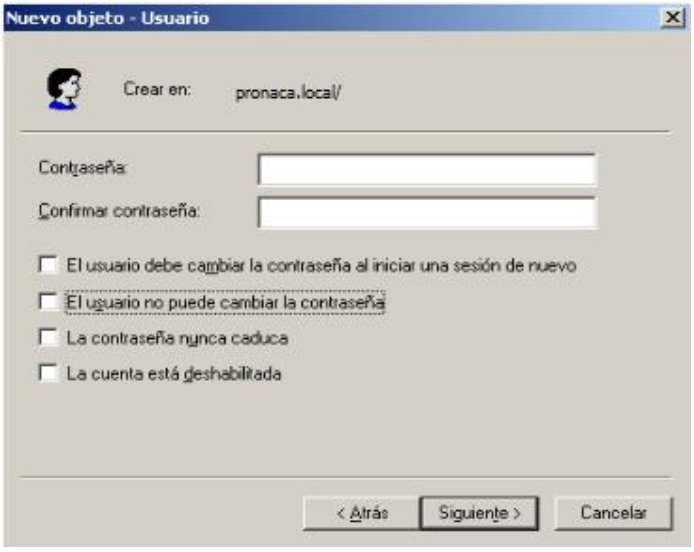

Figura 4.3: Contraseña del usuario [76]

Fuente: Autor Tesis

Una vez creado un usuario, se puede modificar una serie de propiedades sobre él como, por ejemplo, poner una fecha de caducidad a las cuentas o definir en qué días de la semana y horas puede iniciar sesión.

Para cambiar las propiedades de un usuario se sitúa sobre él y con botón derecho escoger la opción “Propiedades”. Se modifica la cuenta del usuario para que tenga una fecha de caducidad, por defecto, no caduca nunca. Ir a la pestaña “Cuenta” y en la parte inferior en “La cuenta caduca” se selecciona sobre “Fin de” y colocar una fecha, por ejemplo, 15 de marzo de 2012.

Figura 4.4: Fecha caducidad contraseña [77]

Fuente: Autor Tesis

4.3.3 GESTIONANDO PERFILES DE USUARIO

Los perfiles móviles, a no ser que se indique lo contrario, almacenarán los cambios en la configuración del perfil indicados por el usuario (este tipo de perfil será el utilizado por los súper usuarios del Centro de Distribución), tales como los archivos almacenados en "Mis Documentos" o los iconos existentes en el "Escritorio", por ejemplo. Los usuarios de la organización también dispondrán de un perfil móvil, pero que no se actualiza cuando el usuario cierra la sesión, denominado perfil obligatorio, y que se descarga cada vez que el usuario inicia sesión. Los perfiles obligatorios son creados por un administrador y asignados a uno o varios usuarios a fin de crear perfiles de usuario invariables.

Para definir perfiles móviles (obligatorios para los usuarios y dinámicos para los súper usuarios), lo primero que se hace es crear una carpeta compartida donde se almacena la totalidad de los perfiles de los usuarios del centro. Para ello se crea en la unidad "C:" (o dependiendo en donde esté instalado) del servidor Windows 2003 una carpeta de nombre "Perfiles", y posteriormente sobre esta con el botón derecho del mouse, seleccionar la opción "Propiedades", sobre la pestaña "Compartir"; activar en este instante la opción "Compartir esta carpeta".

En la caja de texto "Recurso compartido" indicar el nombre "Perfiles$" y a continuación pulsar sobre el botón "Permisos", comprobando que el usuario "Admin" tiene los permisos "Control Total", "Cambiar" y "Leer".

El usuario "Admin" debe disponer de todos los permisos para que cada usuario pueda grabar su perfil en su carpeta; esto permitiría que cualquier usuario podría grabar lo que quisiera en la raíz de la carpeta "Perfiles" si sabe de su existencia.

De ahí el hecho de incluir el "$" en el nombre asignado al recurso para que no sea visible por los usuarios; esta situación no genera un problema de seguridad, pues ningún usuario podrá acceder a visualizar el contenido de otra carpeta de perfiles que no sea la suya propia, finalmente completar el proceso pulsando sobre el botón "Aceptar".

Figura 4.5: Perfiles [78]

Fuente: Autor Tesis

Para crear un perfil obligatorio, lo primero es tener en cuenta que no esté asignada ninguna ruta de acceso al perfil en los usuarios a los que se va asociar el perfil obligatorio.

Se pulsa con el botón derecho del mouse sobre un usuario, y seleccionar la opción "Propiedades", pulsar sobre la pestaña "Perfil" y comprobar que la caja de texto "Ruta de acceso al perfil" está vacía.

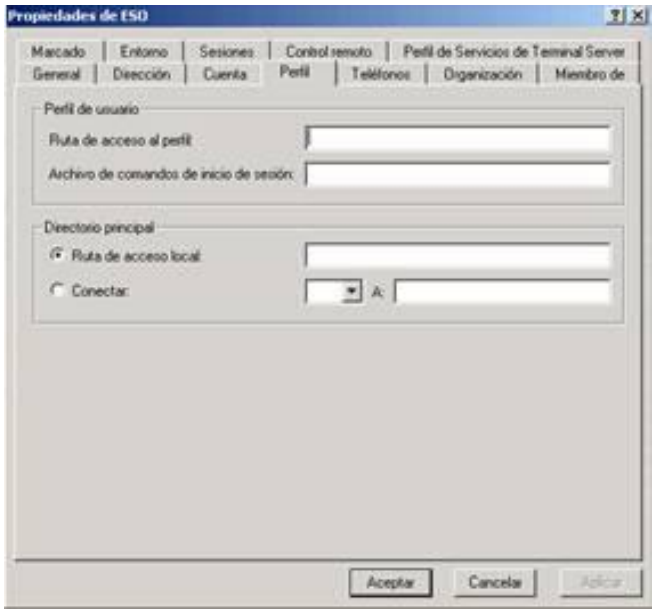

Figura 4.6: Ruta de Acceso [79]

Fuente: Autor Tesis

Una vez comprobado que no existe asociada ruta de acceso al perfil alguna para el usuario, iniciar sesión en un host del dominio con la cuenta del usuario, modificando en dicha sesión el entorno de trabajo, de modo de personalizar el perfil tal cual como lo vean los usuarios; posteriormente cerrar sesión y autenticarse en la misma host como un administrador del dominio (no el administrador de la máquina local).

Figura 4.7: Inicio de Sesión [80]

Fuente: Autor Tesis

Una vez autenticados como el administrador del dominio, ir a la opción “Sistema” dentro de “Panel de Control”; una vez allí pulsar sobre la pestaña “Opciones Avanzadas” y luego sobre el botón “Configuración” del apartado “Perfiles de Usuario”, y seleccionar el perfil “PRONACA\USUARIO”.

Figura 4.8: Perfiles de usuario [81]

Fuente: Autor Tesis

El siguiente paso consistirá en pulsar sobre el botón “Copiar a”, indicando como ruta de destino “\\SERVIDOR\Perfiles$\usuario.man”

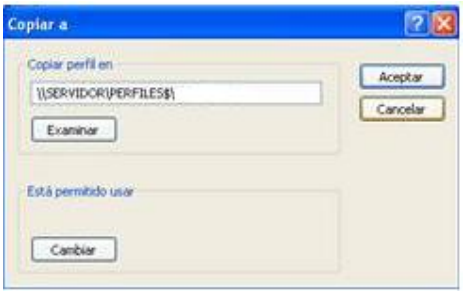

Figura 4.9: Copiar al servidor [82]

Fuente: Autor Tesis

Además en dicha ventana pulsar sobre el botón "Cambiar" para especificar que el perfil puede ser utilizado por el usuario "Admin", tecleando dicho usuario en la caja de texto destinada a tal defecto, tal y como vemos en la siguiente figura. Finalmente pulsar sobre el botón "Aceptar".

Figura 4.10: Seleccionar usuario [83]

Fuente: Autor Tesis

En la pantalla anterior ya aparecerán especificados los usuarios a los que les estará permitido usar dicho perfil; pulsar sobre el botón "Aceptar" para concluir este paso.

Figura 4.11: Especificando usuario [84]

Fuente: Autor Tesis

Una vez completado el proceso anterior, ya se puede cerrar sesión en el host donde se ha realizado el proceso descrito; en este instante ya se encuentra la carpeta “Perfiles$” del servidor, una carpeta de nombre “usuario.man”.

El siguiente paso es ir al servidor y sobre las “Propiedades” de la carpeta “usuario.man”, seleccionar la pestaña “Seguridad”, y sobre el usuario “Admin” definir para dicho usuario permisos de “Lectura y ejecución”, “Listar el contenido de la carpeta” y “leer”, tal y como vemos en la figura 4.11.

Figura 4.12: Asignando permisos [85]

Fuente: Autor Tesis

De este modo se evita que los usuarios que hagan uso del perfil obligatorio puedan realizar una conexión de red y eliminar el perfil obligatorio; una vez hecho lo indicado en el paso anterior, pulsar sobre el botón “Avanzada”, seleccionar al usuario “Admin” de entre los existentes, pulsar sobre el botón “Ver o Modificar” y confirmar que se encuentran activadas las casillas: “Recorrer carpeta/Ejecutar archivo”, “Listar carpeta/Leer datos”, “Atributos de lectura”, “Atributos extendidos de lectura” y “Permisos de lectura”.

Figura 4.13: Permisos de modificación [86]

Fuente: Autor Tesis

NOTA: Estos cambios se propagan automáticamente a las subcarpetas de “usuario.man”, de modo que los usuarios a los que se les asigne el perfil obligatorio, podrán acceder a leer de él, pero no podrán modificar nada, ni siquiera accediendo por medio de una conexión de red al perfil obligatorio. Además, para forzar a que el perfil de los usuarios sea obligatorio, tiene que acceder a la carpeta "usuario.man" y renombrar el fichero **oculto** "NTUSER.DAT" a "NTUSER.MAN".

Hay que tener especial cuidado al renombrar el archivo porque Windows por defecto oculta las terminaciones de los ficheros. Para poder ver la terminación de los archivos y poder renombrar correctamente el fichero "NTUSER.DAT" se procede de la siguiente manera:

En "Mi PC" ir a "Herramientas" y luego a "Opciones de carpeta", pulsar sobre la pestaña "Ver" y una vez allí active la casilla "Mostrar todos los archivos y carpetas

ocultas" y desactive la casilla de "Ocultar las extensiones de archivo para tipos de archivo conocidos". Finalmente cambiar la extensión. Para ver los archivos ocultos que existen dentro de la carpeta "usuario.man", seleccionar la opción "Herramientas" de la barra de menú y a continuación opciones. En la pestaña "Ver" seleccionar que muestre los archivos ocultos.

En este instante ya está definida la carpeta raíz en donde se almacenaran los perfiles de los usuarios del dominio, y también se ha creado almacenando en dicha carpeta, el perfil móvil obligatorio para los usuarios, así pues el siguiente paso es asociar al usuario "nombre_usuario" recientemente creado.

La ruta correspondiente de acceso a su perfil; para ello se accede al servidor Windows 2003, se ubica sobre dicho usuario, y con el botón derecho del mouse seleccionar la opción "Propiedades", yendo sobre la pestaña "Perfil"; una vez allí especificar como "Ruta de acceso al perfil" la ruta "\\SERVIDOR\Perfiles$\usuario.man"

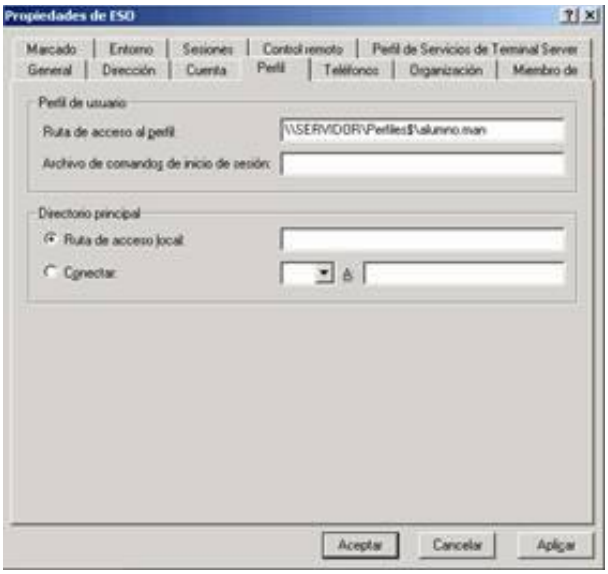

Figura 4.14: Ruta de acceso al perfil [87]

Fuente: Autor Tesis

Para modificar algún aspecto del perfil obligatorio de los usuarios, como por ejemplo incluir un fichero en la ventana inicio o un nuevo acceso directo en el escritorio, se puede hacerlo directamente sobre la carpeta del perfil “usuario.man” del servidor, sin necesidad de hacer todo el proceso descrito anteriormente, copiando dicho fichero o acceso directo en la carpeta adecuada de dicho perfil; por ejemplo podemos incluir posteriormente a la copia de dicho perfil, un fichero de nombre “bienvenida.txt” en la carpeta “Menú Inicio\Programas\Inicio” del perfil del usuario, de modo que cuando el usuario inicie sesión en cualquier estación de trabajo del dominio, se le muestre dicho fichero.

Para el resto de usuarios del dominio (los súper usuarios) especificar como ruta de acceso al perfil la ruta "\\SERVIDOR\Perfiles$\%username%"; la variable "%username%" está asociada al nombre del usuario sobre el que está trabajando, de modo que por ejemplo al usuario "jorge" se le asociará una carpeta de perfil de nombre "jorge", finalmente pulsar sobre el botón "Aceptar". Repetiremos el proceso para los demás súper usuarios.

Figura 4.15: Súper usuarios [88]

Fuente: Autor Tesis

Una vez realizado el proceso anterior, cuando el usuario "jorge" inicie por primera vez sesión desde cualquier host del dominio, se creará una carpeta de nombre "jorge" en la carpeta del servidor donde se almacenan los perfiles; a partir de ese momento cualquier otra autenticación de dicho usuario en cualquier equipo del dominio, provocará el acceso a dicha carpeta del servidor para servir al usuario "jorge" su perfil personalizado (brindándole total movilidad a dicho usuario, pues su perfil siempre será el esperado).

Aunque un usuario pudiera llegar a establecer una conexión a su perfil (y eliminarlo, el usuario no podría eliminar el suyo al no disponer de permisos para ello), en la siguiente autenticación se recrearía de nuevo la carpeta con su perfil en el servidor (obviamente perdería las personalizaciones que hubiera efectuado en el perfil borrado anteriormente).

4.3.4 CREANDO GRUPOS

Las Políticas de Grupo y la infraestructura de servicios del Active Directory en Windows Server 2003 permiten a los administradores de TI automatizar la gestión "uno-a-muchos" de usuarios y host, simplificando las tareas administrativas y reduciendo los costes de TI.

Los administradores pueden implantar de forma efectiva los parámetros de seguridad, aplicar de forma obligatoria las políticas de TI y distribuir software adecuadamente dentro de un site, un dominio o un rango de unidades organizativas.

Los grupos, se hacen para facilitar enormemente la tarea de un administrador, con el siguiente ejemplo:

En una empresa, siempre hay departamentos y cantidades grandes de colaboradores, tienen que acceder a carpetas diferentes, si se tiene a los usuarios distribuidos en grupos, se puede asignar a cada carpeta el grupo que le corresponde, sin tener que enumerar a cada uno de los usuarios en cada carpeta.

En resumen es más fácil asignar un grupo a una carpeta, que asignar muchos usuarios a una carpeta.

A continuación se detalla cómo.

Pulsar con el botón derecho del mouse, en el área en blanco de nuestra unidad organizativa, elegir, nuevo, grupo.

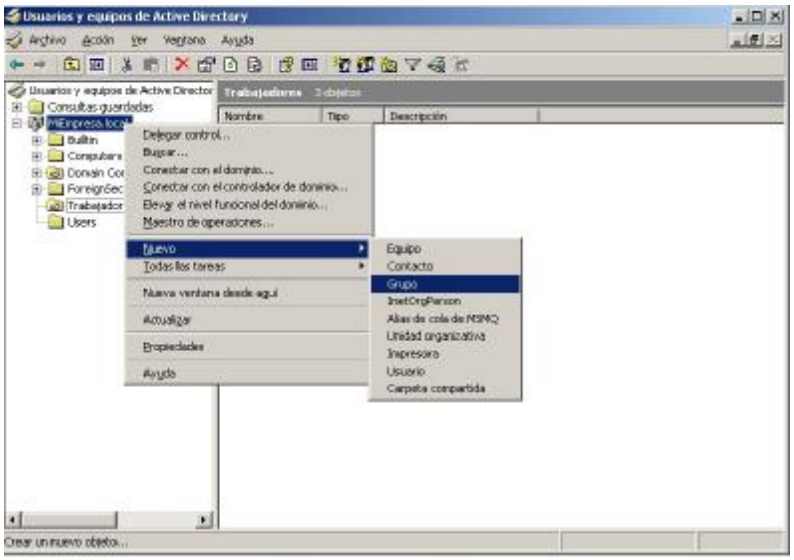

Figura 4.16: Creando grupos [89]

Fuente: Autor Tesis

Colocar el nombre del grupo y pulsar el botón de aceptar.

Figura 4.17: Nombre del grupo [90]

Fuente: Autor Tesis

Con esto se tendrá el grupo creado, pero un grupo vacio no serviría de nada, así que se busca los usuarios que estén en ese grupo. Para ello pulsar con el botón derecho del mouse sobre el grupo y escoger propiedades.

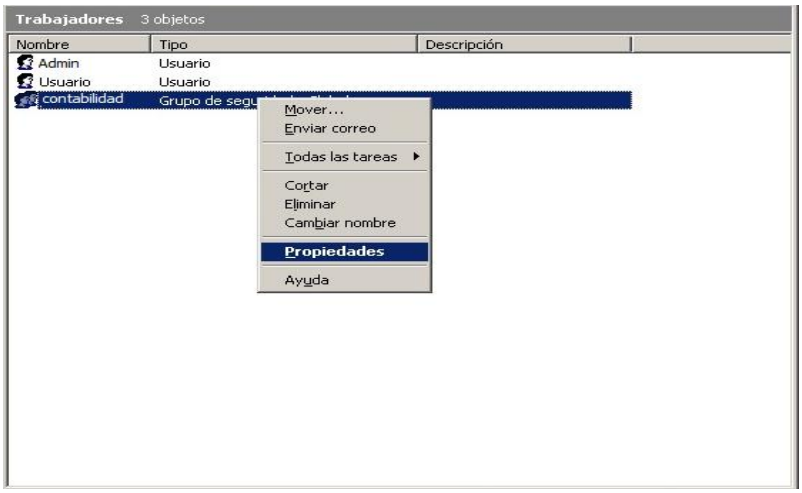

Figura 4.18: Propiedades del grupo [91]

Fuente: Autor Tesis

En la pestaña de miembros, pulsar el botón agregar, e introducir los nombres de los usuarios y pulsar aceptar.

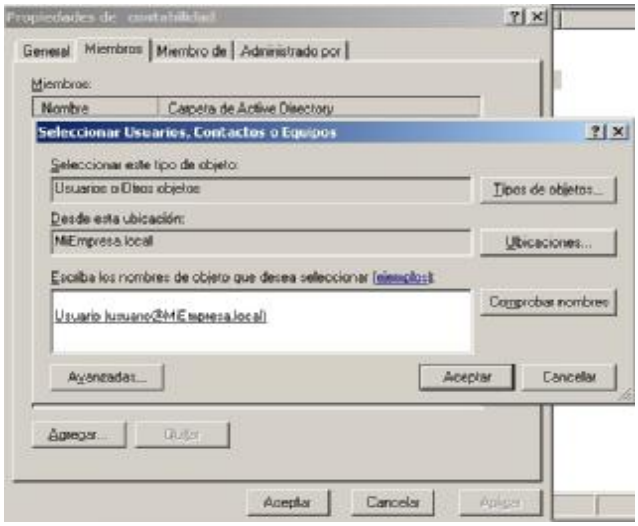

Figura 4.19: Agregando usuarios al grupo [92]

Fuente: Autor Tesis

Se ve que los usuarios están introducidos y volver a pulsar aceptar.

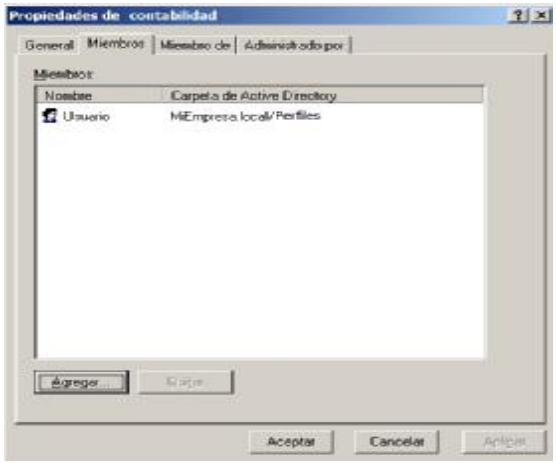

Figura 4.20: Usuarios en el grupo [93]

Fuente: Autor Tesis

Con esto se termino de introducir los usuarios en nuestro grupo.

4.2.5 RESTRINGIENDO EL ACCESO A PROGRAMAS A LOS GRUPOS DE USUARIOS

Una forma de restringir determinadas aplicaciones es el uso de las GPOs [94] de restricción de software.

Existen varios tipos de reglas de restricción de software:

Reglas de certificado: con las que se pueden permitir o restringir aplicaciones según el certificado de editor con el que están firmadas.

Reglas de hash: con las que se crea un algoritmo hash de un ejecutable, permitiendo identificarle aunque se le cambie de ruta o nombre al ejecutable, pudiendo así restringir o autorizar el uso de ese ejecutable. Hay que crear una regla hash por cada versión de cada aplicación, pues al cambiar el ejecutable cambia su hash.

Reglas de ruta (path): estas reglas se basan en la ruta y nombre de un ejecutable. La ventaja que tienen frente a las de hash es que si cambias la versión de una aplicación, se sigue aplicando si la nueva versión tiene el ejecutable en la misma carpeta y con el mismo nombre. Lo malo de estas reglas es que basta con que la aplicación esté instalada en otra carpeta o que se renombre el ejecutable para que no funcionen.

Reglas de Zona de Internet: se aplican solo a paquetes de instalación de Windows Installer y se restringen o autorizan según la zona (Internet, Intranet, Sitios de confianza y Sitios restringidos).

En concreto, se realizara cómo se crea una regla hash. Está hecho utilizando GPMC [95].

---

94 GPO (Group Policy Object - Objeto de Directiva de Grupo)

Se procede a crear una nueva GPO que restringirá el uso de un programa, en este caso el buscaminas, haciendo en el panel del árbol click derecho sobre la carpeta "Objetos de directivas de grupo" y seleccionar "Nuevo":

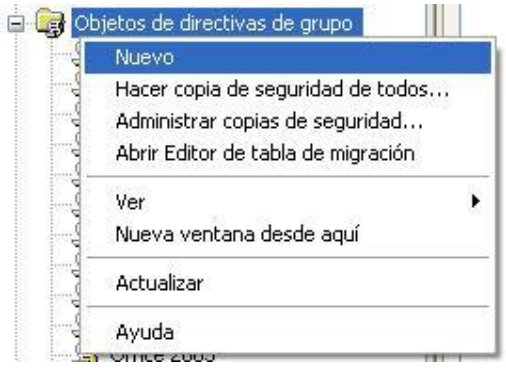

Figura 4.21: Nueva directiva [96]

Fuente: Autor Tesis

Se abre un cuadro de diálogo en el que pide que se establezca el nombre de la nueva GPO:

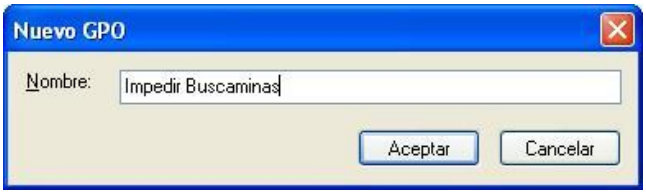

Figura 4.22: Nombre de la directiva [97]

Volver a GPMC y se visualiza que se ha creado la nueva GPO con el nombre establecido en la Figura 4.21. Luego se establece la directiva en ella. Para hacerlo, se necesita editar. En el panel del árbol, hacemos click derecho sobre la GPO y seleccionar "Ejecutar":

---

95 GPMC **(**Group Policy Management Console - Grupo de Política Administrada por Consola)

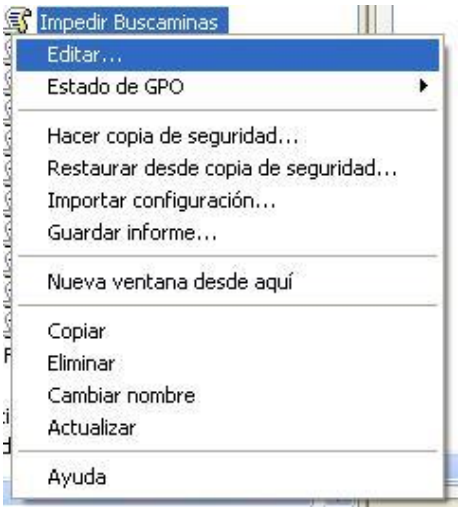

Figura 4.23: Editar directiva [98]

Fuente: Autor Tesis

Se abre el editor de directivas de grupo. Las directivas se pueden establecer a nivel de equipo, de usuario o de grupo, en este caso se va establecer la directiva en la rama de usuario. Hacer click en el panel del árbol en "Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de restricción de software".

En el panel de detalle, advierte de que no hay directivas definidas, en la carpeta "Directivas de restricción de software" no tiene ninguna subcarpeta. En el panel del árbol, hacer click derecho sobre "Directivas de restricción de software" y seleccionar "Crear nuevas directivas" como se muestra en la Figura 4.23:

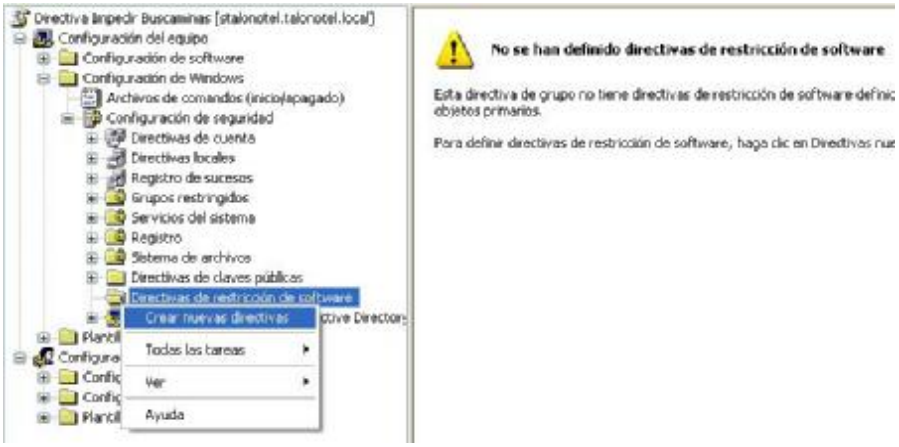

Figura 4.24: Crenado directiva hash [99]

Fuente: Autor Tesis

En el panel de detalle, como muestra la Figura 2.24 ha desaparecido la advertencia anterior y en su lugar han aparecido directivas y carpetas. Ahora, crear la directiva hash de restricción del "Buscaminas".

En el panel del árbol, hacer click derecho sobre la carpeta "Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de restricción de software\Reglas Adicionales" y seleccionar en el menú emergente "Regla de nuevo hash...:"

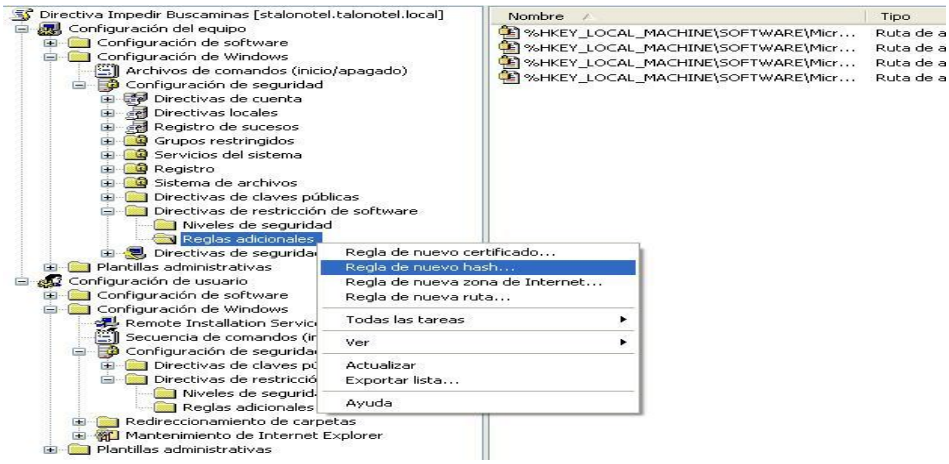

Figura 4.25: Regla de hash [100]

Fuente: Autor Tesis

Se abre el cuadro de diálogo "Regla de nuevo hash":

Figura 4.26: Definir reglas del hash [101]

Fuente: Autor Tesis

Pulsar el botón "Examinar...", navegar a la carpeta "%SystemRoot%\system32" y seleccionar el ejecutable del "Buscaminas", esto es, "winmine.exe":

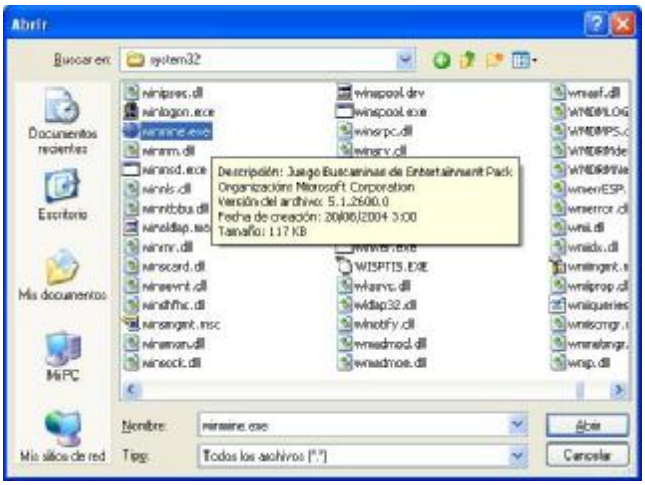

Figura 4.27: Escogiendo aplicación [102]

Fuente: Autor Tesis

Luego pulsar Aceptar, se vuelve al cuadro de diálogo de "Regla de nuevo hash" como se muestra en la Figura 2.47 en la caja de texto "Hash de archivo" el hash generado. Con el desplegable Nivel de seguridad establecer la restricción del archivo seleccionando "No permitido".

También se puede escribir una descripción a la nueva regla en la caja de texto "Descripción":

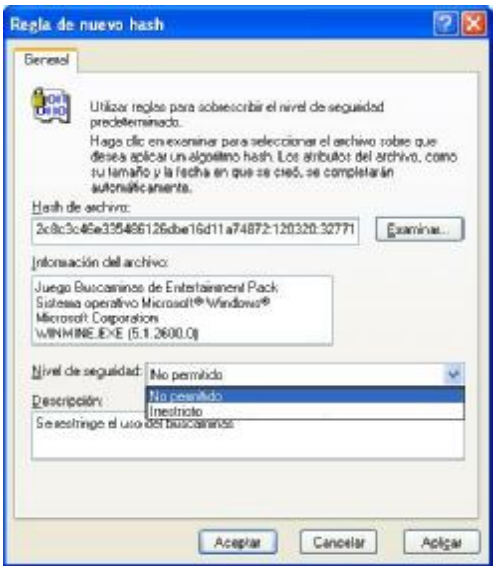

Figura 4.28: Finalizando hash [103]

Fuente: Autor Tesis

Pulsar "Aceptar" y comprobar en el panel de detalle del editor de directivas de grupo que se ha creado la regla hash:

Figura 4.29: Hash establecido [104]

Fuente: Autor Tesis

Ya se puede cerrar el editor de directivas de grupo. Para que la directiva se aplique es necesario que vinculemos la GPO a un contenedor desde el cual se vean afectados los equipos a lo que debe aplicarse.

CAPITULO 5

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El proyecto planteado pretende ayudar al déficit que presenta, los cuales son la falta de políticas de seguridad que controlen y pongan en orden todas las actividades que se realizan dentro de la empresa.

Debido a los grandes cambios tecnológicos que se han venido aconteciendo con el pasar del tiempo, las organizaciones se han dado cuenta que dependen en gran parte de su infraestructura tecnológica. Por lo tanto, las organizaciones e instituciones tanto públicas como privadas deben responsabilizarse por garantizar la seguridad, integridad y confidencialidad de la información que es manejada por ellos. Hay que considerar que este manejo constituye un punto importante para el desarrollo de las operaciones organizacionales, y es por esto que es sumamente necesario el establecimiento de controles de seguridad para la protección y prevención de sus activos de información.

Es de vital importancia tener en cuenta que la alta gerencia debe tomar conciencia sobre la realización de un análisis de riesgos de su información cada cierto tiempo, y poner en práctica métodos más efectivos para protegerlos contra ataques y fallos provocados o no provocados, para alcanzar los objetivos operacionales de una forma efectiva y eficiente.

Crear operaciones organizacionales que permitan realizar un control de las actividades que realizan los usuarios de la empresa, permite llevar a cabo un mejor análisis sobre lo que en realidad se debe proteger y lo que no compromete a una falta de seguridad.

Es importante señalar que en este trabajo de grado se diseña una metodología para establecer las políticas de seguridad de información adecuadas para el Centro de Distribución PRONACA CD Sur las cuales servirán para resguardar sus

activos de información ante cualquier riesgo que se pueda presentar. Una vez lista la metodología el siguiente paso será la implementación de dichas políticas de seguridad de información, en donde la puesta en marcha de las mismas estará a cargo del Centro de Distribución.

El punto más importante de considerar antes de poner en prácticas políticas de seguridad de algún tipo, debe ser un estudio detallado de los riesgos a los que se encuentra expuesta la información, los servicios y el equipamiento de red. Este punto quizás no es muy tomado en cuenta, lo cual conlleva a un gran error, ya que es necesario delimitar el espacio a abarcar por el plan y el espectro de posibles soluciones a cada una de las necesidades específicas.

Además de esto, se debe considerar el nivel de importancia de las aplicaciones, datos o servicios y el tipo de usuarios que las utilizan, ya que son dependientes del tamaño y la naturaleza de las operaciones realizadas por los sistemas automatizados en la empresa. Es necesario destacar además que, aunque se pueden establecer mecanismos para garantizar la seguridad de la información a través de herramientas tecnológicas, no se puede asegurar, que con la implantación de éstas el problema sea resuelto, ya que, luego de analizar los principales riesgos a los que está expuesta la información, se puede afirmar que la mayoría de los problemas, en el área de tecnología en general, son ocasionados por la conducta de los empleados quienes no hacen uso adecuado de los activos de información de las organizaciones.

5.2 RECOMENDACIONES

Una vez que se han aclarado y definido los riesgos a los que está expuesta la información, delimitado el espacio a abarcar y el espectro de posibles soluciones de cada una de las necesidades específicas, se presentan una serie de recomendaciones enfocadas hacia la posibilidad de proveer seguridad y privacidad individual a la información almacenada en los sistemas automatizados del Centro de Distribución PRONACA CD Sur. Estas recomendaciones proveen

las bases para la definición de lineamientos para la seguridad de la información. En forma general, las recomendaciones son los siguientes:

- Establecer una estructura organizativa responsable por definir y mantener los requerimientos de seguridad de la información.
- Evaluar y elegir de manera correcta el método de seguridad, para definir claramente las políticas.
- Formular, documentar y distribuir las políticas, normas y procedimientos en materia de seguridad.
- Evaluar continuamente las políticas, normas y procedimientos de seguridad para, eventualmente, introducir cambios y mejoras necesarias.
- Establecer mecanismos de control para la seguridad de la información en la red.
- Desarrollar políticas escritas sobre la privacidad, describiendo por qué, cómo y qué sobre la recolección de información por la organización.
- Diseñar el procedimiento para asignar las autorizaciones en el sistema y definir los perfiles de los usuarios, de manera que se garantice que las autorizaciones establecidas sean las que el usuario requiere.
- Formular políticas escritas sobre la propiedad de los archivos de datos, escribiendo claramente las responsabilidades de los dueños y usuarios.
- Formular e implementar un compromiso de confidencialidad de información, por parte de los usuarios.
- Definir la función de Auditoría de Seguridad de Información y sus responsabilidades.
- Definir funciones, procedimientos, responsabilidades y permisos de acceso referente a la seguridad de activos de información, dependiendo de las funciones del empleado.
- Establecer medidas disciplinarias a ser tomadas en caso de detectar fraude, hurto o destrucción, modificación o revelación de la información de la organización.

- Definir claramente las limitaciones de los empleados para hacer uso de los recursos de procesamiento de información de la empresa.
- Establecer y formalizar los procedimientos para controlar las modificaciones al sistema operativo y programas de aplicaciones de cada estación de trabajo.
- Formalizar un proceso de documentación que controle el registro de las fallas ocurridas y la descripción de una solución.
- Formalizar, difundir e implementar una política de control de respaldos y recuperaciones.
- Incrementar los niveles de seguridad de la confidencialidad de las claves, restringiendo el acceso a los archivos que contienen la clave secreta de los usuarios, sólo a los niveles supervisores responsables del área de sistemas.
- Establecer controles que garanticen la continuidad de los servicios de informática.
- Establecer mecanismos que permitan la detección y/o eliminación de virus, lo cual puede evitar la pérdida de información vital en la institución.
- Realizar un monitoreo de la red que permita atribuir, de forma rápida, la responsabilidad, al detectarse un procedimiento fraudulento en los activos informáticos.
- Programar, con prioridad, la formalización de un plan de contingencia, debidamente documentado, revisado, actualizado y probado por lo menos una vez al año, con el fin de garantizar la continuidad de las operaciones, en caso de desastres.
- Registrar y realizar un seguimiento formal de fallas para controlar la efectividad de las aplicaciones, así como también conocer los resultados que arrojan para medir y establecer estadísticas sobre las interrupciones generadas y diseñar un plan de mantenimiento efectivo que permita erradicar las mismas.
- Planificar, diseñar y ejecutar planes de educación para los empleados del Centro de Distribución lo cual puede comprender: organizar charlas, conferencias, cursos, programa de inducción y folletos educativos.

- Diseñar y establecer procedimientos para la destrucción de la información confidencial cuando ésta deba ser desechada, a fin de evitar la fuga de la misma a personas no autorizadas.

Tomando en cuenta todas estas recomendaciones se podrá ver posibles soluciones a un futuro, como las siguientes:

- Implementar un sistema de clientes remotos con ayuda de “terminales tontos” o “thin client”, permitiendo el control total de sus actividades y de su información, la cual se almacenara en un solo servidor.
- Generar sistemas en la nube que me permita tener acceso a toda la información, incluso el sistema operativo, desde un servidor que no este ubicado precisamente en la empresa, pero que si se pueda tener acceso a él mediante internet.

BIBLIOGRAFÍA

ANDREU Fernando, *Redes WLAN, Fundamentos y aplicaciones de seguridad*, primera edición, Ediciones Marcombo, 2006.

BURCH, John G. y gary Grudnitski. *Diseño de sistemas de información*, 5ª ed., México, Ed. Limusa, S. A. de C. V, 1998.

CARBALLAR Jose Antonio, *Wi-fi, lo que se necesita conocer*, Primera edición, RC Libros, 2003.

CARBALLAR, José A. Wi-Fi, *Cómo construir una red inalámbrica*, 2ª edición, Ed. Alfaomega Grupo editor, 2005.

GAST, Matthew S., Redes *wireless 802.11*, primera edición, Grupo Anaya Comercial, 2005.

ROYER Jean-Marc, *Seguridad en la informática de empresa*, primera edición, ediciones eni, 2004.

TANENBAUM, Andrew S. *Redes de computadoras*, cuarta edición, editorial Pearson, 2003.

NET GRAFÍA

1. http://www.gsmspain.com/glosario/?palabra=WLAN
2. http://antivirus.asycom.es/1539/el-80-de-fugas-de-informacion-proviene-de-empleados-con-acceso-autorizado-a-la-informacion.html?lang=es
3. http://www.hipertext.net/web/pag251.htm
4. http://delitosinformaticos.info/delitos_informaticos/definicion.html
5. http://www.derechoecuador.com/index.php?option=com_content&view=article&id=5274:registro-oficial-no-87-lunes-14-de-diciembre-de-2009-suplemento&catid=309:diciembre&Itemid=556
6. http://www.pergaminovirtual.com.ar/definicion/IT.html
7. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf, pág. 24
8. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf, pág. 24
9. http://www.alegsa.com.ar/Dic/aes.php
10. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf, pág. 24
11. http://www.cisco.com/web/LA/productos/destacado/nac.html
12. http://en.wikipedia.org/wiki/Intrusion_prevention_system
13. http://www.informaticamoderna.com/Acces_point.htm
14. http://www.simulationexams.com/tutorials/ccna/Cisco-access-control-lists.htm
15. http://www.ieee.org/about/index.html
17. http://www.pronaca.com/site/principal.jsp?arb=168
18. http://es.scribd.com/doc/68432085/3/Historia-General-de-PRONACA-S-A
19. http://www.pronaca.com/site/principal.jsp?arb=8
20. http://www.pronaca.com/site/principal.jsp?arb=8
21. http://padegaindia.in/2011/09/ccna-wireless-tutorial-and-questions/
22. http://gizmologia.com/2011/07/li-fi-transmision-de-datos-por-lu
23. http://visiblelightcomm.com/
30. www.masadelante.com/faqs/voip
31. https://www.u-cursos.cl/ingenieria/2004/1/EL55A/1/.../32643
34. http://www.webopedia.com/TERM/D/DSSS.html
35. http://searchmobilecomputing.techtarget.com/definition/Complementary-Code-Keying

36. http://www.alegsa.com.ar/Dic/ftp.php
39. http://www.definicion.org/telnet
40. http://www.alcancelibre.org/staticpages/index.php/como-arp
41. http://www.significadode.info/palabras-de-internet/wep/
42. http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html
43. http://www.significadode.info/palabras-de-internet/rc4/
46. http://www.ietf.org/rfc/rfc3748.txt
47. NAS (Network Access Server - Servidor de Acceso a la Red).
48. http://tldp.org/HOWTO/8021X-HOWTO/intro.html
50. http://www.formatoweb.com.ar/blog/2007/11/24/el-sistema-de-cifrado-wep/
51. http://www.utpl.edu.ec/seguridad/wpcontent/uploads/2008/10/seg_wifi.pdf
52. http://www.34t.com/box-docs.asp?doc=789
53. http://www.ecualug.org/2007/aug/27/comos/implementaci_n_de_una_red_inal_mbrica_segura_usando_gnu_linux_y_wpa
54. http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html
55. http://conocimientoswirelessnetworkdesign.blogspot.com/2010/05/diseno-de-arquitectura-segura-para.html
56. http://msdn.microsoft.com/en-us/library/aa916736.aspx
57. http://www.h3c.com/portal/ProductsSolutions/Technology/WLAN/Technology_Introduction/200812/624019_57_0.htm
58. http://help.sap.com/saphelp_nw04/helpdata/en/21/53882f3fee0243b6c774e26ebed880/content.htm
60. http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0_ps6366_Products_Data_Sheet.html
61. http://www.cisco.com/en/US/products/ps6018/index.html
62. http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd80635208.html
63. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_at_a_glance0900aecd8047794c.pdf

64. http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&taskId=120&prodSeriesId=4237308&prodTypeId=12883&objectID=c02631865
65. DBA Networking Ing. Omar Gonzalez
66. http://www.itl.nist.gov/fipspubs/fip112.htm
76. http://foro.elhacker.net/hacking_wireless/taller_de_victhor_protocolo_80211_taller_wifi-t261453.0.html

ANEXOS

GLOSARIO

En este glosario se recogen los términos que se utilizan con mayor frecuencia en las tecnologías actuales en el uso de las redes inalámbricas y todas las utilidades que tienen las mismas para el servicio y requerimientos de las personas, en donde podrá entender de una mejor manera el funcionamiento.

1. WLAN (Wireless Local Area Network-Red de Área Local Inalámbrica)

Es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufacturación, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir un acceso a Internet entre varias computadoras.

5. NTCI (Normas Técnicas de Control Interno)

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad.

6. IT (Information Technology -Tecnologías de la Información)

Se refiere en forma generalizada a la tecnología informática.

7. WPA (Wireless Protected Access - Acceso Inalámbrico Protegido)

Implementación de una versión temprana del estándar 802.11i, basada en el protocolo de encriptación TKIP. Es un protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

8. **WPA2**

Está basada en el nuevo estándar 802.11i, creado para corregir las vulnerabilidades detectadas en WPA.

9. **AES (Advanced Encryption Standard - Estándar de Encriptación Avanzada).**

También conocido como Rijndael. Esquema de cifrado por bloques. Algoritmo de encriptación del gobierno de EE.UU, basado en el algoritmo Rijndael, método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

10. **TKIP (Temporal Key Integrity Protocol - Protocolo de integridad de clave temporal)**

Protocolo de encriptación usado en WPA basado en el algoritmo RC4 (como en WEP). Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP

11. **NAC (Network Access Control - Control de Acceso a la Red)**

Un conjunto de tecnologías y soluciones basadas en una iniciativa de la industria patrocinada por Cisco, utiliza la infraestructura de la red para hacer cumplir la política de seguridad en todos los dispositivos que pretenden acceder a los recursos informáticos de la red, limitando así el daño causado por amenazas emergentes contra la seguridad. Los clientes que usan NAC tienen la capacidad de permitir que accedan a la red sólo dispositivos de punto terminal (por ejemplo computadoras, servidores y agendas PDA) confiables que cumplan con las políticas de seguridad y pueden limitar el acceso de los dispositivos que no las cumplen.

12. IPS (Intrusion Prevention Systems - Sistema de detección de Intrusos y Prevención)

Son la red de seguridad que controlan los aparatos de la red, sistemas de actividades para la actividad maliciosa, los dispositivos de seguridad de red que supervisan la red y/o sistema de actividades para la actividad maliciosa. Las principales funciones de los sistemas de prevención de intrusos son la identificación de la actividad maliciosa, registrar información sobre dicha actividad, intento de bloquear, detener la actividad y la actividad de informe.

Los sistemas de prevención de intrusiones se consideran extensiones de los sistemas de detección de intrusos, ya que ambos monitorea el tráfico de red y sistema de actividades para la actividad maliciosa. Las principales diferencias son, a diferencia de los sistemas de detección de intrusos, los sistemas de prevención de intrusiones se colocan en línea y son capaces de prevenir activamente, bloquear las intrusiones detectadas. Más específicamente, IPS puede tomar acciones tales como el envío de una alarma, dejando caer los paquetes maliciosos, restablecer la conexión, bloquear el tráfico desde la dirección IP infractora.

13. AP (Acces Point - Punto de Acceso)

Se trata de un dispositivo utilizado en redes WLAN es aquella que cuenta con una interconexión de host relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada.

Además, los AP pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

14. ACL (Access Control List -Listas de Control de Accesos)

Se usan para filtrar el tráfico sobre la base de un criterio dado de filtrado en un router o un conmutador de interfaz. Sobre la base de las condiciones proporcionadas por el ACL, un paquete se permite o bloquea el movimiento de más.

15. IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos).

Es la más grande asociación de profesionales del mundo dedicada al avance de la innovación tecnológica y la excelencia para el beneficio de la humanidad. Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones.

Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

22. DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuración Dinámica de Host)

Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

23. Li-Fi (Light Fidelity - Fidelidad de Luz).

Se basa en la transmisión de datos mediante la luz a través de un artefacto llamado Fotófono, con el que además, es posible transmitir sonido. Como cualquier otro estándar de transmisión, se usa un emisor y un receptor, en este caso el emisor sería la bombilla LED y el receptor o *fotoreceptor* que se encargaría de interpretar los datos podría ser una *webcam* o la cámara de un dispositivo móvil.

24. VLC (Visible Light Communication - Comunicación de Luz Visible)

Puede ser utilizado para la transmisión en ambas direcciones. El enlace ascendente y descendente se puede aislar en un número de maneras - longitud de onda, hora, código y también por el aislamiento espacial u ópticos. Por razones prácticas y económicas VLC podría aplicarse para el enlace descendente o solo emisión, sólo a partir de aquí es donde existen cuellos de botella con las tecnologías existentes, por ejemplo, Wi-Fi ya se puede proporcionar un enlace ascendente fiable donde la congestión es menos probable y Li-Fi ofrece un enlace descendente de alta capacidad sin congestiones.

25. Wi-Fi Alliance

Es una marca y también la sigla utilizada por la compañía que la creo para referirse a una tecnología de redes inalámbricas se ha usado el término como Wireless Fidelity Wi-Fi por la misma compañía.

26. WECA (Wireless Ethernet Compability Alliance - Alianza de Compatibilidad Ethernet Inalámbrica)

Actualmente llamada Wi-Fi Alliance.

27. Hotspots WI-FI (Punto Caliente)

Los hotspots son los lugares que ofrecen acceso Wi-Fi, que pueden ser aprovechados especialmente por dispositivos móviles como notebook, pdas, consolas, para acceder a internet. Los hotspots generalmente son un servicio que brindan los restaurantes, hoteles, aeropuertos, shoppings, supermercados, universidades y otros lugares públicos.

28. WEP (Wired Equivalent Privacy - Privacidad Equivalente Alambrada)

El protocolo WEP se basa en dos componentes o algoritmos para cifrar los paquetes que van a circular por la red inalámbrica. El primero de ellos es el CRC o Código de Redundancia Cíclica el cual genera una cantidad fija de bits

adicionales para añadir al paquete original con el objetivo de ayudar al receptor a comprobar que los datos que recibe sean los mismos que los enviados. Esta secuencia de bits generados por el algoritmo recibe el nombre de cifra CRC. El otro algoritmo es el RC4, y estará encargado de generar una secuencia pseudo aleatoria de bits que se utilizará para combinar con el contenido de un paquete mediante alguna operación lógica, de manera que no sea posible descifrar el contenido de ese paquete sin la posesión la secuencia generada. Ambos algoritmos serán abordados en las secciones correspondientes de este texto.

29. VoIP Voice Over Internet Protocol - Voz sobre Protocolo de Internet o Telefonía IP)

Una categoría de hardware y software que permite a la gente utilizar Internet como medio de transmisión de llamadas telefónicas, enviando datos de voz en paquetes usando el IP en lugar de los circuitos de transmisión telefónicos.

30. QoS (Quality of Service - Calidad de Servicio)

Se refiere a la calidad en la transmisión y recepción de información a través de una red de datos. es un concepto abstracto y subjetivo, no es una medida estandarizada. Se hace mediante la priorización los paquetes entre sí, dependiendo de su naturaleza y asegurando la exitosa recepción de cada paquete a su destino.

31. TPC (Transmit Power Control - Control Transmisión de potencia)

Control de Potencia Tx determina la potencia de transmisión de la estación base receptora puede variar. El patrón de arriba / abajo, si a partir de un disparador externo o de una secuencia de bits definida por el usuario, dirige la estación base receptora para aumentar o disminuir su potencia de transmisión por una cantidad especificada en el parámetro Paso de alimentación. Este parámetro ajusta la potencia total Tx de todos los canales activos.

32. DSSS (Direct-Sequence Spread Sprectrum - Espectro Ensanchado por Secuencia Directa)

Es una tecnología de transmisión donde se combina una señal de datos a la estación emisora con una secuencia de bits de datos más alta tasa, o código astillado, que divide los datos de usuario de acuerdo con una relación de dispersión. El código de astillado es un patrón de bits redundante para cada bit que se transmite, lo que aumenta la resistencia de la señal a las interferencias. Si uno o más bits en el patrón se dañan durante la transmisión, los datos originales se puede recuperar debido a la redundancia de la transmisión.

33. CCK (Complementary Code Keying - Llave de Código Complementario)

Se emplean para funcionar a velocidades de datos hasta un máximo teórico de 11Mbps en la radio-frecuencia.

34. AES (Advance Encript Standar - Estándar de cifrado avanzado)

AES no es precisamente Rijndael (aunque en la práctica se los llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloques y longitud de claves; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado.

AES opera en una matriz de 4×4 bytes, llamada state (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state).

35. Ad-Hoc.

Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer.

Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

36. JAMMING (interferir con las comunicaciones o la vigilancia)

Cuando se trata de atacar sistemas que empleen señales AJ, el jammer debe emitir una señal portadora en banda base que puede ser modulada por uno o mas impulsos o bien por una señal de ruido.

37. FTP (File Transfer Protocol - Protocolo de transferencia de archivos)

Es ideal para transferir grandes bloques de datos por la red. Permite enviar o recibir cualquier tipo de archivos hacia o desde un servidor.

38. Telnet

Es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto; hoy es poco utilizado. Está definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFC's. Es un acrónimo de telenetwork.

39. ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones)

Se utiliza para supervisar y modificar la tabla de asignaciones de direcciones IP y direcciones MAC.

40. RC4

Es un algoritmo de cifrado de flujo. Los algoritmos de cifrado de flujo, funcionan expandiendo una clave secreta. (En el caso de WEP, un vector de inicialización público (IV) y una clave secreta en una clave arbitrariamente larga de bits pseudo aleatorios (keystream).

41. MAC (Media Access Control - Control de Acceso al Medio)

En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

42. EAP (Extensible Authentication Protocol - Protocolo de Autenticación Extensible)

Es una autenticación framework usada habitualmente en redes WLAN PP. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente su uso en las primeras. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

43. PPP (Point to Point Protocol- Protocolo Punto a Punto)

El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita dos funciones importantes:

- Autenticación. Generalmente mediante una clave de acceso.

- Asignación dinámica de IP. Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

44. RFC3748

En marco de autenticación que admite la autenticación de múltiples métodos.

45. NAS (Network Access Server - Servidor de Acceso a la Red)

Un NAS está destinado a actuar como una puerta de entrada para proteger el acceso a un recurso protegido. Esto puede ser desde una red telefónica, impresoras, o Internet. El NAS a su vez se conecta con otro recurso, preguntándole si las credenciales suministradas por el cliente son válidas. Basado en la respuesta, el NAS permite o impide el acceso a los recursos protegidos, no contiene información acerca de qué clientes pueden conectarse o qué credenciales son válidas. Todos los NAS envían las credenciales suministradas por el cliente a un recurso que sabrá cómo procesar dichas credenciales.

46. PMK (Pairwise Master Key - Clave Principal de la jerarquía de pares de claves)

Se desplaza desde el AS (Authenticator System) al autentificador AP. Sólo el WN (Wireless Node) y el AS puede derivar el PMK, de lo contrario el AP podría hacer que las decisiones de control de acceso en lugar de la AS. El PMK es una clave simétrica fresca vinculado a esta sesión entre el WN y el AP.

47. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - Modo de Cifrado de Encadenamiento de Bloques de Codigo de Autenticacion de Protocolo de Mensajes)

CCMP es el protocolo de cifrado estándar para su uso con el estándar WPA2 y es más seguro que el protocolo WEP y TKIP protocolo WPA. CCMP proporciona los siguientes servicios de seguridad: Confidencialidad de los datos, garantiza que sólo las personas autorizadas puedan acceder a la información; Autenticación, proporciona la prueba de la autenticidad del usuario; Control de acceso en relación con la gestión de capas.

49. SERVIDORES RADIUS

Los servidores de autentificación remota de usuarios por dial-in (RADIUS) permiten la autentificación de usuarios cuando estos intentan acceder al servidor. Utilizan el protocolo AAA (autentificación, autorización y manejo de cuentas) lo cual permite un manejo adecuado de todos los clientes que hacen uso del servidor. Cuando el usuario intenta acceder a la red misma, necesita identificarse por medio de un nombre de usuario y una contraseña. Esta información es recibida por el servidor RADIUS el cual valida una petición de autentificación contra la información almacenada en su base de datos. Si la petición fue aceptada, el servidor se encargará de asignar una dirección IP y los demás parámetros necesarios para la conexión y manejo de la cuenta.

50. PSK (Pre-Shared Key - Clave Compartida Inicial)

Es la que identifica a cada una de las partes en la primera fase del intercambio de claves. Se llama compartida porque los dispositivos la comparten entre si antes de inicializar la conexión segura.

52. AAA (Authentication, Authorization and Accounting - Autenticación, Autorización y Contabilidad)

De la red de servicios de seguridad constituyen el marco principal por la que un administrador de red puede configurar el control de acceso en puntos de la red de servidores de acceso de entrada o de la red, que suele ser la función de un servidor de acceso o enrutador. Identifica a un usuario de la autenticación, la autorización determina lo que el usuario puede hacer, y la contabilidad controla el tiempo de uso de la red para fines de facturación.

54. OSA (Open System Authentication - Autenticación de Sistema Abierto)

No proporciona autenticación. Proporciona la identificación con la dirección del adaptador inalámbrico de MAC. Se utiliza cuando no se requiere autenticación. Es el algoritmo de autenticación por defecto.

65. LOG

Archivo que registra movimientos y actividades de un determinado programa (log file). Utilizado como mecanismo de control y estadística

66. VPN (Virtual Private Network - Red Privada Virtual) VPN, Virtual Private Network.

Herramienta de seguridad que permite mantener en privado una comunicación a través de una red pública. Puede ofrece otros servicios como autentificación de los extremos involucrados, integridad, entre otros.

67. SSH (Secure SHell - Intérprete de órdenes Segura)

Es el nombre de un protocolo y del programa que lo implementa.

68. IPsec (Internet Protocol Security - Protocolo de Seguridad de Internet)

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP)

69. SSL (Secure Sockets Layer - Protocolo de Capa de Conexión Segura)

Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

70. FCFS (First Come First Served - Primero en Llegar Primero Servido)

Se utiliza en estructuras de datos para implementar colas. La implementación puede efectuarse con ayuda de arrays o vectores, o bien mediante el uso de punteros y asignación dinámica de memoria.

71. SSID (Service Set Identification - Identificar y Nombrar la Red)

Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad. Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo.

La infraestructura, el SSID se denomina ESSID o BSSID.

73. ESSID (Extended Service Set ID - Servicio de Identificación Extendido)

Es el nombre de la red o identificador, uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

94. GPO (Group Policy Object - Objeto de Directiva de Grupo)

Directiva de grupo es un conjunto de reglas que controlan el medio ambiente de trabajo de cuentas de usuario y cuentas de equipo. Directiva de grupo proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios en un entorno de Active Directory.

En otras palabras, la Directiva de Grupo, en parte, controla lo que los usuarios pueden y no pueden hacer en un sistema informático.

95. GPMC (Group Policy Management Console - Grupo de Política Administrada por Consola)

Se utiliza para administrar la configuración de las políticas a través de múltiples dominios de Active Directory. GPMC consolidado una variedad de la política anterior y Active Directory snap-ins en la interfaz de usuario.