UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS

SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

PLAN DE PROTECCIÓN Y ADMINISTRACIÓN DE LA INFORMACIÓN DE LA GESTIÓN Y CONTROL DE BONOS DE VIVIENDA QUE MANEJA EL MINISTERIO DE DESARROLLO URBANO Y VIVIENDA MIDUVI A TRAVÉS DEL ANÁLISIS TÉCNICO PRÁCTICO MEDIANTE EL MANEJO Y CONFIGURACIÓN DE HERRAMIENTAS PARA LA GESTIÓN DE SEGURIDAD Y PROCESAMIENTO DE INFORMACIÓN.

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

ANCHALUISA CAZA, ANGEL RICARDO

DIRECTOR: ING. DANIEL DÍAZ

Quito, Febrero 2011

DECLARACIÓN

Yo, Ángel Ricardo Anchaluisa Caza 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 normativa institucional vigente.

Ángel Ricardo Anchaluisa Caza

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ángel Ricardo Anchaluisa Caza, bajo mi dirección.

_____

Ing. Daniel Díaz
Director de Tesis

AGRADECIMIENTOS

Mi agradecimiento y reconocimiento a mi director de tesis, Ing. Daniel Díaz, por todo el tiempo que dedicó a orientarme en la realización del proyecto de tesis, ya que gracias a sus recomendaciones, observaciones, sugerencias y asesoramiento pude culminar satisfactoriamente este trabajo de investigación.

A Dios por darme la vida y regalarme a la hermosa familia que tengo hoy en día, que sin su ayuda no tendría la oportunidad de seguir creciendo profesionalmente y como ser humano.

A mi padre y madre por entregarme todo el amor, cariño, compresión, afecto, dedicación y sobre todo la confianza que depositaron en mí, y de esta manera poder demostrarles que todo su esfuerzo no es en vano. Gracias padres.

A mi querida hermana, gracias beba, por hacerme ver cuando estoy bien y mal, por todas las palabras que siempre las tome como consejos que me ayudarán en mi vida.

A mi querido hermano, gracias ritos, por compartir pequeños y grandes momentos de mi vida, por enseñarme a luchar por lo que uno quiere y tener las suficientes ganas de querer conseguirlo.

A mis queridos abuelitos, Mami Carmencita, Blanquita, Gonzalito y Agustín, por darme a los padres más maravillosos del mundo. Porque en cada una de las palabras que compartían conmigo me enseñaban los buenos valores y el verdadero sentido de la vida, que se resumen en una simple palabra, amor.

A ti, por regalarme los días más felices de mi vida. Siempre te recordaré MJ.

DEDICATORIA

Dedico todo mi esfuerzo, tiempo e investigación al realizar este proyecto de tesis a un ser que ya no está conmigo, a mi mami Carmencita, la persona que me vio crecer desde cuando era un niño. Gracias mami Carmencita, por todo lo que aprendí junto a tu lado, por darme a una madre ejemplar que siempre me apoyó en las buenas y malas.

Por enseñarme a ser un hijo y nieto de bien, y por hacer que nuestra familia siempre se mantenga muy unida. Por eso y mucho más te dedico este pequeño proyecto de tesis, con mucho cariño, tu nieto Ricky.

R!ck….!

Índice

Índice de Figuras.

Índice de Tablas

RESUMEN

La información es el recurso más importante de grandes empresas e instituciones en el mundo actual. Avances tecnológicos y científicos se han logrado con la ayuda de un manejo adecuado de la información, combinado con una amplia investigación, logrando resultados fantásticos.

Es por esto, que el presente proyecto, presenta las mejores alternativas para promover y aplicar una correcta manipulación y gestión de la información en el Ministerio de Desarrollo Urbano y Vivienda, procurando siempre establecer un alto nivel de seguridad, para mantener a este recurso protegido contra agentes que puedan causar daños a la misma.

Asegurar y planificar un correcto manejo de la información, requiere realizar un análisis minucioso de los componentes físicos y lógicos que actualmente posee. Al estudiar los principales problemas de seguridad que existe en la red de datos, se puede sugerir varias alternativas y soluciones que ayudarán enormemente en el desarrollo de la institución.

La forma más práctica para evaluar y verificar el nivel de seguridad que posee el MIDUVI, en cuanto a la protección de la información, es la configuración y utilización de herramientas especializadas en escaneo, rastreo, intrusiones, etc., que permitan realizar un testing de la situación actual y posteriormente sirvan para solucionar los problemas más graves que fueron detectados.

Existen en la actualidad varios programas, aplicaciones y herramientas que trabajan y procesan información de manera rápida y confiable. El proceso de elección de cuáles podrían ser las mejores y más apropiadas, puede ser complicado, pero se debería tomar en cuenta aquellas que cumplan al máximo con las necesidades y requerimientos de la institución.

1. CAPÍTULO: ANTECEDENTES.

1.1. INTRODUCCIÓN

El Ministerio de Desarrollo Urbano y Vivienda, como un organismo que maneja información importante requiere facilitar y agilitar los procesos de procesamiento de la misma, con el objeto de facilitar las actividades que se realizan habitualmente dentro de este Ministerio.

Al hablar de la importancia de la información en la actualidad es conveniente analizar y conocer las diferentes tecnologías de la información, estas se definen como el estudio que envuelve el soporte, administración, análisis, diseño, así como el desarrollo y la implementación de los nuevos sistemas de información que corren bajo un ordenador o PC.

Todo esto abarca componentes físicos, hardware, y por otro lado el equipamiento lógico, conocido como software, que sirve de enlace entre las personas y el computador, que no son más que los programas que ayudan a que la máquina pueda funcionar.

En el mundo actual, hablar de una computadora es algo cotidiano, ya que la ciencia y tecnología va avanzando a pasos gigantescos. Al trabajar con una computadora, se manipula a la vez datos, registros, números, imágenes, videos, etc. que se convierten en información importante y algunas veces crítica y confidencial para las personas u organizaciones. Es por esto, que la información generada debe ser bien cuidada y protegida además de ser manejada de manera adecuada, para poder procesarla y utilizarla de mejor manera.

Para obtener un correcto manejo y administración de la información, así como un nivel adecuado de seguridad de la misma se debe trabajar con las nuevas

Tecnologías de la Información[1] (TI), que proveen un sin número de opciones y alternativas para lograr el objetivo.

El área de aplicación que tienen estas tecnologías de la información es muy amplia y variada, ya que está ganando impulso cada día que pasa, con gran impacto en los campos de trabajo y estudio.

Anteriormente la tecnología de la información se limitaba a las personas que trabajaban en determinados sectores propios de esta rama, como la banca, ciencia, ingeniería, etc.

Según va avanzando el tiempo, se ha podido observar un brote de crecimiento enorme en el uso de tecnologías de la información. La llegada del ordenador personal o computadora ha hecho posible esto y hasta incluso para que grandes grupos de personas puedan beneficiarse de las bondades que provee la misma.

Hay muchos que todavía se preguntan del porqué estas tecnologías de información están revolucionando al mundo, pero está en cada una de las personas aprovecharla de la mejor manera, con la finalidad de seguir enriqueciendo el conocimiento hasta encontrar las verdaderas bondades que puede alcanzar con las tecnologías de la información.

En las empresas, la tecnología de la información juega un papel importante en la gestión y mantenimiento de grandes cantidades de información. Esto ayuda a la creación y generación de información tan buena como la que se podrá intercambiar y emitir a los demás. Es por esto que las empresas podrían trabajar con sus clientes y usuarios en cualquier parte del mundo, como si estuvieran en su propio edificio o lugar de trabajo.

[1] Tecnología de información: El conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión de la información.
Fuente: www.tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=875

Lograr identificar con precisión pequeños y grandes cambios en las instituciones, y así poder implementar un conjunto adecuado de controles, políticas, procesos, procedimientos, estructuras organizativas y software de protección como mecanismos de seguridad.

Las tecnologías de la información han contribuido a diversos sistemas de seguridad para los hogares, empresas e instituciones, en gran medida. Los sistemas más complejos de seguridad se están utilizando en los casos de los organismos de estado y bases militares.

Todo esto se logra conjuntamente con políticas de seguridad y utilización de la información, así como un correcto manejo y gestión de la misma.

Al hablar de grandes bases de datos públicas sin supervisión y de información confidencial con un nivel bajo de seguridad, hace que se desarrollen nuevas herramientas tecnológicas que permitan aprovechar estas vulnerabilidades. De hecho, no es para extrañarse que los delincuentes o piratas informáticos utilicen estas tecnologías como medios de indagación de personas para conocer su estatus y así poder planear un ataque.

Es por todo esto que la información es de vital importancia, para todo el mundo, y la seguridad de la información juega una parte fundamental del éxito en una institución u organización.

Poder garantizar que la información más importante va a tener los niveles de seguridad más alto hace que la institución pueda alcanzar sus metas y desarrollo productivo.

1.2. PLANTEAMIENTO Y DESCRIPCIÓN DEL PROBLEMA

La protección y administración de la información en una empresa, hoy en día, es de vital importancia para mantener los datos y registros correctamente respaldados y administrados, frente a algún daño o desastre que pueda ocurrir.
Si bien es cierto que hace algunos años atrás, la seguridad y el correcto manejo de la información se la colocaba en un segundo plano frente al cuidado y protección de los equipos e instalaciones de una empresa, actualmente el avance tecnológico y científico ha hecho que este concepto cambie notablemente.

El éxito de una empresa no depende solamente de cómo se maneje los recursos materiales, sino también de cómo aproveche sus activos intangibles. El correcto desarrollo de estos últimos depende de que exista un adecuado flujo de información entre la empresa y su entorno, por un lado, y entre las distintas unidades, por otro.

Un grave problema que presentan las empresas e instituciones con respecto a la información, es que no toman las medidas de seguridad y protección apropiadas para este recurso, lo que conlleva a perder datos importantes y en algunos casos confidenciales. Esto se ve reflejado al momento que los usuarios manejan la información de manera irresponsable sin tomar las medidas de seguridad necesarias o que no se cuenta con las herramientas necesarias.

La información que maneja una empresa u organización, además de contener los procesos y procedimientos de la gestión de ésta, acoge muchos datos de la vida del empleado, por lo tanto deben estar sujetos a diversas normas de seguridad y protección, puesto que el uso indebido y substracción de los mismos por terceras personas (internas o externas) puede perjudicar tanto a la empresa o institución como al empleado, generando problemas no fáciles de detectarlos y solucionarlos.

En algunas instituciones del país se maneja información importante sin tener medidas preventivas de respaldo y seguridad en los datos, esto hace que la información pueda quedar expuesta a que otras personas mal intencionadas, la utilicen para fines maliciosos y perjudiciales. Aquellas personas interesadas en conseguir la información de una empresa u organización, buscan la manera más rápida y fácil de extraerla, por lo tanto se debe analizar una solución al problema.

Por otro lado, el poco interés que existe al administrar y manipular la información, conlleva la aparición de problemas graves que pueden costar mucho tiempo y dinero en solucionarlos.

En el MIDUVI se maneja información sobre el control y gestión de proyectos de vivienda, ésta información es vital para el mismo y por lo tanto debe estar bien respaldada y administrada, es por esto que se plantea una solución a los posibles riesgos y amenazas que puedan perjudicar de manera radical su información, diseñando un plan para un correcto manejo y gestión de la información, y por otro lado, proponer y sugerir las mejores alternativas que pueden ser implementadas utilizando herramientas y aplicaciones para la administración y seguridad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

GENERAR UN PLAN DE PROTECCIÓN Y ADMINISTRACIÓN DE LA INFORMACIÓN DE BONOS DE VIVIENDA, QUE MANEJA EL MINISTERIO DE DESARROLLO URBANO Y VIVIENDA A TRAVÉS DEL ANÁLISIS TÉCNICO PRÁCTICO MEDIANTE EL MANEJO Y CONFIGURACIÓN DE HERRAMIENTAS PARA LA GESTIÓN DE SEGURIDAD Y PROCESAMIENTO DE INFORMACIÓN.

1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Analizar e investigar las mejores soluciones para el manejo correcto de la información de bonos de vivienda en el MIDUVI, en cuanto a la seguridad y administración de datos.
- ✓ Determinar el software de monitoreo de red para evaluar el nivel de seguridad en que se encuentra la información.
- ✓ Identificar los mayores riesgos y amenazas que existen en el mundo exterior y que ponen en peligro la información existente en el MIDUVI.
- ✓ Analizar el rendimiento de los servidores que almacenan y donde se procesa toda la información de bonos de vivienda.
- ✓ Desarrollar una aplicación web utilizando software libre para facilitar el proceso de consulta de postulantes y beneficiarios de bonos de vivienda.
- ✓ Determinar las aplicaciones más seguras y más confiables en el manejo de la información que existen actualmente.
- ✓ Presentar los resultados obtenidos utilizando las herramientas necesarias para dar a conocer las mejores alternativas que pueden ser implementadas.

1.4. JUSTIFICACIÓN

La información sobre la gestión y control de bonos de vivienda que procesa el Ministerio de Desarrollo Urbano y Vivienda es de vital importancia para los nuevos sistemas que se van a implementar a futuro por parte de diferentes instituciones encargadas de los programas sociales que se realizan en el Ecuador.

Es por esto que el presente proyecto surge con la necesidad de proteger y administrar de mejor manera la información que se encuentra actualmente en el ministerio. Además que dicha información está expuesta a que personas con mala intención puedan modificar o alterar los registros de los bonos de vivienda que se adjudicaron anteriormente en el MIDUVI.

Las bases de datos que se manejan en la institución se encuentran segmentadas, es decir, que no se maneja un concepto de base de datos centralizada con tablas relacionadas, en la cual se alojen los registros de beneficiarios de bonos de vivienda. Como se dijo anteriormente el sistema mono usuario que se utiliza para la calificación de los postulantes que aplican al bono que otorga el ministerio no permite centralizar en una sola base de datos todos los beneficios que la institución ofrece al pueblo ecuatoriano.

De la misma manera toda esta información no se encuentra protegida adecuadamente, ya que no existen ningún tipo de políticas de seguridad como por ejemplo, un plan de contingencia y respaldo de los datos, además la falta de un control de acceso de usuarios a los registros de bonos de vivienda.

Luego de reorganizar la información y proponer un plan de seguridades que ayude al control efectivo de los registros y datos que se encuentran dispersos en las direcciones provinciales del MIDUVI, se llegará a tener en el edificio matriz una sola base de datos que pueda responder a todos los pedidos por parte de otras instituciones y de esta manera la información generada servirá para los diferentes sistemas y aplicaciones que existen en la actualidad.

1.5. DESCRIPCIÓN DEL PROYECTO

El plan de protección y administración propuesto, comprenderá dos subtemas principales, los cuales son: la seguridad y protección de la información y el correcto manejo y administración de la misma. Esto quiere decir que no solo se evaluará las posibles fallas y amenazas a las que está expuesta la información confidencial de bonos de vivienda en el MIDUVI, sino que además se planteará una mejor solución en la administración de los datos mediante alternativas de seguridad, respaldo de datos, reestructuración de la información y desarrollo de interfaces de consulta y control de la gestión de proyectos de vivienda.

Para lo cual se debe seguir un proceso que defina primeramente los principales problemas que tiene la institución en cuanto a los recursos de información, identificando las posibles causas del mal manejo de la misma, así como las amenazas y vulnerabilidades existentes con la ayuda de software de escaneo como Nmap, Netcat o Nessus y de esta manera llegar a plantear un plan de seguridad como solución al problema.

Para verificar el nivel de protección que brindan los servidores que alojan la información importante de bonos, se pretende evaluar y analizar el tráfico de la red, utilizando software especializado, que permitirá visualizar las principales vulnerabilidades existentes y de esta manera proponer una mejor alternativa para prevenir ataques de sniffers, rastreadores, spoofing, scanners de puertos, etc.

Como alternativa de protección a la información importante que maneja el MIDUVI, se analizará y sugerirá las mejores soluciones en cuanto a respaldos de información para la gestión y control de bonos de vivienda, con la cual se manejará backups y restauración de datos.

Para lograr un mejor manejo de la información, se desarrollará una aplicación web que permitirá consultar, actualizar y emitir reportes de bonos de vivienda que otorga el MIDUVI, la cual acogerá los estándares y normas que exige el gobierno actual, es decir, será desarrollado con herramientas de software libre y además que cuente con un nivel considerable de seguridad en los datos.

Para la parte de base de datos se utilizará MySQL ya que este motor de base de datos ofrece una flexibilidad, adaptación y protección de datos elevada la cual servirá al momento de unificar toda la información que posee el MIDUVI en cuanto a bonos de vivienda.

El servidor Web será Apache, ya que éste es de libre distribución y no tiene costo en la adquisición inicial.

Para el desarrollo se utilizará PHP 5, ya que presenta muchas ventajas como el manejo de clases y objetos, a diferencia de la versión 4 que presenta problemas en la ejecución.

Esta aplicación contará con dos módulos principales los cuales son:

1. Interfaz de consulta de bonos de vivienda.
2. Aplicativo del control de gestión de proyectos de vivienda.

El primer módulo comprenderá una interfaz amigable al usuario, que podrá ser accedida desde el portal del MIDUVI y permitirá realizar consultas sobre el bono de vivienda.

El segundo módulo será de uso exclusivo de personal de la subsecretaria de vivienda, con el fin de controlar de mejor manera la gestión de los proyectos de vivienda.

Este aplicativo será instalado en los servidores que posee el ministerio y servirá para poder evaluar el nivel de seguridad que presta en cuanto al procesamiento de información. Se utilizará software espías, de intrusión y escaneo de datos para verificar el nivel de seguridad que posee, y de esta manera realizar las respectivas observaciones y recomendaciones que se deberían tomar en cuenta al desarrollar aplicaciones web seguras.

Con el fin de poseer servidores capaces de responder rápidamente a peticiones será de gran utilidad evaluar la potencialidad de la virtualización, como nueva tecnología, que permita trabajar con información centralizada en un solo equipo y con varias aplicaciones ejecutándose al mismo tiempo.

Para efecto de trabajar conjuntamente con instituciones externas que trabajan con programas sociales, se deberá ejecutar el plan de reestructuración de la información de acuerdo al análisis correctivo y apoyándose en normas estandarizadas, que permitan corregir los errores que presentan las bases de datos existentes, para de esta manera lograr consolidar la información de bonos de vivienda urbano, rural y urbano marginal de los años 2007, 2008, 2009 y 2010 que no tienen un mismo formato y que no poseen códigos de acuerdo a la División Política Administrativa (DPA) para las ubicaciones geográficas en el Ecuador.

2. CAPÍTULO: SEGURIDAD EN LA RED Y PROTECCIÓN DE LA INFORMACIÓN.

La seguridad en una red merece en la actualidad una atención especial, ya que es necesario y de vital importancia conocer las vulnerabilidades a las que puede estar expuesto un sistema conformado por un conjunto de computadoras que trabajan con información confidencial en una institución.

Muchas de las vulnerabilidades son el resultado de una implementación incorrecta de tecnologías, otras son consecuencia de la falta de planeamiento de las mismas, pero la mayoría de los agujeros de seguridad son ocasionados por los propios usuarios que utilizan los sistemas incorrectamente.

2.1. CONCEPTOS GENERALES DE SEGURIDAD

2.1.1. ELEMENTOS DE SEGURIDAD

Confidencialidad

Se refiere a la privacidad de los elementos de información, almacenados y procesados en un sistema informático. Garantizar que solo personas autorizadas accedan a los datos.

Las herramientas de seguridad informática deben proteger a los sistemas de intrusiones, escaneos y accesos no autorizados.

Integridad

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Es decir, que se pueda asegurar que la información en procesos de actualización esté sincronizada y no sea duplicada, alterada, borrada, reordenada, etc., bien durante el proceso de transmisión o en el propio equipo local.

Disponibilidad

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

Es decir, que la información pueda ser recuperada en donde las herramientas de seguridad informática deben reforzar la permanencia de los datos para que los usuarios accedan y utilicen los recursos con cualquier frecuencia requerida.

Seguridad de la Información

Se refiere a todas aquellas acciones que se enfoquen al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de los elementos de información, así como la continuidad de las operaciones ante un evento que las interrumpa.

Al referirse a seguridad de información se identifica un conjunto de elementos para controlar y salvaguardar este recurso generado por sistemas, software de desarrollo y por programas en aplicación.

Activo

Se refiere a todos aquellos recursos con los que cuenta una empresa o institución y que tiene valor, éstos pueden ser tangibles (servidores, desktop, equipos de comunicación) o intangibles (información, políticas, normas, procedimientos).

Vulnerabilidad

Es la exposición a un riesgo, fallo o problema de seguridad detectado en cualquier aplicación o software que maneje recursos de información.

Generalmente son detectados o encontrados por intrusos y atacantes de sistemas informáticos, provocando desastres y daños irreparables.

Amenaza

Cualquier situación o evento posible con potencial de daño, que pueda presentarse en un sistema informático.

Riesgo

Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto.

2.2. SEGURIDAD DE ACCESO A LA RED

La seguridad del acceso a redes de información es vital en cualquier sistema, ya que se debe proporcionar un total control sobre los usuarios y host que se conectan entre sí para evitar intrusiones que puedan afectar a la red.

Es posible implantar reglas de acceso a la red muy refinadas. Se pueden definir varias reglas y políticas de acceso como por ejemplo un usuario A no puede conectarse a la red, el usuario B debe utilizar una determinada máquina o PC para conectarse y un usuario C puede conectarse libremente desde cualquier lugar que desee.

De esta manera se puede restringir el acceso a usuarios no autorizados que intenten ingresar libremente a los sistemas y aplicaciones que manejan información importante de una empresa o institución.

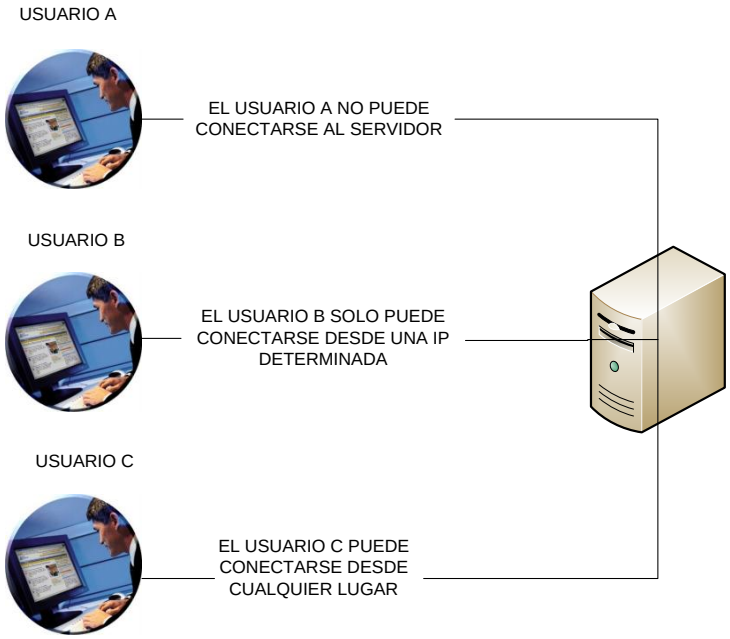


Figura 2.1: Control de acceso de los usuarios.
Fuente: Autor de tesis.

Esta funcionalidad viene muy bien en los entornos de red o cuando se trabaja con un servidor de internet por ejemplo, ya que permite mantener un servidor que realice funciones especificas para cada perfil de usuario.

2.2.1. CONTROL DE ACCESO

Un punto central es el control de acceso, que permite controlar el grado hasta que los usuarios pueden acceder a los archivos y directorios en uno o varios sistemas. Es decir, es permitir o denegar el acceso a diferentes aplicaciones y lugares que procesen información.

Si se presenta un ejemplo, se diría que es posible especificar con total exactitud la forma en que distintos usuarios acceden a los mismos archivos y directorios. Un usuario A podría tener el permiso de lectura, escritura y ejecución para varios archivos. De la misma manera un usuario B solo podrá leerlos y escribir en ellos, y finalmente un usuario C no tendrá permisos de lectura, es decir, no podrá siquiera acceder a ellos.

Si las empresas u organizaciones se dividen en departamentos o direcciones y que es posible que varios usuarios de dichos departamentos tengan que acceder a los mismos archivos. Los sistemas operativos actuales permiten agrupar a estos usuarios. De esta forma, cuando se definen permisos para determinados archivos y directorios, no es necesario hacerlo para todos y cada uno de los usuarios.

Si se presente un ejemplo donde un grupo A tiene acceso solo a escritura, mientras que un grupo B tiene acceso a lectura y escritura. Dicha gestión a nivel de grupo resulta muy útil cuando hay muchos usuarios y varios grupos de usuarios necesitan privilegios idénticos o muy parecidos.

2.3. CRIPTOGRAFÍA Y CONTRASEÑAS

Desde hace mucho tiempo atrás, con el nacimiento de los computadores el hombre vio la necesidad de utilizar algún método para proteger la información, pero la primera evidencia concreta de esto, se encuentra en el antiguo Egipto. Cuando un egipcio importante moría, las personas trabajadoras preparaban su cuerpo mediante la momificación. Luego lo enterraban con pergaminos que portaban frases del Libro de los Muertos.[2]
En estos pergaminos los sacerdotes escribían contraseñas secretas que permitían al fallecido comprar su entrada en el cielo.

La mayoría de las contraseñas no estaban cifradas. En su lugar, los sacerdotes confiaban en el destino, jugando con que el fallecido alcanzaría el cielo antes de que los ladrones de tumbas lo descubran. De todo esto, lo que se sabe es que aproximadamente 2000 años A.C, los egipcios empezaron a usar contraseñas de texto sin formato. En los siguientes 1000 años, los egipcios lograron desarrollar una criptografía rudimentaria.

2.3.1. CRIPTOGRAFÍA

La palabra criptografía viene de 2 antiguas palabras: Krypto (oculto) y graphia (escritura), por lo tanto, la criptografía es la ciencia de escribir en forma secreta para lograr cifrar y descifrar información mediante técnicas especiales, se emplea para permitir un intercambio de mensajes que solo pueden ser leídos y entendidos por personas a las que van dirigidos, y que poseen los medios para descifrarlos.
La criptografía al inicio se lograba al realizar una mezcla de los componentes de los datos a ser cifrados, donde los caracteres eran simplemente reordenados. Más tarde, se utilizaron cifrados por sustitución, con fórmulas sencillas para convertir de manera uniforme cada carácter en otro.

[2] Libro de los Muertos: una colección de sortilegios o fórmulas mágicas que se incluían en las tumbas del Reino Nuevo, y pretendían ayudar al difunto en su difícil camino al Mas Allá.

Actualmente los cifrados por sustitución simple existen, pero ya no se utilizan para ocultación de datos. Los simples cifrados por sustitución son demasiado rudimentarios para proteger datos. De ahí que durante varios siglos, y en los últimos 100 años, los investigadores han desarrollado muchos tipos de cifrado diferentes.

2.3.1.1 Tipos de Criptografía:

- Criptografía simétrica

Este tipo de cifrado emplea una clave única para cifrar y descifrar el mensaje. El emisor cifra el mensaje con la clave y el receptor descifra el mensaje usando la misma clave. El único requisito previo es que ambas partes deben conocer dicha clave. Es un algoritmo de cifrado muy rápido, pero plantea dos inconvenientes, el primero es que la clave común debe ser enviada por un canal seguro y el segundo inconveniente es que debe ser mayor de 40 bits para que sea robusto.

- Criptografía asimétrica o de clave pública

Este tipo utiliza un par de claves para el envío de mensajes cifrados.
Existe una clave pública y una clave privada. La clave pública es conocida por todos y la clave privada solo por el propietario, y permanece siempre en secreto. Es más lento en proceso que las claves simétricas y los mensajes resultantes son de mayor tamaño.

- Criptografía de Curva elíptica CCE

Este tipo es una variante de la asimétrica y en lugar de usar la matemática de los números primos para generar las claves de cifrado, utiliza curvas elípticas.

- Criptografía híbrida

Es una combinación de cifrado simétrico y asimétrico. Utiliza una clave pública para cifrar el mensaje en el que envía una clave para el cifrado simétrico.
Para darle mayor seguridad la clave simétrica, es diferente para cada sesión.

2.3.2. DATA ENCRYPTION STANDAR (DES)

Data Encryption Standar (DES) es el cifrado más popular de muchos años, a pesar que solo tiene 25 años.
Esta forma de encriptación nace a principios de los años 70, cuando el gobierno de los EEUU, carecía de un método de codificación estandarizado para un uso más general. Muchas empresas desarrollaron propuestas, pero la que ganó fue la de IBM. El DES de IBM fue objeto de rigurosas pruebas y, en 1977, la National Bureau of Stándar la apoyaron. Desde entonces este algoritmo tomado fuerza en los últimos años, aunque en la actualidad existen otros y más poderosos tanto para sistemas UNIX-Linux como Windows.

Funcionalmente, DES es un cifrado de bloque, que trabaja sobre bloques de datos de un tamaño determinado (64 bits). Los bloques de datos que superan este tamaño se dividen en fragmentos de 64 bits. Las porciones restantes inferiores a 64 bits se rellenan. Cuando se habla de rellenar se refiere a que DES puede añadir bits sin significado a partes mas pequeñas para conseguir un bloque completo.

A partir de esta instancia, DES emplea tres operaciones importantes, la primera de las cuales es la permutación inicial. En este proceso, los bits de datos se desplazan a otras posiciones en una tabla. Sigue un proceso de transformación con la ayuda de complicadas operaciones matemáticas con el fin de crear un bloque de presalida. Y para finalizar, al bloque se le aplica otra permutación mas y el resultado final es el texto mezclado, al que a veces se lo denomina texto cifrado, pero es más conveniente llamarlo texto codificado.

2.3.3. CIFRADO EN INFORMACIÓN CONFIDENCIAL

Además de una administración centralizada y del control de acceso a redes, los sistemas deben proporcionar más mecanismos de protección, en este caso se refiere al cifrado de datos.

Se define a cifrado como el proceso de mezclar datos para que no puedan ser leídos por agentes no autorizados. En la mayoría de los esquemas de cifrado, es necesario tener una contraseña para reorganizar los datos de forma que puedan leerse. El cifrado se utiliza para efectos de privacidad y protección de información importante.

Habitualmente cuando se transmiten datos a través del internet, atraviesan varias pasarelas o gateways, que en su camino los datos son vulnerables a escuchas electrónicas. Es por esto que se busca tener opciones y utilidades complementarias que permitan cifrar o codificar los datos para que si alguien los captura, solo pueda ver signos raros o de caracteres especiales de difícil entendimiento.

Si un usuario desea utilizar una tarjeta de crédito, el proceso empezará cifrando los datos antes de salir de su red interna y permanecerá así hasta que el servidor de comercio logre descifrarla para utilizar el código y así realizará la transacción. Este proceso protege a los datos de ataques y posibilita un comercio electrónico seguro, algo que está obrando cada vez mayor importancia.

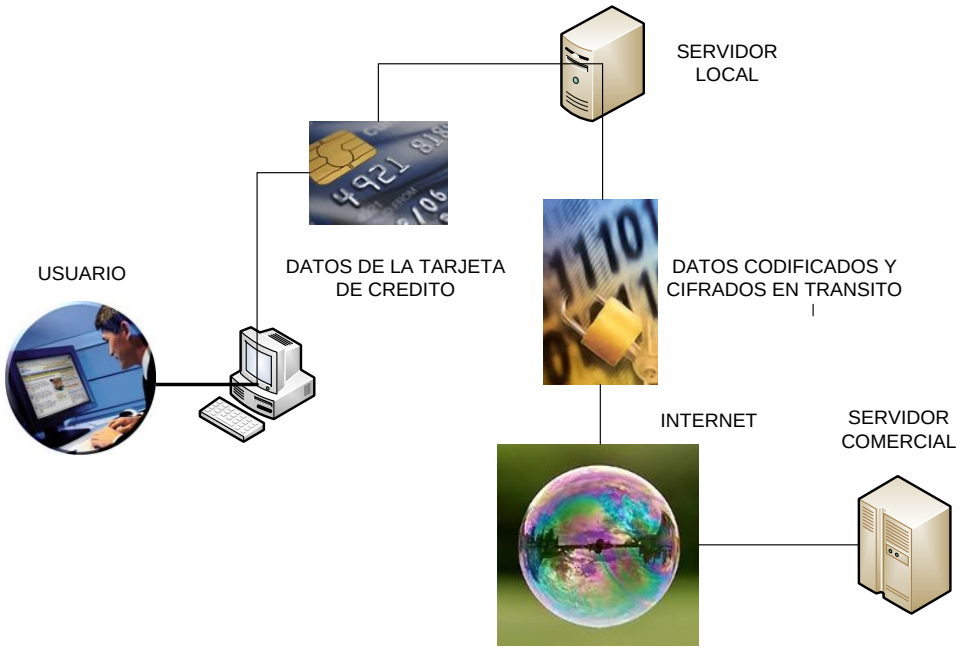


Figura 2.2: Conexión para cifrado de datos.
Fuente: Autor de tesis.

2.3.4. GENERACION Y ALMACENAMIENTO DE CONTRASEÑAS

Una parte esencial de un sistema seguro consiste en poseer las más fuertes medidas de seguridad en los datos e información, esto se logra protegiendo el acceso con las denominadas contraseñas.

La seguridad de la contraseña es tan importante que sin ella ningún sistema podrá ser seguro. Es posible instalar un grupo de potentes firewalls y, aun así, si las contraseñas son fácilmente descifrables y vulnerables, el sistema sería una puerta abierta.

Se puede enfocar en dos niveles de seguridad de contraseñas: Por un lado hay que aplicar herramientas avanzadas para reforzar la contraseña. Por el otro, es necesario educar a los usuarios para inculcar políticas de prevención básicas.

La generación y almacenamiento de contraseñas en sistemas actuales tienen que ver directamente con la distribución o sistema operativo que se instalará a lado del servidor.

Por ejemplo, si se tiene una distribución Linux, los usuarios se guardarán en /etc/passwd, lo que no resultaba seguro, ya que este directorio es y debe ser legible, en la siguiente figura se muestra el anterior fichero.

$cat /etc/passwd

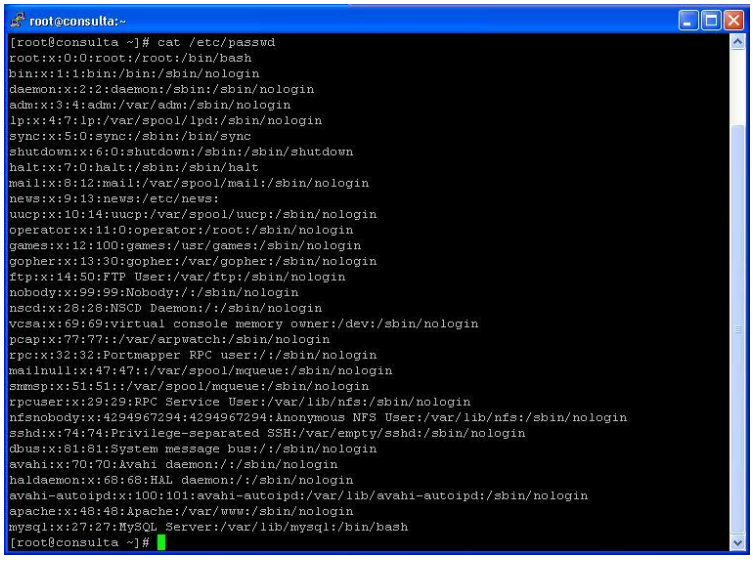


Figura 2.3: Información del archivo "passwd", que contiene información de contraseñas en Linux. Fuente: Autor de Tesis.

2.4. NIVELES DE SEGURIDAD

Utilizando el estándar más utilizado propuesto por TCSEC Orange Book[3] los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.
Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).
Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

2.4.1. NIVEL D: PROTECCIÓN NULA

Este nivel contiene solo una división y ha sido reservado para sistemas que luego de ser evaluados no cumplen con ninguna especificación de seguridad. Son sistemas no confiables, no existe protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a usuarios y sus políticas de acceso a la información.

Ejemplos: MS-DOS, System 7.0 de Macintosh.

2.4.2. NIVEL C1: PROTECCIÓN DISCRECIONAL

Aparece la identificación de usuarios, con lo cual permite el acceso a información variada pero especifica. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene el control total de acceso.

Ejemplos: Linux 1.0 posterior a Minix, Primeras versiones de Unix.

Muchas de las tareas de administración del sistema solo pueden ser realizadas por este “súper usuario” quien tiene gran responsabilidad en la seguridad del mismo. Los requerimientos mínimos para cumplir la clase C1 son:

[3] El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Acceso de control discrecional.- existe una distinción entre usuarios y recursos. Se podrán definir grupos de usuarios y grupos de objetos sobre los cuales podrán actuar los usuarios o grupos de ellos. Se define un mecanismo de control y acreditación, así como la capacidad de hacer cumplir las restricciones de acceso de una base individual, es decir, garantizar de una forma convincente a los usuarios de que sus proyectos o información privada está protegida y evitar que otros usuarios accidentalmente puedan leer o destruir sus datos.[4]

Identificación y autentificación.- en este nivel se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre cualquier sistema, existe un mecanismo de protección y de control de acceso, en el cual se genera una tabla de control para los usuarios entrantes. En este punto es vital la utilización de contraseñas para autenticar la identidad del usuario y lograr un nivel más alto de confiabilidad. Además se debe establecer restricciones a usuarios no autorizados que quieran acceder al sistema.

2.4.3. NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las principales debilidades del C1. Posee un ambiente de acceso controlado ya que incorpora características adicionales. Se debe llevar una auditoría de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aun más el que los usuarios ejecuten ciertos comandos o tengan accesos a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no solo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema, logrando llevar un registro de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

[4]Acceso de control discrecional: Tomado del Libro Naranja, página. 9, NIVELES DE SEGURIDAD.

Los usuarios de un sistema C2 tiene la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Además permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Ejemplos: Sistemas posteriores de Unix, VMS, MAC OS 9.

2.4.4. NIVEL B1: SEGURIDAD ETIQUETADA

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

Ejemplos: Mac OS X 10.0, rPath de Ret Hat

2.4.5. NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios. El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

Ejemplos: Sistemas como Multics de Honeywell, XENIX, Windows 95

2.4.6. NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.
Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones.

Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Ejemplos: Federal System de Honeywell, XTS – 200, Windows Vista, Ubuntu

2.4.7. NIVEL A: PROTECCIÓN VERIFICADA

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

Ejemplos: Honeywell Information System SCOMP, Boeing Aerospace: SNS, Qubes basado en Fedora.

3. CAPÍTULO: SEGURIDAD FÍSICA.

3.1. GENERALIDADES Y COMPONENTES.

3.1.1. REDES DE INFORMACIÓN.

Una red de información es aquel sistema en el cual los elementos que la componen, son autónomos y están conectados entre sí por algún medio físico y/o lógico, y que además pueden interactuar y comunicarse entre sí para compartir recursos. Al hablar del concepto de una red, se establece una diferenciación entre el concepto de red física y red de comunicación.

Respecto a los componentes físicos, conexión física o flujos de datos se sabe que la constituyen dos o más equipos computadores que comparten determinados recursos, hardware o software. Desde una perspectiva más comunicativa, se puede decir que una red aparece cuando se encuentran involucrados algún componente humano, un componente tecnológico y un componente administrativos por ejemplo: persona – PC – institución.

De cualquier modo, se dice que una red a más de varios computadores conectados, la constituyen varias personas que solicitan y presentan requerimientos, que podrán ser intercambiadas y procesadas a través de los sistemas de comunicación.

3.1.1.1. COMPONENTES

Los componentes de una red, no son más que todos los recursos o elementos que conforman e interactúan con la red.

Servidor.- aquel o aquellos computadores que van a compartir recursos hardware y software con los demás equipos de red. Son potentes, con grandes capacidades de almacenamiento y procesamiento.

Estación de trabajo.- son aquellos computadores que toman un papel de equipos de trabajo o tienen a su disposición los recursos que ofrece la red.

Gateways o pasarelas.- es aquel hardware y software que permite que se conecten dos redes locales entre sí. Se lo puede relacionar como un túnel o puente que conecta servidores y estaciones de trabajo.

Tarjeta o placas de interfaz de red.- se le denomina NIC (Network Interface Card). Su función principal es la de intermediario entre el computador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de red.

El medio.- se constituye por el cableado y los conectores que enlazan los componentes de red.

Concentradores del cableado: son conexiones hacia las estaciones que distribuyen las conexiones al concentrador como un único dispositivo centralizado.

3.1.2. ESTRUCTURA Y CLASIFICACIÓN DE REDES.

3.1.2.1. ESTRUCTURA

La estructura de una red se compone de tres tipos:

- **Software de Aplicaciones**

Son los programas que actúan como intermediarios entre las PCs y los usuarios de red, permiten compartir recursos e información.

- **Software de red**

Son los programas que establecen protocolos para que las PC se comuniquen unas con otras. Estos protocolos son los que permiten que interactúen enviando y recibiendo datos, también denominados paquetes.

- **Hardware de red**

Son los equipos o componentes materiales que unen las PCs. Entre los más importantes se describe el medio de transmisión que transporta las señales a las PC (cables o fibras ópticas) y el adaptador de red, que permite el acceso al equipo.

3.1.2.2. LAS REDES SEGÚN SU UTILIZACIÓN:

Redes Compartidas, aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión.

Redes exclusivas, aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

3.1.2.3. LAS REDES SEGÚN SU ESTRUCTURA:

Redes privadas, aquellas que son gestionadas por personas particulares, empresa u organizaciones de índole privado, en este tipo de red solo tienen acceso los terminales de los propietarios.

Redes públicas, aquellas que pertenecen a organismos estatales y se encuentran abiertas a cualquier usuario que lo solicite mediante el correspondiente contrato.

3.1.2.4. LAS REDES SEGÚN LA COBERTURA DE SERVICIO:

Redes LAN (Local Area Network), Redes MAN (Metropolitan Area Network), Redes WAN (Wide Area Network), Redes internet y las redes inalámbricas.

3.1.3. TOPOLOGÍAS DE RED.

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

- Topologías físicas.

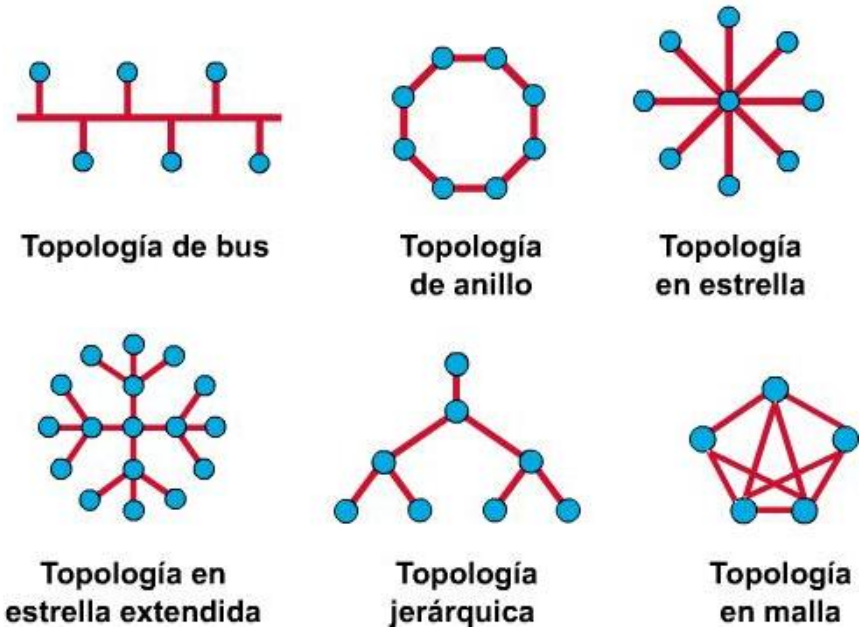


Figura 3.1: Topologías físicas de red.
Fuente: http://yainy.net/

- Topologías lógicas

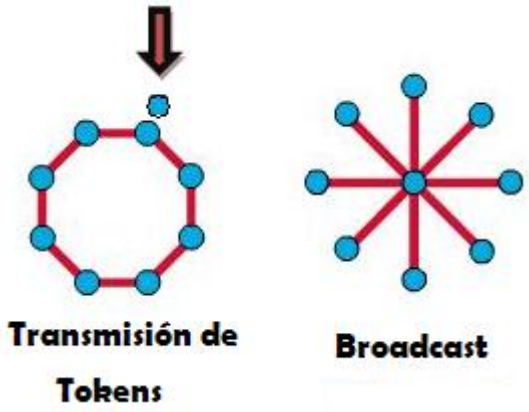


Figura 3.2: Topologías lógicas de red.
Fuente: http://yainy.net/

3.1.4. SEGURIDAD EN LAS TOPOLOGÍAS DE RED.

La base de una red LAN es la topología o arquitectura utilizada, ya que cada topología tiene sus ventajas y aspectos de seguridad que los arquitectos de redes deben tomar en cuenta cuando diseñan su esquema o distribución de red.

La topología de red se compone de la distribución de red, componentes y la forma que se conectan entre sí. Dado que la topología de red determina el modo en que se conectan los dispositivos hardware y la forma en que fluye la información a través de dichas conexiones, tiene claras implicaciones de seguridad detalladas en los siguientes puntos.

3.1.4.1. RIEGOS AL ELEGIR UNA TOPOLOGÍA DE RED:

Punto único de fallo: es un elemento (Servidor, Hub, Router) al que se conectan uno o varios dispositivos de red. Si uno de estos dispositivos falla, una o varias estaciones de trabajo perderán la conexión a la red. La tarea consistirá en minimizar los efectos de los puntos de fallo, es decir, llevar un control de daños.

Susceptibilidad de "escucha electrónica": es la práctica de captura oculta del tráfico de red. Todas las topologías son susceptibles de sufrir escuchas electrónicas, aunque algunas son más susceptibles que otras.

Tolerancia a Fallos: es la capacidad de la red para recibir todo ataque posible y seguir trabajando sin percances. Si falla una, dos o más estaciones de trabajo, la red debería seguir funcionando para ser considerada con tolerancia a fallos.

Resumiendo lo anterior, al momento de escoger una topología de red, hay que tener presente que la topología bus y anillo no presentarían mucha seguridad, ya que existe un punto único de fallo, por lo que no sería recomendable trabajar en este ambiente.

Si la red es grande, se puede dividirla en segmentos, para permitir de esta manera una mejor gestión y mayor control al limitar hasta dónde puede llegar un fallo de seguridad.

Tratar de aislar el hardware y cableado de los usuarios para prevenir intervenciones encubiertas de red.

3.1.4. PROTOCOLOS DE RED

Un protocolo de red son una o más normas que especifican el método de enviar y recibir datos entre elementos de una red. Su instalación está en correspondencia con el tipo de red y el sistema operativo que la computadora tenga instalado.
Existen varios protocolos de red, y es posible que en un mismo ordenador coexistan instalados uno de ellos. La variedad de protocolos puede suponer un riesgo de seguridad, cada protocolo de red que se instala en un sistema queda disponible para todos los adaptadores de red existentes en dicho sistema, físicos o lógicos.
Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no deseado a los recursos de la red. En estos casos, la regla de seguridad más sencilla es tener instalados el número de protocolos indispensable; en la actualidad y en la mayoría de los casos debería bastar con sólo TCP/ IP.

La clasificación de protocolos se los distingue de la siguiente forma:

Protocolos de red:

- DDP (Delivery Datagram Protocol)
- IP (Internet Protocol)
- IPX (Internet Packed Exchange)
- NetBEUI Desarrollado por IBM y Microsoft.

Protocolos de transporte:

- ATP (Apple Talk Transaction Protocol)
- NetBios/NetBEUI
- TCP (Transmission Control Protocol)

Protocolos de aplicación:

- FTP (File Transfer Protocol)
- Http (Hyper Text transfer Protocol)

3.2. SEGURIDAD Y CONTROL FÍSICO DEL HARDWARE.

La seguridad física puede abarcar varios aspectos, generalmente se centra en la seguridad en la red, aunque es importante tomar en cuenta este punto, no se debe olvidar de la seguridad en los servidores que muchas veces pueden ser más vulnerables a ataques físicos que a los remotos.
De hecho, no solo es más probable que ataquen a un servidor con un hacha que mediante una utilidad de spoofing o sniffers, sino que cuando esto ocurre, los efectos posteriores pueden ser mucho más devastadores y más cuando la información que se aloja en el equipo es realmente importante y confidencial. Además si lograr alterar un sistema de forma remota, se podría reiniciar o reinstalar, pero si ha sido dañado o puesto en peligro físicamente, el problema si sería muy serio.

Es por esto, que la seguridad física debe estar en primer lugar como objetivo a proteger. Pese a que muchas medidas de seguridad física parecen obvias, generalmente los usuarios pocas veces las aplican.

Se debe actuar cuidadosamente con los siguientes elementos:

- Ubicación del hardware y su acceso físico.
- Control de acceso a los servidores.
- Control de acceso al hardware de red.
- Contraseñas de BIOS y consola.
- Controles biométricos de acceso.

3.2.1. UBICACIÓN DEL SERVIDOR Y SU ACCESO FÍSICO.

Existen dos aspectos importantes para este punto: el primero es el lugar en que se encuentra ubicado el servidor y el segundo son las personas que tienen acceso físico al mismo.
No existirá ningún control de seguridad si aquellas personas que tienen acceso físico al equipo piensan en acciones malintencionadas y dañinas.
Existen una gran cantidad de ataques generados de esta forma.

Un ataque, puede significar muchas cosas en este contexto. Si por ejemplo se permite que un usuario malintencionado se quede solo durante 30 segundos, es muy probable que estos sufran daños importantes en ese intervalo de tiempo. El usuario podría realizar un simple ataque de denegación de servicio[5] desconectando cables, desconectando hardware de red o simplemente reiniciando los equipos.

Estas situaciones pueden darse muy pocas veces, ya que estudios han estimado que el 80 % de las intrusiones provienen del personal interno. El motivo es que este personal tiene acceso a información que los agresores externos no podrían obtener.

En muchas instituciones del estado, los empleados de confianza pueden acceder libremente a estos recursos y muchas veces a la información que no cuenta con las debidas seguridades del caso. La pregunta sería:

¿Cómo se puede proteger un sistema frente a los enemigos internos?

Por tal motivo una gran alternativa sería crear o adecuar un centro de operación de red, que no es más que un sitio seguro con una infraestructura adecuada, construida específicamente para alojar este tipo de equipos, donde el acceso sea restringido con claves y llaves de acceso solo a personas autorizadas.

3.2.2. CONTROL DE ACCESO A LOS SERVIDORES

Para lograr una buena seguridad física es cuestión de sentido común y análisis de los peligros más comunes que pueden darse. Siempre que sea posible, se debe tratar de implementar todas las medidas de seguridad prescritas por el fabricante de los equipos de hardware y elementos que componen la red.

La vigilancia en particular de las contraseñas predeterminadas y similares es un buen hábito para aumentar el nivel de seguridad en la empresa o institución. El tener una contraseña común por un rango de tiempo prolongado produce que

[5] Denegación de Servicio se refiere a dejar inoperativo al servidor de forma malintencionada provocando que usuarios legítimos no accedan a los servicios que provee.

alguien pudo haberla extraído y está haciendo uso inadecuado de esta, provocando en varios casos fallos de funcionamiento y errores en la red.

Poseer equipos de red relativamente nuevos, hace que sea fácil localizar documentación en la web para cualquier recomendación o tipo de seguridad. El hardware antiguo de red puede albergar defectos.

En conclusión la mejor manera de controlar la seguridad física es tomando las precauciones posibles para evitar que usuarios no autorizados accedan físicamente a los servidores o al hardware de red.

3.2.3. CONTROL DE ACCESO AL HARDWARE DE RED

Un tema de vital importancia es la seguridad en el hardware de red, ya que implica un mantenimiento y control adecuado de cada uno de los componentes que permiten a las PC formar un conjunto de equipos que interactúan compartiendo recursos.

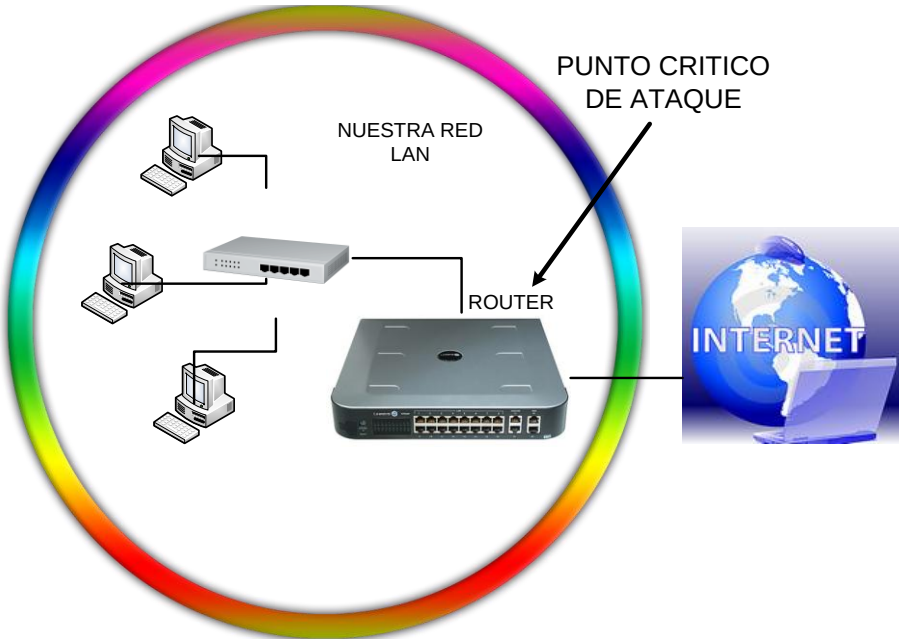


Figura 3.3: El hardware de red o router como punto crítico de ataque desde mundo exterior.
Fuente: Autor de tesis.

Uno de los elementos más críticos en una red podría ser el router, un blanco de ataque atractivo, ya que éste dispositivo cumple con varias funciones y además sirve de pasarela a través de la que los usuarios de red pueden comunicarse con el mundo exterior y viceversa. Si los agresores consiguen colapsar o desconfigurar los routers u otros dispositivos importantes el servicio de red, estará inactivo para mucha gente.

PROBLEMAS HABITUALES CON CONTRASEÑAS EN EQUIPOS DE RED		
3COM	SWITCH	El login (debug) y la contraseña (synnet) de mantenimiento de varios switches 3 Com. Por ejemplo CoreBuilder y Super Stack II
ERICSSON	ROUTER	Algunos routers Ericsson Tigris permiten a usuarios remotos enviar comando de validación sin autenticarlos.
BAY NETWORKS	ROUTER	Algunos equipos de esta marca tienen una cuenta sin contraseña. Esta información ha sido muy distribuida y conocida.

Tabla 3.1: Problemas comunes con contraseñas en equipos de red.
Fuente: Autor de tesis.

Asegurar un aislamiento del hardware de red de usuarios locales, que generen desconfianza y que puedan dañar o alterar el correcto funcionamiento de cada equipo de red. Si un usuario no controlado que tenga acceso físico a los equipos logra recuperar alguna contraseña de un router, switch o bridge, no tardará en empezar a manipular incorrectamente los mismos provocando serios problemas.

Por esta razón, al momento de instalación de equipos nuevos en la red se debe tomar las siguientes recomendaciones:

- Definir correctamente las contraseñas de administración, de mantenimiento y de los usuarios para evitar que agresores puedan acceder a través de valores predeterminados o comunes en las contraseñas de la empresa o institución.

La mayoría de routers y switches admiten algún tipo de cifrado, pero no emplean por defecto. Trate de que se tenga presente el cifrado.

Una buena práctica sería desactivar el control remoto de administración (telnet), en caso que fuese necesario podría activarlo temporalmente. Si el hardware de red posee puertos sensibles, bloquear el acceso a ellos sería recomendable.

3.2.4. CONTRASEÑAS DE BIOS Y CONSOLA

Las arquitecturas más comunes utilizan contraseñas de BIOS-PROM, contraseñas de consola o de ambos tipos. Estos tipos de contraseña son incluidos como un filtro extra de seguridad, como un obstáculo para disuadir a los usuarios audaces de curiosear.

Las contraseñas de la BIOS o de la PROM evitan que los usuarios malintencionados accedan a la configuración del sistema, mientras que las contraseñas de consola protegen los perfiles de usuario de la estación de trabajo o PC. En cualquier de los dos casos, estas contraseñas ayudan de manera especial al control efectivo de accesos sin autorización.

Sin embargo, hay que tener cuidado de no obviar establecer las contraseñas de configuración y de usuario, ya que si no se hace, entraría en un problema peor y sería mucho más lamentable.
Actualmente las teclas y contraseñas predeterminadas de configuración de la BIOS de casi todos los fabricantes son muy conocidas. Aquí se muestran algunas de ellas.

TECLAS Y CONTRASEÑAS CONOCIDAS	
AMERICAN MEGATRENS	Incluye AMI y AMI_SW
AWARD	Incluye 589589, Award, AWARD
TECLAS GENERICAS	Incluye F1,F3,Ctrl+F1,Ctrl+F3, Ctrl+Mayus+Esc,Supr,Ctrl+Alt+S
IBM APTIVA	Presionando repetidamente los dos botones del raton durante el arranque
TOSHIBA	Algunos modelos pueden obviar la contraseña manteniendo pulsada la tecla Mayus

Tabla 3.2: Tabla resumen de teclas y contraseñas conocidas según el fabricante.
Fuente: Autor de tesis.

Asegurarse también de que las contraseñas no coincidan con otras que se utilicen comúnmente, esto garantizará que si rompen la contraseña de la BIOS o de consola, las otras estaciones y PC no estarán expuestas a otro ataque.
Pero lo más recomendable, es no fiarse de estas contraseñas como una seria defensa ya que tiene efectos inherentes, como un jumper para borrar la CMOS o provocando un cortocircuito de la batería de la placa.

3.2.5. CONTROLES BIOMÉTRICOS DE ACCESO

Se piensa como una idea futurista de seguridad física del hardware en el uso de dispositivos de acceso biométrico. Estas herramientas autentican a los usuarios en base a características biológicas como: estructura facial, huellas dactilares, patrones de retina, voz, etc.

Este tipo de control no siempre será el más adecuado, por las reacciones sociales que pueden generar. Por ejemplo, los empleados de una institución pueden ofenderse de este control y pueden considerarlos una violación a la intimidad.
Los controles de acceso biométricos no son adecuados para entornos que van más allá de una red local. La utilización de este tipo de acceso sería aconsejable dentro de las oficinas en aquellas máquinas que se usen para el control y administración de la red.

HERRAMIENTAS DE ACCESO BIOMÉTRICO	
SERVICIO	DESCRIPCIÓN
BIOMOUSE	Es un ratón de American Biometric, que lee bien huellas digitales. Es compatible con Linux 2.0
IRIS SCAN	Es un sistema de autenticación biométrica en red que admite 256 estaciones de trabajo en segmentos de red LAN.
SECURE START ISA	Es un sistema de autenticación por huella digital de I/O Software que autentica a los usuarios antes de arrancar. Incluye un analizador de huellas digitales compacto.
VERIVOICE	Este sistema comprueba su identidad mediante el reconocimiento de voz, ademas es compatible con Linux 2.0 o posterior.

Tabla 3.3: Tabla resumen sobre las principales herramientas de acceso biométrico.
Fuente: Autor de tesis.

3.3. ATAQUES Y PROTECCIÓN DE LA INFORMACIÓN

3.3.1. ATAQUES DE CONTRASEÑAS

Cuando se habla del término ataque de contraseña se refiere a un término genérico. Esto describe diversas formas y tareas entras las que se incluye cualquier acción dirigida a romper, alterar, borrar contraseñas o a la vez evadir de otra forma los mecanismos de seguridad de las contraseñas.
En orden jerárquico, los ataques de contraseña son lo primero a romper en un sistema. Los piratas e intrusos de la red aprenden a romper contraseñas antes que cualquier otra actividad. Actualmente, cualquier persona con conocimientos básicos puede romper contraseñas si sabe utilizar de forma adecuado las herramientas automatizadas.

Pero no se debe confundir la sencillez con la ineficacia, en la mayoría de los casos, una deficiente seguridad en las contraseñas pone en peligro a todo el sistema. Los atacantes que inicialmente obtiene solo acceso limitado pueden extender y ampliar el acceso mediante el ataque a una seguridad de contraseña débil.

3.3.2. PRINCIPALES HERRAMIENTAS Y FORMAS DE ATAQUE

- **TCP Wrappers**

Los TCP Wrappers son una de las herramientas más famosas del mundo para reforzar el control de acceso a la red.

Este tipo de aplicación brinda una capa adicional en cuanto a la seguridad de la red y sistemas de información. Si bien es cierto que se aplica mas en sistemas UNIX / Linux, también se lo puede utilizar en otros sistemas como Windows por ejemplo.

Las brillantes capacidades de TCP Wrappers no deben considerarse una alternativa a un buen firewall. TCP Wrappers puede utilizarse conjuntamente con un cortafuegos u otro sistema de seguridad, pues ofrece varios servicios adicionales que brindan una protección extra a los sistemas.

Para un control más avanzado en cuanto a seguridad utilizando esta herramienta, se pueden configurar las opciones para tener un mayor control sobre la gestión de conexiones. En algunos casos puede convenir el envío de un comentario a ciertos equipos o conexiones de servicios. En otros, tal vez se deba registra una entrada en un log o enviar información de lo ocurrido al administrador. Otro tipo de situaciones pueden requerir el uso de un servicio solamente para conexiones locales.

Para concluir, el servicio de TCP Wrapers es lo más parecido a la funcionalidad del firewall que puede conseguir sin hacer uso de un filtro de paquete a escala total, y es una opción perfecta cuando no se pueda utilizar un firewall, pero necesita control de acceso a la red.

- **IPFwadm**

La herramienta Ipfwadm permite el filtrado de paquetes, además se utiliza para configurar, mantener e inspeccionar el firewall y las normas de cuenta en el kernell de Linux.

Para una utilidad tan pequeña, ipfwadm es más que suficiente y, por qué no, podría ser una formidable solución de firewall personal.

Al analizar la herramienta de forma general, ipfwadm permite establecer normas estrictas sobre el tráfico entrante y saliente.

En un ejemplo para sistemas Linux se procedería de la siguiente manera:

Ipfwadm [rule_category] [policy_action] [policy] [interface] [target]

La categoría de la normas es el tipo de norma que se esta definiendo y si se aplica a la cuenta, tráfico entrante, saliente, normal, no filtrado o tráfico enmascarado. La normativa es lo que quiere hacer con el tráfico especificado: aceptarlo – negarlo – rechazarlo.

El objetivo es la dirección IP a la que está aplicando estas normas.

Otras opciones de Ipfwadm

Esta herramienta soporte muchas más opciones que se lo detalla a continuación:

PARAMETRO	FUNCION
-b	Se utiliza para aplicar la normativa actual tanto al trafico entrante como al saliente. Sirve para cuando se adjunte, inserte o borre una normativa.
-e	Se utiliza para obtener una salida más extensa
-m	Se utiliza para especificar que os paquetes que vienen bajo la normativa actual, estarán enmascarados como si vinieran del host local.
-n	Se utiliza para especificar que ipfwadm debería mostrar toda la información en formato numérico (direcciones IP y NO nombres de host).
-o	Se utiliza para activar el logging en todos los paquetes que vengan bajo la normativa actual.
-r [puerto]	Se utiliza para redirigir los paquetes hacia un socket local.
-v	Se utiliza para obtener una salida amplia.

Tabla 3.4: Tabla resumen con las principales funciones en la utilización de IPfwadm.
Fuente: Autor de tesis.

3.3.3. COPIAS DE SEGURIDAD

Las copias de seguridad son vitales para la protección de la información, al hablar de un plan de contingencia se seguridad informática se refiere a los pasos que se deben seguir, luego de un desastre, para recuperar la información y además la capacidad de funcionalidad de los sistemas.

La recuperación y restauración de información se refiere a la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido algún problema, así como la posibilidad de volver al estado anterior del mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información.

Es así, que la recuperación de la información se basa en el uso de una política de copias de seguridad o Backup adecuado.

El Backup de archivos permite tener disponible y de manera integra la información para cuando sucedan ciertos accidentes. Sin un Backup, simplemente, es imposible volver la información al estado anterior al desastre.
La falta de concientización de los usuarios en este sentido es muy alta. Más allá de lo que cabe esperar, un alto porcentaje de usuarios y personas que utiliza información sabe lo que es un Backup o copia de seguridad pero nadie sabe cómo hacerlo, o peor aun saben cómo hacerlo pero nadie lo hace.

Los motivos para esto son muy variados pero siempre se puede concluir que hacer una copia de seguridad es molesto, involucra tiempo, y a veces resulta complicado seguir al pie de la letra los pasos que se necesitan para obtener un Backup favorable.

Para realizar un Backup funcional que permita recuperar información importante luego de un desastre se debe tomar varias recomendaciones y consejos que pueden ayudar a una recuperación más satisfactoria.
Cuando se pretenda realizar una copia de seguridad se debe tomar las siguientes precauciones:

- Realizar copias en disquetes o cintas que pueden estar dañados.
- Realizar copias en CDs de baja calidad, lo barato sale caro.
- Realizar backups parciales pensando en que lo demás ya está respaldado.
- Realizar backups cada 6 meses más o menos.
- Realizar backups y guardarlo en un lugar seguro.

Hacer un Backup no es una tarea trivial, involucra recursos y costos que generalmente ni los usuarios finales ni las empresas consideran.

Las posibilidades para realizar un Backup son muchas, si bien unas más adecuadas que otras según se considere el caso:

- Se puede realizar una simple copia con el viejo y conocido copy / cp de DOS / UNIX.

- Se puede grabar en algún medio removible (Disquete, CD, Flash memory)
- Se puede copiar en algún equipo espejo del original.
- Se puede subir la información a hostings de la web.
- Se puede crear una tarea programada que envíe el Backup por correo.

No se debe pasar por alto que la copia de seguridad se la haya realizado correctamente, es recomendable realizar comprobaciones periódicas cada cierto tiempo prudencia para asegurar que el proceso se completo satisfactoriamente.

En lo que respecta a empresas, las acciones a realizar son un poco más complejas, pero el concepto es el mismo: hacer Backup es ahorrar tiempo y dinero.
En este caso será necesario realizar un análisis costo/beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el Backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura / escritura, tiempo de Backup, etc.
3. El almacenamiento de los Backups se deben realizar en lugares diferentes de donde se encuentra la información original. Con esto se evita la pérdida si el desastre abarca todo un edificio por ejemplo.
4. La verificación de la integridad de los respaldos de información se debe realizar periódicamente y no se debe esperar hasta el momento en que ocurre el desastre, problema o pérdida de información.

5. Se debe contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
6. Es importante tener una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Encriptar antes de respaldar.
7. Se debe mantener equipos de hardware, de características similares a los utilizados para el proceso normal, que puedan suplantar a los originales y puedan comenzar a procesar en caso de desastres físicos.

3.3.4. FIREWALLS

Un firewall es un dispositivo que evita que ingresen extraños en una red. Es un direccionador, una computadora autónoma con filtro de paquetes o software proxy, o un paquete de firewall.

Este dispositivo puede ser hardware como software, según la aplicación que se le quiera dar, además puede servir como punto de entrada único a un sitio, normalmente llamado punto de estrangulamiento. A medida que se reciben las peticiones de conexión, el firewall las va evaluando. Sólo se procesan las peticiones de conexión de los hosts autorizados; el resto de peticiones son descartadas.

Los firewalls realizan varias tareas, como por ejemplo:

- Filtro y análisis de paquetes. Los firewall pueden analizar paquetes entrantes de múltiples protocolos. Basándose en ese análisis, estos equipos pueden realizar evaluaciones condicionales.
- Bloqueo de protocolos y contenidos. Los firewall le permiten proteger contenidos. Pueden explotar esta capacidad para bloquear sentencias scripts que ejecutan acciones como java, javascript, vbscrip, activex y otras más.

- Creación de normas para bloquear Firmas de Ataques[6] particulares.
- Autenticación y encriptación de usuario, conexión y sesión. Muchos firewall utilizan varios algoritmos y sistemas de autenticación (DES, Triple DES, SSL, SHA, MD5, IDEA, etc.) para verificar la identidad de sus usuarios, comprobar la integridad de la sesión y proteger los datos en tránsito de los rastreos.

Como conclusión, dependiendo del diseño, un firewall protege a la red al menos en dos de estos niveles (y en algunos casos en todos):

1. ¿Quién puede entrar?
2. ¿Qué puede entrar?
3. ¿Dónde y cómo pueden entrar?

En el sentido más técnico, un firewall es la suma total de todas las normas que se puedan aplicar a una red. Generalmente un firewall proporcionará normas que reflejen la normativa de acceso de la propia organización.

3.3.4.1. FIREWALL A NIVEL DE RED

Son aquellos direccionadores con capacidad de filtro de paquetes. Al utilizar un firewall a nivel de red, puede permitir o negar el acceso a su sitio basándose en varias variantes, como pueden ser:

- Dirección de fuente
- Protocolo
- Número de puerto
- Contenido

Los firewall, basados en direccionadores son populares porque son soluciones de perímetro, es decir, son dispositivos externos.

[6] Las firmas de ataque son patrones de comando comunes a un ataque en particular.

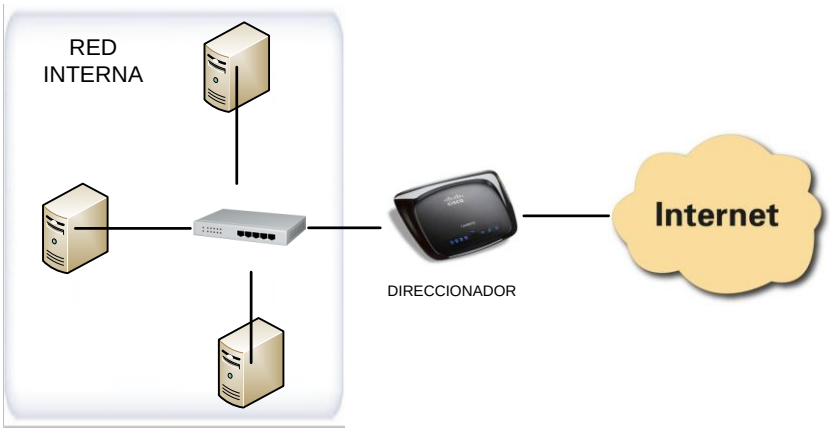


Figura 3.4: Diagrama que muestra el equipo direccionador como la única entrada desde el exterior. Fuente: Autor de tesis.

Aquí se puede apreciar que todo el tráfico exterior debe pasar a través del direccionador, que manipula todos los procedimientos de aceptación y negación. Estos firewall ofrecen una solución limpia y rápida gracias a que son de sistema operativo y neutral en cuanto a la aplicación.

Además, los firewall basados en direccionadores avanzados[7] pueden vencer al spoofing y a los ataques DoS, e incluso convertir a la red en invisible para el mundo exterior.

Como todo dispositivo y equipo, poseen fallos y deficiencias. Algunos direccionadores son vulnerables a algunos ataques.

3.3.4.2. PASARELA DE APLICACIONES

El otro tipo importante de firewall es el de aplicación-proxy, llamado pasarela de aplicación. Estas sustituyen a las conexiones entre los clientes externos y su red interna. Durante este cambio nunca se envían paquetes IP. En su lugar se realiza una traducción, actuando como pasarela de conducto y se interprete.

[7] Firewalls con direccionadores: Son enrutadores que incorporan un sistema de filtro de paquetes y su arma más eficaz es la navegación oculta, disfrazando las direcciones y puertos.

Además con este tipo se logra tener un control más global sobre cada uno de los servicios individuales, y en muchos casos puede mantener la información del estado del paquete.

De la misma forma, este también tiene algunas deficiencias, una de estas es que requieren una implicación substancial por su parte porque deben configurar aplicaciones proxy para cada servicio de red. Además, los usuarios internos deben utilizar clientes que estén al tanto del proxy, caso contrario deberán adoptar nuevas normativas y procedimientos.

Un ejemplo de este tipo es el Firewall Tool kit (FWTK). Es un paquete de uso no comercial, que incluye proxies para los siguientes servicios:

- Telnet, FTP, rlogin, sendmail, y http.

3.3.4.3. EVALUACIÓN DE UTILIZACIÓN DE FIREWALL

Para que una empresa o institución implemente un equipo firewall debe primeramente analizar la factibilidad y necesidad que posee. Hay muchos entornos en los que los firewalls no son adecuados:

Universidades.- ya que las universidades a menudo la dirigen 2 o más departamentos que se convierten en segmentos de red separados, lo que conlleva a ofrecer un acceso limitado a los estudiantes.

Proveedores de servicio de internet (ISP).- ya que los usuarios acceden a sus cuentas desde diferentes puntos y sitios de conexión, es muy difícil determinar y controlar la procedencia de cada dirección IP con la cual se conectan.

A mas de esto, el compromiso de manejar, gestionar y administrar un firewalls es realmente grande, si se piensa en tener un servidor web con páginas publicitarias no sería aconsejable implementar este servicio. Los firewall son más adecuados para proteger redes privadas que necesitan acceso de salida a internet y ofrecen al público entrada mínima y un control estricto.

3.3.5. CÓDIGO DAÑINO

El denominado código dañino es un proceso codificado dentro de un programa legal, que realiza acciones que el usuario desconoce y probablemente no lo desea. También puede definirse como un programa legal que ha sido modificado insertando en él código no autorizado que ejecuta funciones desconocidas.
Este código generalmente esta creado para permanecer oculto y enmascarado para que no pueda ser fácilmente detectado, produciendo funciones no deseadas por el usuario.

Existe una variedad de código dañino que se encuentra en los sistemas actuales de información, los cuales son:

Residentes: son aquellos que se ocultan en la memoria RAM de forma permanente o residente.

Acción directa: no pertenecen en memoria y su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutado.

Sobreescritura: su característica es que destruyen la información de los ficheros que afectan.

Boot: estos no afectan los ficheros, sino los discos que los contienen.

Macro: infectan los ficheros creados usando determinadas aplicaciones que contengan macros.

Enlace o directorio: aquellos que alteran las direcciones que indican donde se almacenan los ficheros.

Encriptados: son aquellos que cifran o encriptan a sí mismos para no ser detectados y poder ejecutar las acciones por los que fueron creados.

Polimórficos: los que en cada infección que realizan se cifran de una forma distinta, así es más difícil detectarlos.

Multipartes: estos pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Actúan sobre archivos, programas, macros, discos, etc.

Fichero: principalmente infectan programas o ficheros ejecutables, existen en mayor cantidad.

Compañía: son virus de tipo residente y de acción directa, su característica es que acompañan a otros ficheros existentes en el sistema antes de su llegada.

FAT: actúan sobre la tabla de asignación de ficheros, ya que impiden el acceso a ciertas partes el disco, donde se almacenan los ficheros críticos.

Gusanos(Worms): los gusanos se limitan a realizar copias de sí mismos a la máxima velocidad posible, su acción se enfoca en saturar o colapsar los sistemas o redes en donde se infiltran.

Troyanos: técnicamente no se deben considerar virus, ya que no se reproducen infectando otros ficheros. Tampoco se propagan haciendo copias de sí mismo, pero si son detectados por los antivirus para su eliminación, ya que el fin y objetivo básico es la introducción e instalación de otros programas en el ordenador, para permitir su control a través de equipos remotos.

Bombas lógicas: no se podrían considerar estrictamente virus, ya que no se reproducen, pero su objetivo es destruir los datos del sistema o PC.

Virus falsos: existen ciertos tipos de mensajes o programas que son confundidos como virus, pero no son más que mensajes de correo engañosos que llegan masivamente a los destinatarios sin procedencia conocida.

VIRUS DE OTROS SISTEMAS

Los virus de Mac se pueden clasificar en:

1. **Infectores específicos de sistemas y archivos Mac.**

Ejemplos:

a. AIDS.- infecta aplicaciones y archivos de sistema.
b. CDEF.- infecta archivos del escritorio.

2. **Infectores HiperCard.**

Ejemplos:

a. Dukakis.- despliega el mensaje Dukakis para presidente.
b. MerryXmas. - En ejecución infecta el sector de inicio de la memoria, que a su vez infecta otros sectores en uso. Esto ocasiona caída del sistema y otras anomalías.

3. **Mac Trojans.**

Ejemplos:

a. ChinaTalk.- parecería un controlador de sonido, pero borra carpetas.
b. CPro. - supuestamente es una actualización de Compact Pro, pero intenta dar formato a los discos montados.

4. **Macro virus.**

Virus que manejan cadenas de texto en un documento, pueden trabajar igual en una Macintosh como en una PC. Desde que Word 6.x para Macintosh soporta macros, es vulnerable a ser infectado por este virus. Cualquier aplicación para Macintosh que soporte Visual Basic también será vulnerable.

Ejemplo:

a. W97M/Remplace.b.- Consiste de 17 macros en un módulo llamado akrnl. Utiliza un archivo temporal c:\Étudiant.cfg para copiar su código. Desactiva la protección de Macro Virus, deshabilita las opciones de Macros, Plantillas y Editor de visual Basic.

3.4. AGENTES EXTERNOS

En el anterior punto se hizo referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su falta de prevención.

3.4.1. DESASTRES NATURALES

TERREMOTOS

Los terremotos son el desastre natural menos probable en la mayoría de organismos e instituciones en el Ecuador, si se compara con otros países donde por la localización geográfica se podrían producir temblores o terremotos de intensidad considerable con mucha más frecuencia.

Los terremotos no suelen alcanzar la magnitud necesaria para causar daños en los equipos y hardware, por lo tanto, no se suelen tomar las medidas necesarias contra los movimientos sísmicos, ya que la probabilidad de que sucedan es tan baja que no mecere la pena invertir dinero para minimizar sus efectos.

De cualquier forma aunque algunas medidas contra terremotos son excesivamente caras para la mayor parte de instituciones, no cuesta nada tomar ciertas medidas de prevención, por ejemplo:

Es muy recomendable no situar los equipos delicados en superficies muy elevadas, aunque tampoco a ras del suelo, ya que el problema aquí sería si existe una inundación. Si no se cumple con esta recomendación un pequeño temblor puede tirar desde una altura considerable un complejo hardware, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente utilizar fijaciones para los elementos más críticos, como CPUs, monitores o los routers. De la misma forma,

tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el hardware.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos grandes cerca de las ventanas, ya que en algún caso podrán caer por ellas, causando pérdida total de la información e incluso podría aparecer un problema mayor, un posible accidente a otra persona a la cual le puede caer encima ese objeto o pieza de algún equipo.

TORMENTAS ELÉCTRICAS

Las tormentas con aparato eléctrico, generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica. Si cae un rayo en una estructura metálica de un edificio donde están situados servidores y equipos es casi seguro que se debería pensar en comprar otros o sustituirlos; la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir el hardware incluso protegido contra voltajes elevados.

Este problema posee una ventaja, y es que las tormentas pueden ser predecibles con más o menos exactitud, lo que permite a un administrador detener el funcionamiento de los servidores y desconectarlas de la línea eléctrica. La caída de un rayo es algo poco probable, pero no imposible que suceda, es por esto que son muy pocos administradores los que se molestan en detener las máquinas y desconectarlas previniendo que sus equipos sufran los estragos de la naturaleza.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad, almacenándolas lo más alejado posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas las cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de los sistemas.

INUNDACIONES Y HUMEDAD

Cierto grado de humedad es necesario para un correcto funcionamiento de los equipos informáticos, en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que puede provocar un daño irreparable en el hardware y a la información.

Por otro lado, niveles de humedad elevados son perjudiciales para los equipos ya que pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Poder controlar el nivel de humedad en los entornos de trabajo de servidores y equipos que alojan información importante es algo necesario, para la protección de los datos. Ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de los equipos más críticos e indispensables. Una alternativa es utilizar alarmas que se activen al detectar condiciones de muy poca o demasiada humedad, especialmente un sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Al punto extremo, si se llega a producir una inundación, los problemas generados son mucho mayores. Casi cualquier medio (computadores, discos, routers, servidores) que entren en contacto con el agua quedan automáticamente inutilizados, bien por el líquido o por el cortocircuito que se genera.

Ciertamente, contra las inundaciones las medidas más efectivas son las de prevención, con la utilización de detectores de agua en los suelos o falsos suelos del cuarto de servidores y a la vez con el apagado de los equipos y sistemas. Además puede existir un proceso para cortar la corriente mediante un sistema automático.

Algo común hacer frente a este problema, es tratar de sacar los equipos, previamente apagados o no, de la sala que está empezando a inundarse, a primera vista parece lógico efectuar esta acción para tratar de salvar la información, pero lo cierto es que es el mayor error que se puede cometer si no se

ha desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte de la persona.

Otro error común relacionado con los detectores de agua es situar a los mismos a un nivel superior que a los propios equipos a salvaguardar, evidentemente cuando en estos casos el agua llega al detector poco se puede hacer ya por las máquinas y la información que contienen.

Una medida de protección menos sofisticada podría ser la instalación de un suelo falso por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación con respecto al suelo, cuidando de no situarlos en lugares muy altos por los problemas que pueden aparecer si se producen terremotos y vibraciones.

3.4.2. DESASTRES DE ENTORNO

ELECTRICIDAD

Tal vez los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta los equipos; cortapicos, picos de tensión y cortes de flujo, a diario amenazan la integridad tanto del hardware como de los datos que se almacenan en estos equipos.

Un problema muy habitual y común en las instalaciones modernas son las subidas de tensión, a conocidos como “picos” porque generalmente duran muy poco y que normalmente apenas afectan al hardware o datos gracias a que la mayoría de equipos actuales vienen diseñados para soportar este incremento de tensión. Una medida efectiva de protección sería la utilización de conexiones a tierra, este mecanismo evita los problemas de sobretensión desviando el exceso de corriente hacia el suelo de un edificio o institución, o simplemente hacia cualquier lugar con voltaje nulo.

Un problema que los estabilizadores de tensión o las tomas de tierra no pueden solucionar es las bajas de tensión, en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema, pero sin llegar

a ser lo suficientemente bajo para que la máquina se apague. En estas situaciones el equipo se comportará de forma incorrecta, por ejemplo no acepta algunas instrucciones, tampoco completa todas las escrituras en disco o memoria, etc.

La forma más efectiva de proteger los equipos y hardware contra problemas de la corriente eléctrica es utilizar un SAI(Servicio de Alimentación Interrumpido), instalado en el cuarto de equipos y servidores. Estos dispositivos mantienen un flujo correcto y estable de corriente, protegiendo de los altos y bajas de tensión. Es así que este sistema puede ser implementado para que una máquina se conecte al SAI y a través de un software reciba información y se puedan conocer cuánto tiempo de corriente queda antes de que se apague completamente.

Como último punto se debe mencionar un problema que ni siquiera la SAI protege a los sistemas y equipos, este es, la corriente estática, un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos, sólo a las personas.

Nada más lejos de la realidad, simplemente tocar con la mano la parte metálica del teclado o un conductor de una placa puede destruir un equipo completamente. Se trata de un tipo de corriente de muy poca intensidad pero con un nivel demasiado alto de voltaje, por lo que aunque la persona no sufra ningún daño, el equipo sufre una descarga que puede ser suficiente para destrozar sus componentes. Existen algunas soluciones como por ejemplo: spray antiestático, ionizadores antiestáticos, manillas, etc. Aunque en la mayoría de situaciones solo hace falta de un poco de cuidado y sentido común al momento de manipular estos equipos.

RUIDO ELÉCTRICO

Este problema no es una incidencia directa de la corriente en los equipos, sino una incidencia relacionada con la corriente de otros dispositivos que pueden afectar al funcionamiento los computadores o servidores. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros computadores o equipos electrónicos, y se transmite a través del espacio o

de líneas eléctricas cercanas a las instalaciones donde se encuentran los servidores de información.

Para prevenir que el ruido eléctrico dañe los equipos informáticos, se podría intentar no situar el hardware cercano a la maquinaria que puede causar dicho ruido, si no existe otra alternativa que hacerlo, se puede instalar filtros en las líneas de alimentación que llegan hasta los computadores. Es recomendable mantener alejados de los dispositivos emisores de ondas,, como celulares, transmisores de radio, walkie-talkies, etc; ya que pueden influir directamente en elementos de detección de incendios o algunas alarmas.

INCENDIOS Y HUMO

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo. Un simple cortocircuito o un equipo que se recalienta demasiado pueden convertirse en la causa directa de un incendio en un edificio, o al menos en la planta, donde se encuentra toda la información vital para una empresa.

Una solución efectiva contra los incendios y el humo son los extintores instalados en el techo, que se activan automáticamente al detectar humo o calor. Los más antiguos, expulsaban agua para apagar el incendio, luego se fabricaron aquellos que arrojan una solución de halón; este compuesto no conduce la electricidad ni deja residuos, lo que resulta ideal para no dañar los equipos pero contamina gravemente el medio ambiente y es solución toxica para las personas. Los extintores de dióxido de carbono son los que reemplazan a los de halón, ya que son menos contaminantes y menos perjudiciales, pero no precisamente sano para las personas.

En muchos manuales de seguridad se habla de que los usuarios, administradores y personal en general debe intentar controlar el fuego y salvar el equipamiento y la información, esto tiene, sus pros y contras. Pero se debe analizar muy bien el ambiente con el cual se enfrentará cada persona, si es un incendio de pequeñas dimensiones, tal vez con la ayuda de un extintor se pueda solucionar el problema, pero si las dimensiones de las llamas son considerables lo último que se debe hacer es tratar de controlar el fuego por si solos, en esta situación no importa el

precio de los equipos o el valor de la información, nunca será tan importante como la vida humana.

TEMPERATURAS EXTREMAS

Las temperaturas extremas, tanto calor como frio elevado, perjudican gravemente a los equipos que se posea. La temperatura recomendable para que puedan operar sin ningún inconveniente y en condiciones normales varía entre 10 y 32 grados Celius[8].

Para poder controlar la temperatura ambiente en el entorno de operaciones es aconsejable un acondicionador de aire, este dispositivo ayudará enormemente para mantener la temperatura adecuada para los servidores y de esta manera responderán de mejor manera y trabajarán mucho mejor los sistemas.

Otra condición básica para el correcto funcionamiento de los computadores, es que cuenten con el sistema de ventilación en buen estado, sin elementos que obstruyan los ventiladores el CPU, ya que esto puede ocasionar el sobrecalentamiento de los discos duros, procesador, memorias, etc.

[8] El grado Celsius, símbolo ºC, pertenece al sistema internacional de unidades, creada por Anders Celsius, esta escala es muy utilizada para expresar las temperaturas de uso cotidiano.

4. CAPÍTULO: HERRAMIENTAS PARA LA INTRUSIÓN EN UNA RED.

4.1. INSTRUSIÓN Y DEFACING BÁSICO DE UNA WEB

4.1.1. QUÉ ES DEFACING BÁSICO.

El defacing o intrusión consiste en aprovechar uno o varios bugs (errores), en un servidor web, con el fin de alterar o investigar los componentes que en éste se encuentran.

Para realizar una primera prueba de defacing a una página web con altas opciones de vulnerabilidad se utilizarán algunos comandos comunes y algunos tips para lograr ingresar en la página sin previa autorización logrando encontrar las principales fallas de programación y seguridad.

4.1.2. VULNERABILIDAD DEL COMANDO DE REDIRECCIÓN.

El siguiente comando pude ser ingresarlo en un textbox de la página web vulnerable a este comando, lo que se logra al realizar esta acción es redirigir a la página indicada en el tag de URL como muestra la figura.

<meta http-equiv="REFRESH" content="1; URL=***pagina_a_redireccionar***">

Ejemplo:

Para el ejemplo se utilizará una página vulnerable, en la cual existe un textbox para las búsquedas, en este espacio se precede a ingresar la siguiente línea y provocará que luego de 1 segundo se dirigirá a la página que muestra la URL.

<meta http-equiv="REFRESH" content="1;URL=../contenido.php?cd=2554">

Figura 4.1: TextBox vulnerable a javascript. Fuente: Página protegida por seguridad.

4.1.3. VULNERABILIDAD DEL COMANDO “alert()”.

El comando alert(); es utilizado en JavaScript conjuntamente con algún lenguaje de programación en ambiente WEB, de la misma manera se puede ingresar el comando en un textbox de la página vulnerable, para tener acceso a propiedades que permitirán la utilización de Javascript.

<script>alert(“TEXTO”);</script>

Ejemplo:

Para el ejemplo utilizará la misma página, en la cual existe un textbox para las búsquedas, en este espacio se precede a ingresar la siguiente línea y provocará una alerta con el botón Aceptar.

<script>alert(“VULNERABLE A JAVASCRIPT”);</script>

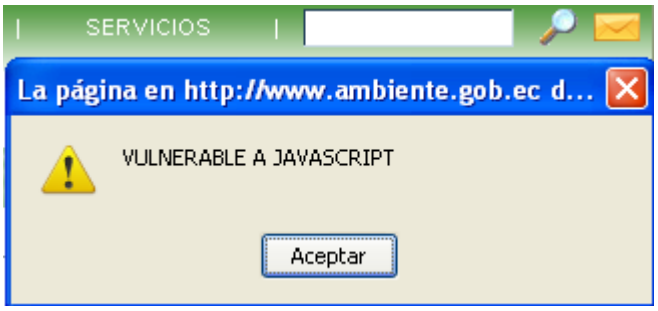


Figura 4.2: Mensaje de alerta donde presenta la vulnerabilidad a javascript.
Fuente: Autor de tesis.

4.2. SQL INJECTION PARA EL ACCESO NO AUTORIZADO

4.2.1. QUÉ ES SQL INJECTION.

SQL Injection en la actualidad es una forma muy común y no tan avanzada del ingreso a páginas web sin autorización. Este método consiste en poder modificar el comportamiento de las consultas SQL normales, con la introducción de caracteres o parámetros no deseados en los campos permitidos y que tiene acceso un usuario externo.

La mayoría de vulnerabilidades que se puede encontrar en una determinada página web se identifica en aquellas donde necesitan un login de ingreso, en otras palabras, donde exista un textbox para el ingreso de un usuario y otro para el password.

4.2.2. CAPTURANDO PETICIONES UTILIZANDO ACHILLES.

El método post en un formulario web sirve para procesar peticiones de envío de datos. La característica principal del método es que los parámetros de petición se encuentran en el cuerpo de la petición, a diferencia del método GET que lo envía codificada en la URL.

Ejemplo URL método POST:

http://savmiduvi.miduvi.gov.ec/seguimientobono/emision_matriz.php

Ejemplo URL método GET:

http://savmiduvi.miduvi.gov.ec/miduvibono/index.php?errorusuario=1

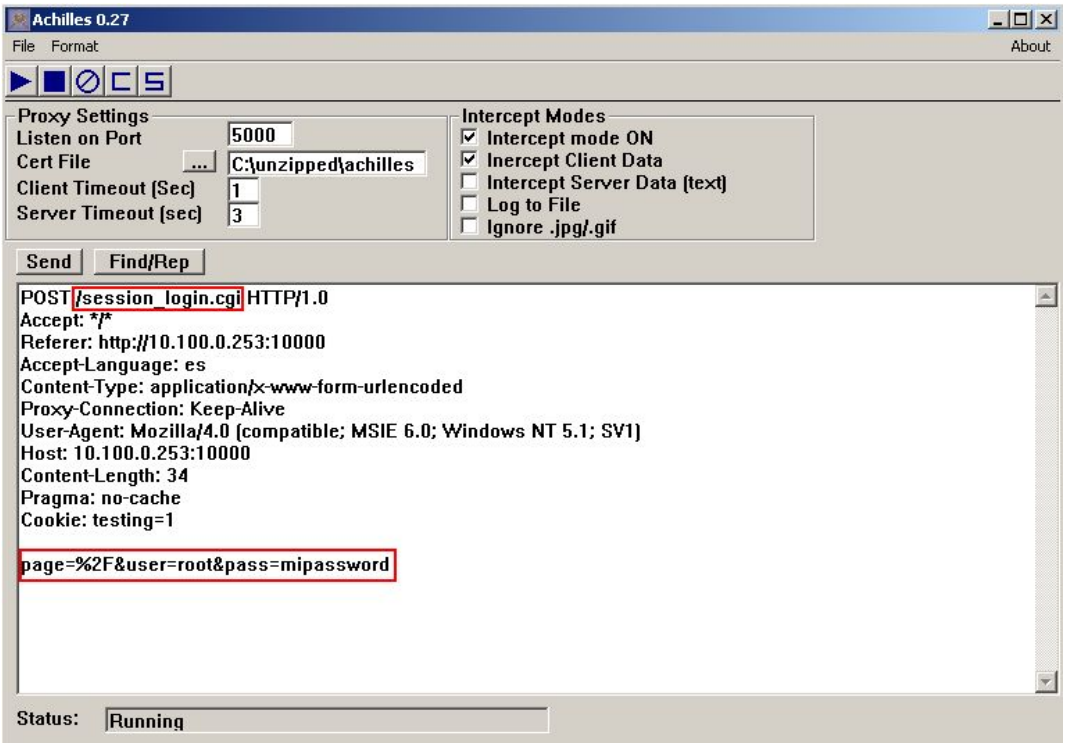


Figura 4.3: Proxy Achilles capturando datos a la dirección 10.100.0.253:10000
Fuente: http://www.juanfelipe.net/files/pictures/achilles.jpg

Ejemplo:

Luego de configurar el número de puerto y los modos de intercepción en Achilles, proxy local, se procederá a ingresar a la web que se desee obtener información valiosa y a la vez que sirva para capturar o interceptar algún dato importante que pueda ayudar en los ataques de SQL injection posteriores.

Dirección Web: **http://savmiduvi.miduvi.gov.ec/seguimientobono/index.php**

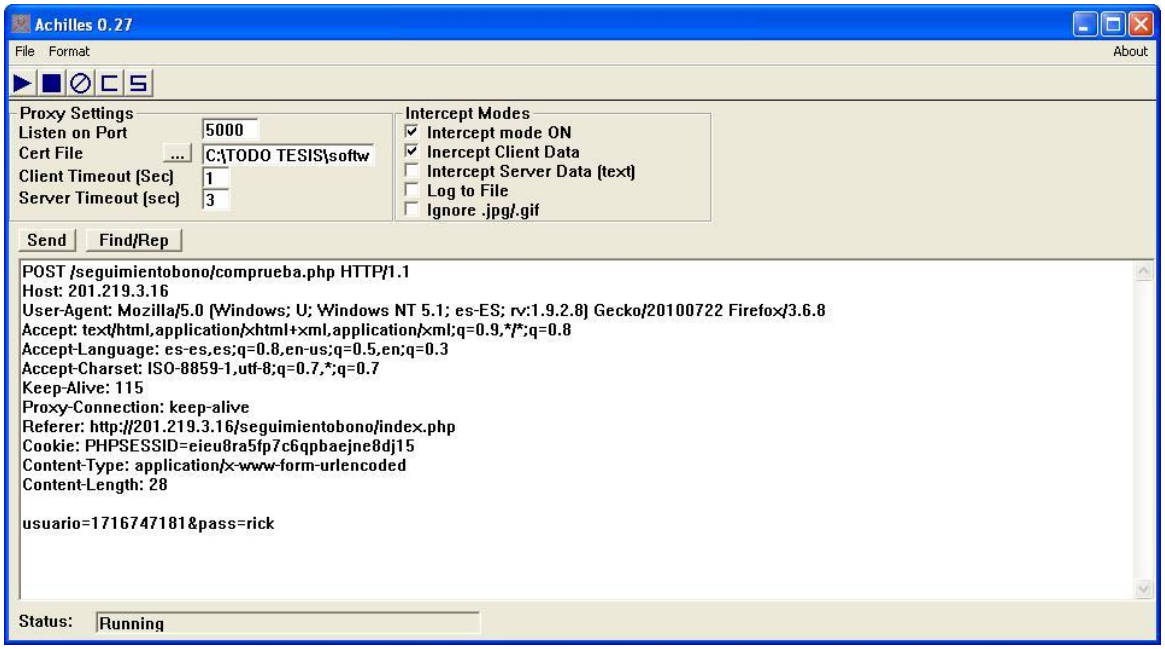


Figura 4.4: Proxy Achilles capturando datos a la web http://savmiduvi.miduvi.gov.ec/seguimientobono/index.php
Fuente: Autor de tesis.

Con esta información capturada por Achilles se puede obtener el identificador de sesión, con la ayuda de los datos generados en las cookies al momento de que el usuario procesa a autenticarse en la página web, si se logra obtener el dato del usuario se podrá tratar de atacar con SQL Injection como se lo intentará en el siguiente punto.

4.2.3. CÓMO SE LOGRA EL ACCESO POR SQL INYECTION.

Para lograr una inyección de código en una aplicación que requiera un login se puede utilizar las siguientes variaciones de caracteres especiales, conjuntamente con palabras reservadas SQL, en el cual se logrará que la condición de la sentencia SQL sea verdadera y se otorgue acceso autorizado.

' ' = ' ' ***1!= ' '*** ***1=1*** ***0=0***

Ejemplo:

Para el ejemplo se utilizará la siguiente página: http://savmiduvi.miduvi.gob.ec/miduvibono, en la cual existe un login para el ingreso al sistema de control de bonos de vivienda y se utilizará el usuario que se logró capturar con la herramienta Achilles.

Figura 4.5: Interfaz de acceso al sistema de incentivos para la vivienda.
Fuente: http:savmiduvi.miduvi.gob.ec

En la siguiente figura se puede apreciar que para los textbox no existe un control de errores comunes y básicos que siempre se deben tomar en cuenta al momento de desarrollar una aplicación web. Si un desarrollador no valida la longitud de los

campos ni tampoco el tipo de caracteres permitidos, es muy posible que tarde o temprano caiga en un ataque de inyección SQL.

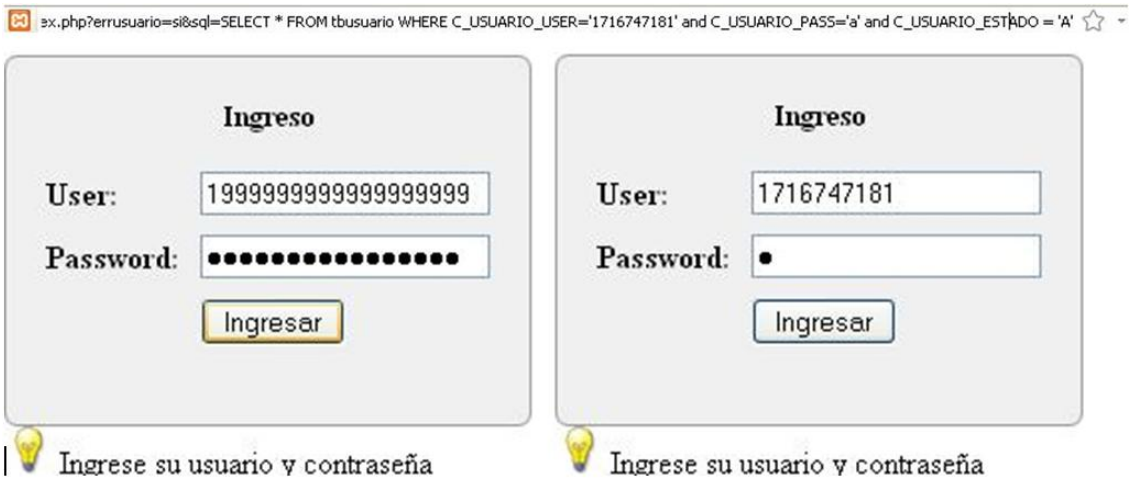


Figura 4.6: Ventanas de login que muestran la validación de campos para cada acceso.
Fuente: Autor de Tesis.

Es por esto que siempre se debe tomar un tiempo prudente para la validación de errores de seguridad en las aplicaciones a desarrollarse.

Si un intruso detecta estas vulnerabilidades lo que intentará será lo siguiente:

Figura 4.7: Ataque por SQL injection al detectar una vulnerabilidad.
Fuente: Autor de Tesis.

Y lo que obtendrá es: UN ACCESO SATISFACTORIO.

Figura 4.8: Ingreso por SQL injection al menú de administrador de la aplicación.
Fuente: Autor de Tesis.

4.2.4. SQL INYECCION EN UNA BASE SIN CONTROL DE PRIVILEGIOS

Para lograr este tipo de inyección de código es necesario conocer un poco más sobre las variaciones de caracteres que se puede utilizar al combinar sentencias SQL que alteren la base de datos.
Para acceder a la base de datos con determinados privilegios se puede enviar el siguiente comando perjudicial:

User: ***< '; + setencia_sql_peligrosa + carácter_inicio_comentario >***

Password: ***< '; + carácter_inicio_comentario>***

Ejemplo:
Lo que se puede realizar es generar una sentencia SQL que altere la acción inicial para la que fue creada, es decir, con la ayuda de los caracteres " -- " o " # ", según el tipo de base que utilice la aplicación, se puede generar una nueva sentencia que perjudique o altere enormemente las tablas de la base de datos. Si el cambio se produce en tablas importantes como por ejemplo la de usuarios, el daño será un desastre para la aplicación.

Figura 4.9: Ingreso de comandos peligrosos por SQL injection.
Fuente: Autor de Tesis.

User: ***'; drop table tabla_usuario; # (a partir de aqui se vuelve comentario)***

Password: ***123***

La sentencia SQL quedaría asi:

sql=SELECT * FROM tb_user WHERE campo_user=' '; drop table tb_user; # and campo_pass='123'

Select * from tb_user where campo_user = ‘ ‘ ; drop table tb_user; *#and campo_pass = ‘123’;*

Antes de ejecutar el login con SQL INJECTION	Se despliega la tabla para visualizar los campos	Luego de ejecutar SQL INJECTION.
basehack nacional sentencias tb_user tbadjudicado	basehack nacional sentencias tb_user Indice principal id campo_user campo_pass tbadjudicado tbanulado	basehack nacional sentencias tbadjudicado tbanulado

Figura 4.10: Verificación de la tabla “tb_user” al aplicar un comando SQL injection peligroso.
Fuente: Autor de Tesis.

4.3. HERRAMIENTAS DE ACCESO LA CONSOLA O TERMINAL

4.3.1. CARACTERÍSTICAS DE LA HERRAMIENTA NETCAT

NetCat es muy popular si se habla de herramientas de intrusión de sistemas y equipos remotos, ya que posee varias funciones que se aplican a través del intérprete de comandos bajo el protocolo TCP/IP y con una sintaxis muy fácil de entender y aprender.

Entre sus principales y más utilizadas funciones están la de abrir y cerrar puertos, asocia una Shell a un puerto específico y forzar conexiones TCP y UDP para el rastreo de equipos remotos.

Posee la gran ventaja de funcionalidad de líneas de comandos bajo MS-DOS y desde la Shell de Linux.

Esta herramienta podría ser utilizada en conjunto con lenguajes de programación como Perl y C, y como ya se mencionó antes se acopla muy bien a los Shell Scripts.

Sintaxis:

nc [-options] equipo_remoto port [ports] [acciones]

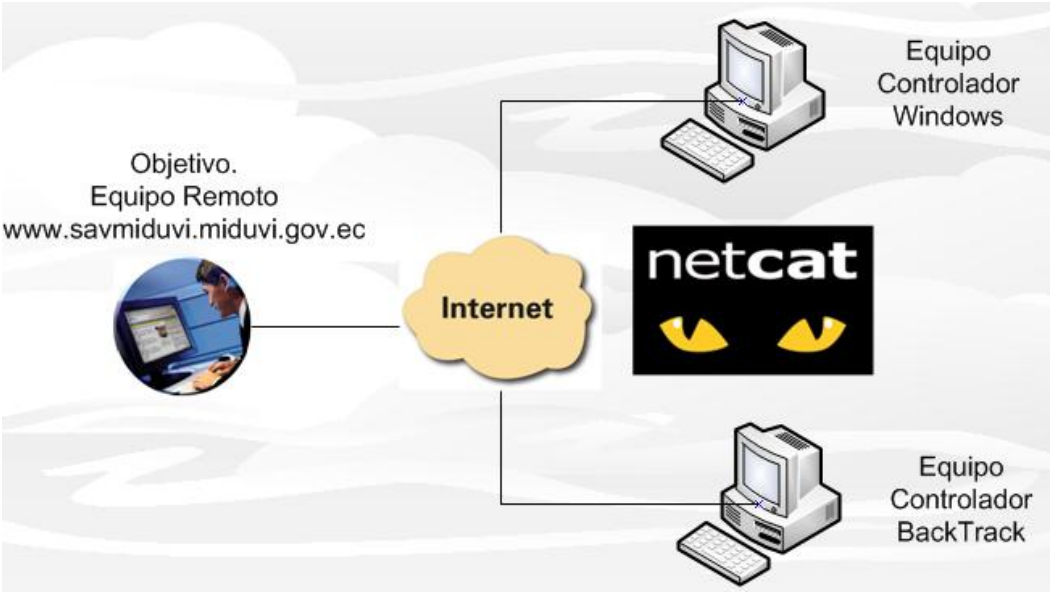


Figura 4.11: Diagrama de intrusión a un equipo remoto mediante NetCat.
Fuente: Autor de tesis.

4.3.2. CONFIGURACIÓN DEL EQUIPO REMOTO PARA EL ATAQUE.

EQUIPO REMOTO (Objetivo de Ataque)

Para realizar el ejemplo de intrusión utilizando NetCat, se hablará del **Equipo Remoto** (Objetivo de Ataque) y los equipos **Controladores** (Atacantes), en este caso se realizará la intrusión desde un equipo con sistema operativo Windows y otro con "BackTrack"[9].

Ingresando a la Web:

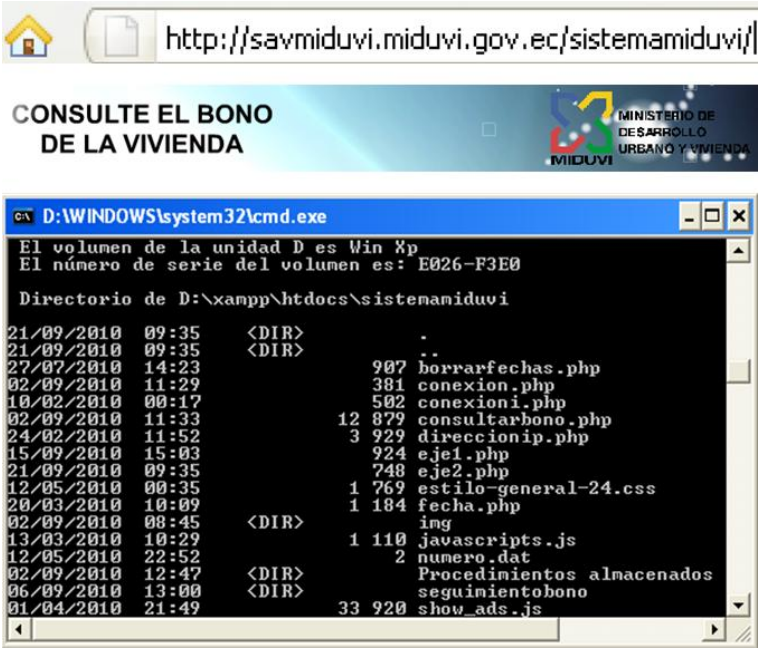


Figura 4.12: Verificación de los archivos alojados en "htdocs" del servidor web.
Fuente: Autor de Tesis.

Luego de ingresar a la dirección antes mencionada, se procederá a preparar al equipo remoto, en este caso el equipo que contiene el sistema de bonos del MIDUVI. Para entender el funcionamiento del ataque se abrirá una consola en la cual se ingresará el siguiente comando, según el SO del servidor:

nc - l - p 10000 - e /bin/bash (LINUX)

nc - l - p 10000 - e cmd.exe (WINDOWS)

[9] BackTrack: es una de las más conocidas y apreciadas distribuciones GNU/Linux orientadas a profesionales de la seguridad, con un enfoque especial hacia la realización de tests de penetración.

Para entender el comando anterior se describe a continuación los parámetros enviados:

ACCIONES Y PARAMETROS	FUNCION
nc	llamamos al programa NetCat
- l	Sirve para cambiar el modo a escucha
- p 10000	Se asiga el puerto de escucha
- e consola del SO (cmd.exe ó bin/bash)	Sirve para invocar a un elemento de control

Tabla 4.1: Cuadro de parámetros y funciones de la herramienta NetCat.
Fuente: Autor de Tesis.

Como se puede apreciar en la siguiente figura, el servidor cambia al estado de escucha en el puerto 10000 y si un equipo de cualquier parte del mundo localizaría este puerto abierto del servidor podría acceder con la ayuda de NetCat.

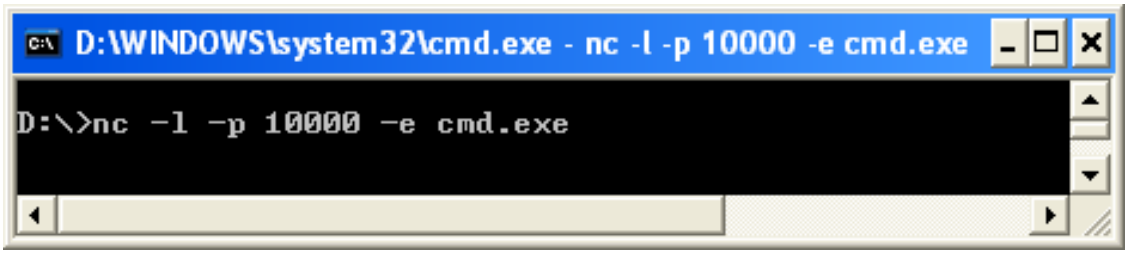


Figura 4.13: Ingreso del comando "nc –l " para cambiar a estado escucha utilizando NetCat.
Fuente: Autor de tesis.

4.3.3. ATAQUE DESDE UN EQUIPO CON WINDOWS MEDIANTE NETCAT

Para el primer caso en el computador 1 con sistema operativo Windows, se procede a revisar si existe conexión con el equipo remoto y de esta manera conocer la dirección IP del equipo.

Figura 4.14: Comando PING para comprobar que el equipo remoto este en línea.
Fuente: Autor de tesis.

Equipo Atacante 1: Windows

Para poder realizar la intrusión al equipo remoto, se procede a inicializar la herramienta NetCat enviando los 2 parámetros necesarios, que son la dirección IP del equipo y el puerto que está en modo escucha.

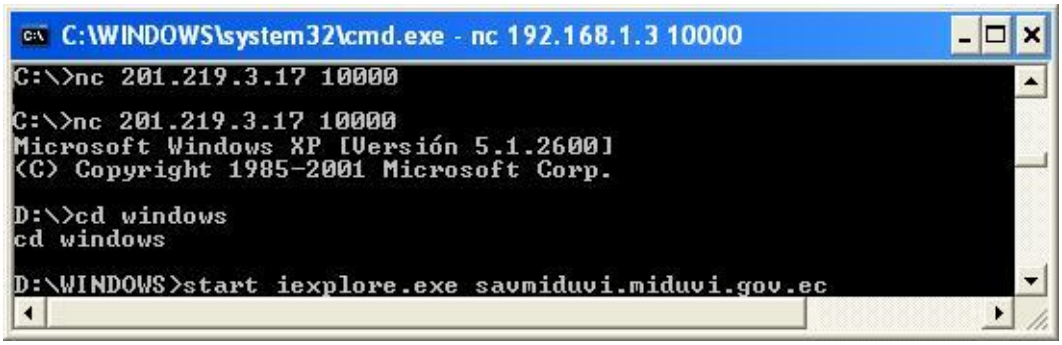


Figura 4.15: Inicialización de NetCat desde el equipo Controlador1 en Windows.
Fuente: Autor de tesis.

En la figura anterior, se puede visualizar que el equipo controlador 1 estableció la conexión con el equipo remoto y obtuvo la consola de comandos en la cual puede realizar todas las opciones permitidas en la Shell de Windows.

Para este ejemplo el comando que se utilizó, abrirá una página en Internet Explorer y redireccionará a la página ***savmiduvi.miduvi.gov.ec***, como se puede visualizar en la siguiente figura.

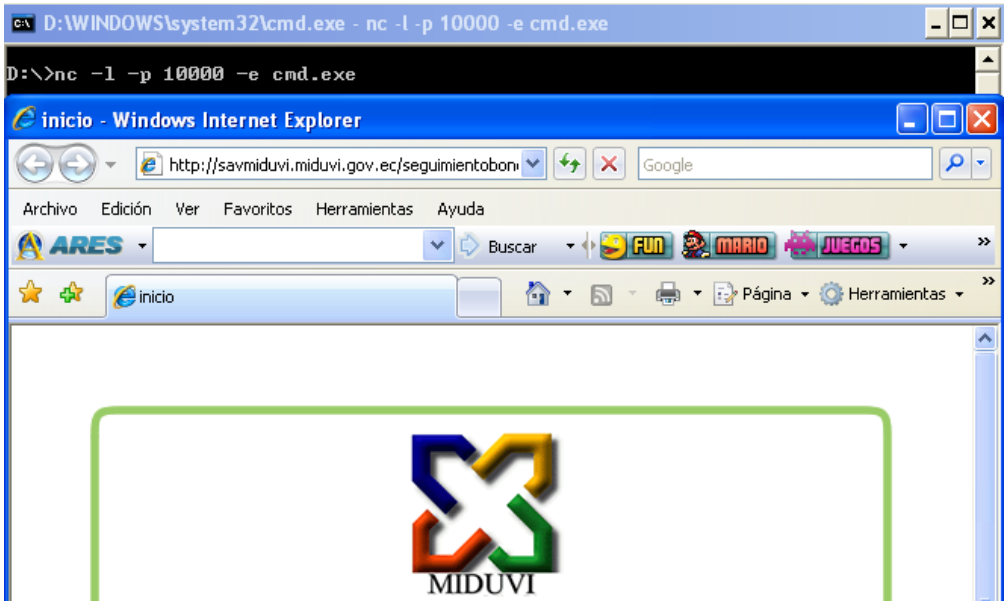


Figura 4.16: Equipo Servidor, está siendo controlado por un atacante desde la consola de Windows.
Fuente: Autor de tesis.

4.3.4. ATAQUE DESDE UN EQUIPO CON BASE LINUX (BACKTRACK) MEDIANTE NETCAT

Al utilizar la herramienta BackTrack se procede a abrir la consola y se tipea exactamente el mismo comando, con la dirección IP del equipo remoto y el puerto escucha.

Como se aprecia en la siguiente figura, al ejecutar el comando se presenta la etiqueta de Microsoft Windows XP, es decir, se logró establecer la conexión.

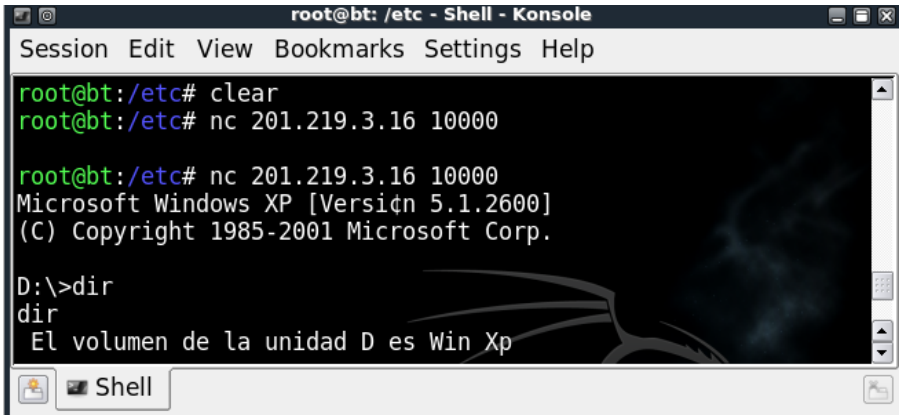


Figura 4.17: Conexión desde BackTrack al servidor que tiene abierto el puerto 10000.
Fuente: Autor de tesis.

Si se posee el control del intérprete de comandos del equipo remoto se puede realizar muchas cosas, hasta se puede decir, que el atacante esta frente al servidor con todos los permisos asignados y sin ningún tipo de restricción.

Para este ejemplo el atacante podría ejecutar un comando para dejar inactivo al equipo remoto, con un simple comando ***shutdown*****,** lograría conseguir que el sistema pase a un estado **offline.**

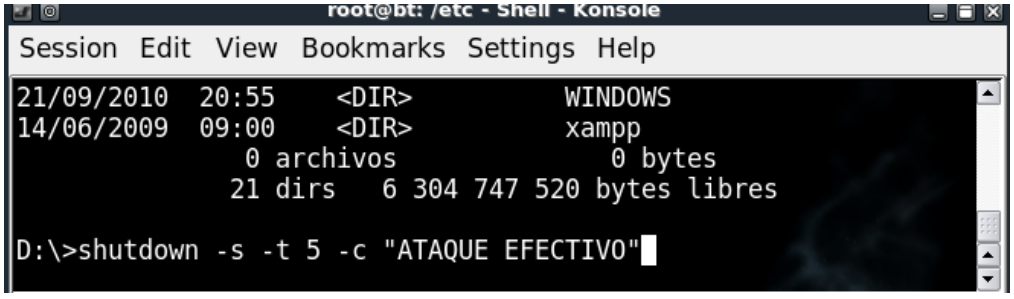


Figura 4.18: Comando shutdown desde atacante 2 en BackTrack que perjudicará al servidor.
Fuente: Autor de tesis.

En la siguiente figura se puede apreciar que el comando fue efectivo en el equipo remoto, y que estará en línea unos cuantos segundos más, luego de este tiempo se apagará.

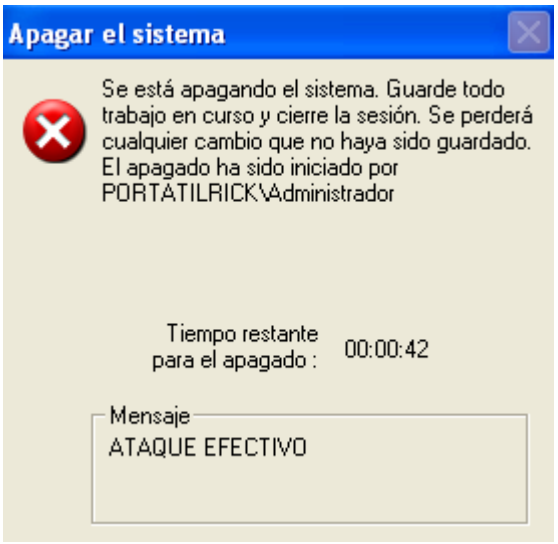


Figura 4.19: Mensaje de apagado de equipo. Generado desde un atacante que estableció la conexión. Fuente: Autor de tesis.

Estos tipos de ataques pueden convertirse en una catástrofe, si la información que se maneja es de vital importancia para la institución o empresa. Los administradores de red y seguridades deben estar muy pendientes de nuevas herramientas de este tipo para tener un plan para evitar estos ataques.

4.4. HERRAMIENTAS PARA ESCANEO DE PUERTOS Y VULNERABILIDADES

4.4.1. TESTING Y ESCANEO DE UN SERVIDOR WEB CON LA HERRAMIENTA NIKTO

La herramienta Nikto es un escaner de servidores web, en el cual puede realizar todo tipo de pruebas de ataques y vulnerabilidades por medio de una gama de plugins que vienen instalados.

Es además un excelente punto de partida para verificar que tan seguro es el servidor web en el que está actualmente corriendo un sistema importante y que trabaja con información vital para una determinada institución.

Otra de las ventajas es que trabaja muy bien, tanto en Windows como en Linux, con una amplia y robusta base de datos de ataques a servidores distintos.

Objetivo para ataque → http://201.219.3.16/

Sintaxis de un escaneo Básico:

Nikto.pl <-host> Dirección_Ip ó Nombre_de_dominio

Ejemplo 1: http://201.219.3.16/

./nikto.pl -host 201.219.3.16

Para este ejemplo se procederá a escanear el servidor web donde se encuentra instalado el aplicativo de bonos de vivienda del MIDUVI, el cual se utiliza para el control y seguimiento de los proyectos de vivienda.

Como se puede visualizar en la siguiente figura, el comando ingresado devuelve información del servidor web al cual se definió anteriormente.

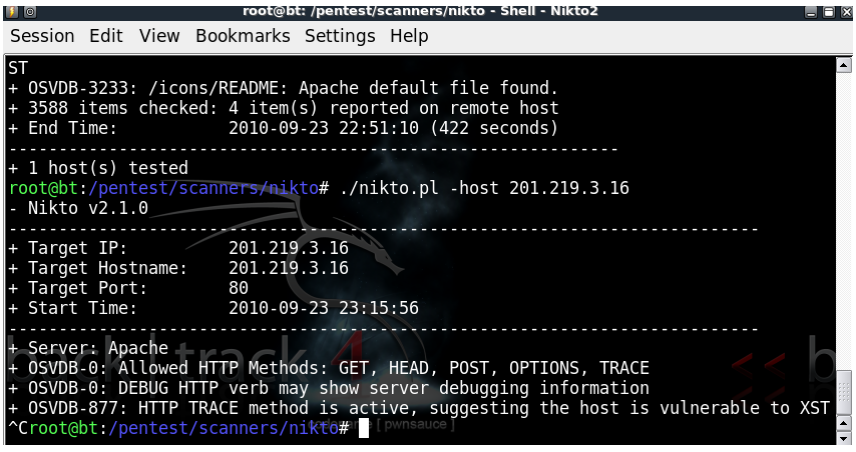


Figura 4.20: Escaneo básico utilizando Nikto al host 201.219.3.16.
Fuente: Autor de tesis.

El servidor web luego del análisis presenta pocas vulnerabilidades, pero esto no quiere decir que está libre de ataques, sino que debería implementar tareas de verificación de puertos y servicios para de esta manera asegurar el rendimiento y estabilidad de este equipo.

Ejemplo 2: Página web vulnerable.

La nueva página o servidor web escogido es www.xxxxx.xxx.ec (url escondida por políticas de privacidad), en el cual se procederá a correr varias aplicaciones para obtener información sobre las posibles vulnerabilidades de este servidor.

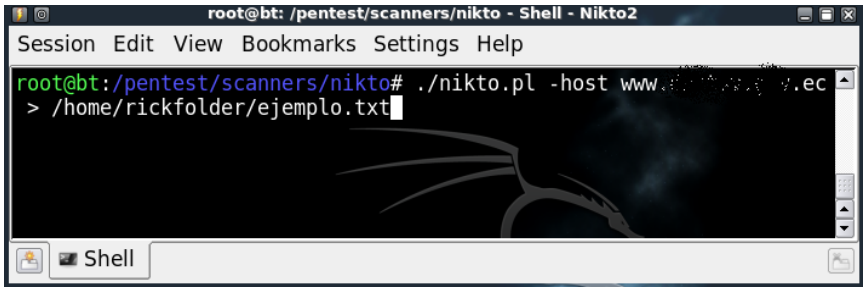


Figura 4.21: Escaneo a un host remoto para verificar si existe vulnerabilidad.
Fuente: Autor de tesis.

De la misma forma se puede aplicar y analizar la seguridad del host con la ayuda de la herramienta Nikto, pero a diferencia del ejemplo anterior se generará un reporte en el cual se detalla las vulnerabilidades encontradas.

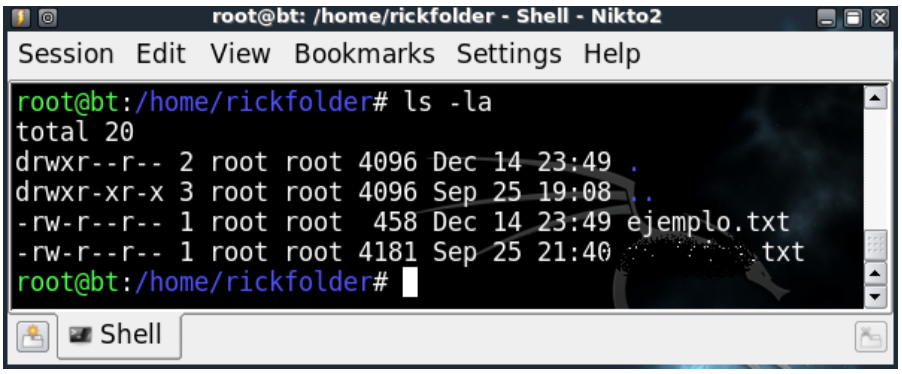
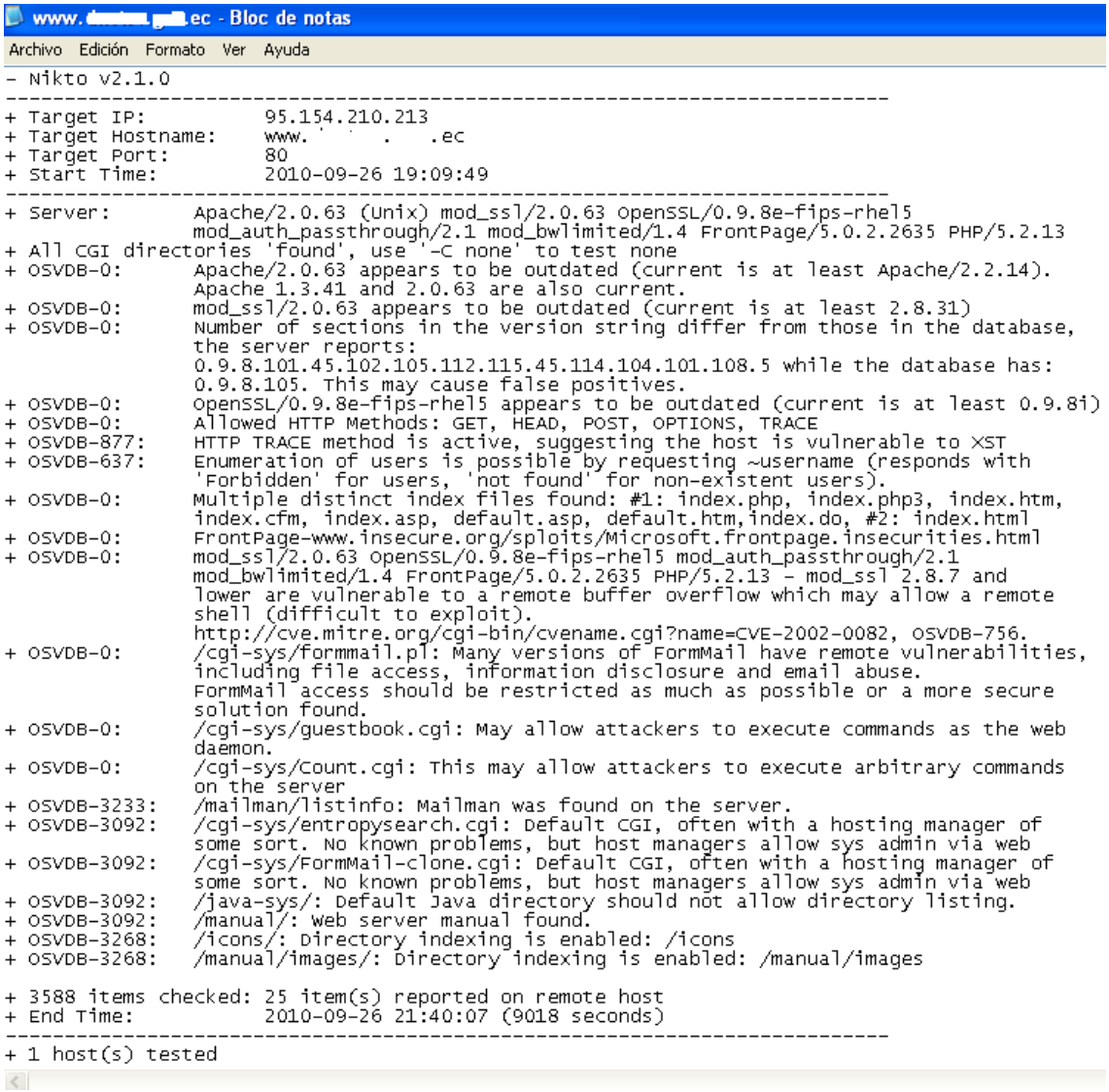


Figura 4.22: Generación de reporte al archivo "ejemplo.txt", con la descripción de vulnerabilidades.
Fuente: Autor de tesis.

Luego de abrir el archivo generado por la herramienta de escaneo, se puede apreciar en la siguiente figura, en resumen de las principales vulnerabilidades con sus respectivas descripciones para cada una de ellas.

Este escáner realiza varias pruebas exhaustivas que ponen a prueba la seguridad del servidor web, y a la vez sirve para que un administrador de red y seguridad puedan analizar cada una de las vulnerabilidades y a la vez puedan trabajar en la solución a los problemas más graves y peligrosos.



www.[redacted].ec - Bloc de notas

Archivo Edición Formato Ver Ayuda

```
- Nikto v2.1.0
---------------------------------------------------------------------------
+ Target IP:          95.154.210.213
+ Target Hostname:    www.[redacted].ec
+ Target Port:        80
+ Start Time:         2010-09-26 19:09:49
---------------------------------------------------------------------------
+ Server:       Apache/2.0.63 (Unix) mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5
                mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.13
+ All CGI directories 'found', use '-C none' to test none
+ OSVDB-0:      Apache/2.0.63 appears to be outdated (current is at least Apache/2.2.14).
                Apache 1.3.41 and 2.0.63 are also current.
+ OSVDB-0:      mod_ssl/2.0.63 appears to be outdated (current is at least 2.8.31)
+ OSVDB-0:      Number of sections in the version string differ from those in the database,
                the server reports:
                0.9.8.101.45.102.105.112.115.45.114.104.101.108.5 while the database has:
                0.9.8.105. This may cause false positives.
+ OSVDB-0:      OpenSSL/0.9.8e-fips-rhel5 appears to be outdated (current is at least 0.9.8i)
+ OSVDB-0:      Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877:    HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-637:    Enumeration of users is possible by requesting ~username (responds with
                'Forbidden' for users, 'not found' for non-existent users).
+ OSVDB-0:      Multiple distinct index files found: #1: index.php, index.php3, index.htm,
                index.cfm, index.asp, default.asp, default.htm,index.do, #2: index.html
+ OSVDB-0:      FrontPage-www.insecure.org/sploits/Microsoft.frontpage.insecurities.html
+ OSVDB-0:      mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1
                mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.13 - mod_ssl 2.8.7 and
                lower are vulnerable to a remote buffer overflow which may allow a remote
                shell (difficult to exploit).
                http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ OSVDB-0:      /cgi-sys/formmail.pl: Many versions of FormMail have remote vulnerabilities,
                including file access, information disclosure and email abuse.
                FormMail access should be restricted as much as possible or a more secure
                solution found.
+ OSVDB-0:      /cgi-sys/guestbook.cgi: May allow attackers to execute commands as the web
                daemon.
+ OSVDB-0:      /cgi-sys/Count.cgi: This may allow attackers to execute arbitrary commands
                on the server
+ OSVDB-3233:   /mailman/listinfo: Mailman was found on the server.
+ OSVDB-3092:   /cgi-sys/entropysearch.cgi: Default CGI, often with a hosting manager of
                some sort. No known problems, but host managers allow sys admin via web
+ OSVDB-3092:   /cgi-sys/FormMail-clone.cgi: Default CGI, often with a hosting manager of
                some sort. No known problems, but host managers allow sys admin via web
+ OSVDB-3092:   /java-sys/: Default Java directory should not allow directory listing.
+ OSVDB-3092:   /manual/: Web server manual found.
+ OSVDB-3268:   /icons/: Directory indexing is enabled: /icons
+ OSVDB-3268:   /manual/images/: Directory indexing is enabled: /manual/images

+ 3588 items checked: 25 item(s) reported on remote host
+ End Time:           2010-09-26 21:40:07 (9018 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figura 4.23: Archivo txt generado con la descripción del reporte de escaneo de vulnerabilidades. Fuente: Autor de tesis.

Esta herramienta es súper compleja y potente al referirse a la seguridad de servidores web. Varias son las alternativas y funciones que presenta este escáner, entre las principales: escaneo de host, soporte de SSL, técnicas de mutación, formatos de presentación, escaneo personalizado y aplicación de plugins.

4.4.2. TESTING Y ESCANEO DE UN SERVIDOR WEB CON LA HERRAMIENTA NESSUS

Esta herramienta es muy completa, ya que a más de ser un programa de escaneo de vulnerabilidades, provee de un cliente y un servidor que manejará y controlará toda actividad generada por cada una de las máquinas conectadas a Nessus, obteniendo de esta manera un verdadero sistema de scanning y ataques a servidores y equipos remotos.

Tiene la facilidad de instalarse en varios sistemas operativos como Linux, BSD, Solaris, Windows. Está basado en plugins y permite generar reportes descargables a medio magnético.

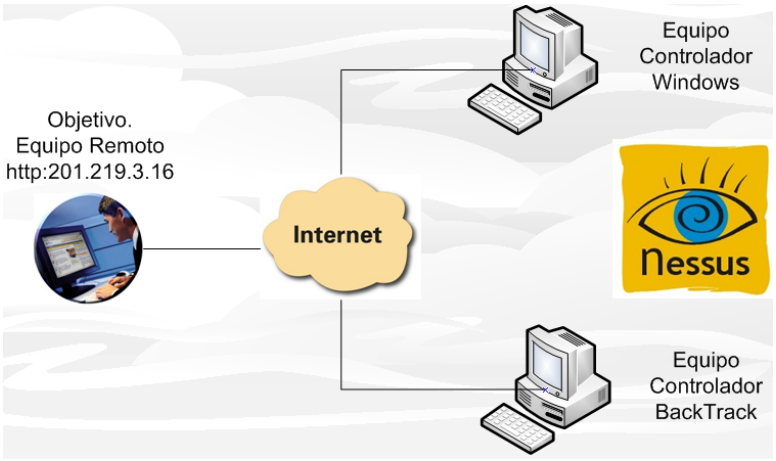


Figura 4.24: Diagrama de intrusión a un equipo remoto mediante Nessus.
Fuente: Autor de tesis.

Ejemplo:

Para este ejemplo se realizará un escaneo al siguiente servidor:

http://201.219.3.16

Como se presentó en anteriores ejemplos el servidor 201.219.3.16 aloja una aplicación web para el control y seguimiento de bonos de vivienda, lo que se hará es probar a la herramienta Nessus y verificar si la información obtenida es importante en cuanto a pruebas de seguridad remotas que debe soportar un servidor seguro que maneja información importante.

4.4.2.1. EQUIPO ATACANTE 1: WINDOWS

El primer paso para lograr un equipo atacante con Nessus es instalar el cliente y el servidor de Nessus en el sistema operativo Windows, con la ayuda del instalador se presentará el wizard para completar la instalación.

Como se puede apreciar en la siguiente figura, primero que nada hay que configurar el servidor añadiendo un usuario el cual podrá utilizar la herramienta para el escaneo de cualquier equipo remoto.

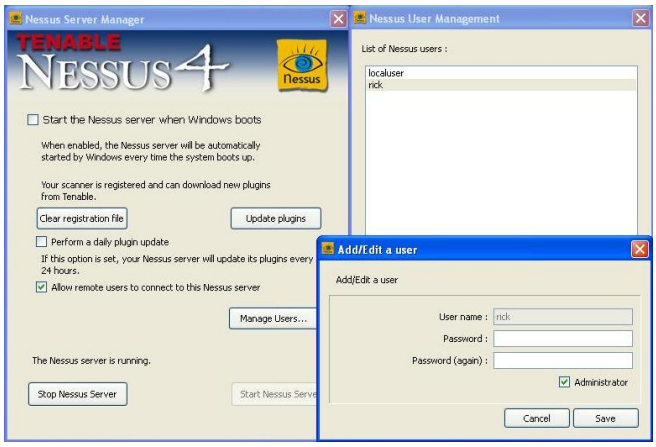


Figura 4.25: Configuración del servidor Nessus en Windows luego de su instalación.
Fuente: Autor de tesis.

Luego de tener un usuario con el cual se puede ingresar a la herramienta se procede a ejecutar el cliente de Nessus en el cual se ingresará y se visualizará la interfaz que posee y en la cual se podrá obtener resultados muy interesantes y amigables al usuario como se presenta en la siguiente figura.

Figura 4.26: Pantalla principal con el login de Nessus desde el cliente Windows.
Fuente: Autor de tesis.

Luego de ingresar a la herramienta mediante esta interfaz amigable, se presentará un menú de opciones donde la más importante será la de “Scans”, pues aquí se realizarán los escaneos a las direcciones deseadas.

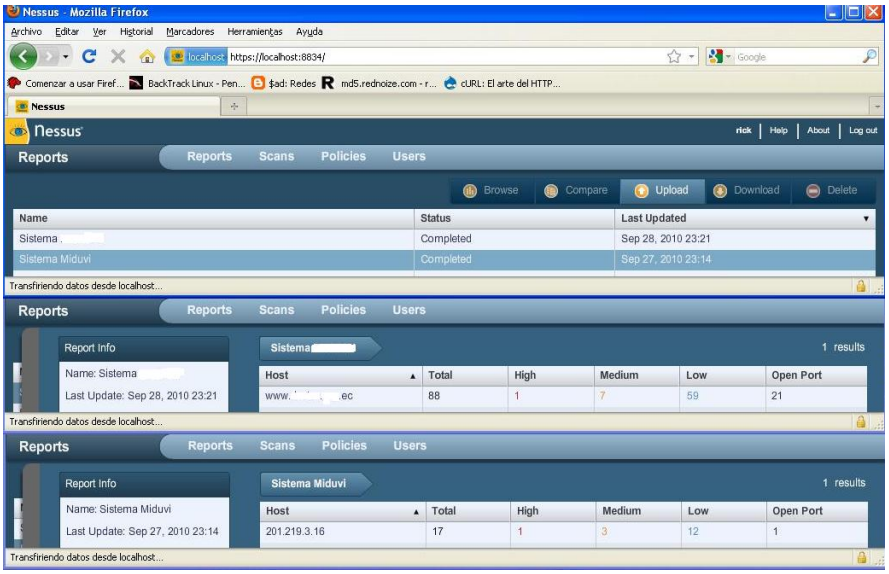


Figura 4.27: Pantalla general con el detalle de escaneo a las 2 páginas de la web.
Fuente: Autor de tesis.

Como se puede apreciar en la figura anterior, se ha realizado un scanning a 2 páginas en concreto, si se compara una con otra, lo que resalta a simple vista es el total de vulnerabilidades de la primera con respecto a la otra, para la página ejemplo existen muchas más vulnerabilidades que para el sistema de control y seguimiento de proyectos de vivienda.

Host Remoto: Acceso a escaneo de 24 puertos.

Sistema DNCTSV | www.dnctsv.gov.ec | 24 resu

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
21	tcp	ftp	7	0	1	5	1
22	tcp	ssh	5	0	0	4	1
53	tcp	dns	2	0	0	1	1
53	udp	dns	5	0	0	5	0
80	tcp	www	7	0	0	6	1
110	tcp	pop3	6	0	1	4	1
111	tcp	sunrpc?	2	0	0	1	1
143	tcp	imap	6	0	1	4	1
443	tcp	www	7	1	1	4	1
465	tcp	smtp	7	0	1	5	1
993	tcp	imap	7	0	1	5	1
995	tcp	pop3	7	0	1	5	1
2077	tcp	trellisagt?	1	0	0	0	1
2078	tcp	trellissvr?	1	0	0	0	1
2082	tcp	infowave?	1	0	0	0	1
2083	tcp	radsec?	1	0	0	0	1

Figura 4.28: Detalle de escaneo al host remoto que se tomo como ejemplo.
Fuente: Autor de tesis.

Sistema MIDUVI: Acceso a escaneo de 4 puertos.

Sistema Miduvi | 201.219.3.16 | 4 results

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	5	0	0	5	0
0	udp	general	1	0	0	1	0
53	udp	dns	3	0	0	3	0
80	tcp	www	8	1	3	3	1

Figura 4.29: Detalle de escaneo con la herramienta Nessus a http://201.219.3.16.
Fuente: Autor de tesis.

4.4.2.2. EQUIPO ATACANTE 2: BACKTRACK.

En este caso, el sistema BackTrack no posee instalado esta herramienta por lo que se procederá a instalar el paquete de Nessus con el siguiente comando:

Cliente: ***# apt-get install nessus***
Demonio: ***# apt-get install nessusd***

- **Instalación de Cliente Nessus**

Lo que se puede visualizar en la siguiente figura es el proceso de instalación del cliente Nessus en BackTrack.

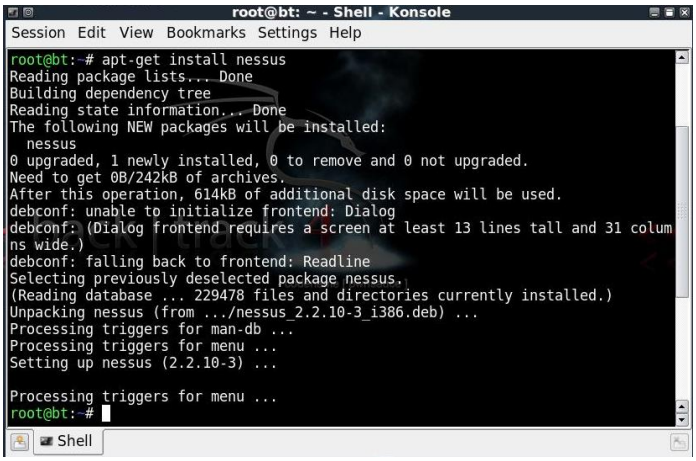


Figura 4.30: Proceso de instalación del cliente Nessus con el comando "apt –get install".
Fuente: Autor de tesis.

- **Instalación de Servidor Nessus**

Luego de instalado el cliente se procede a instalar el Demonio de Nessus, que es este caso será "**nessusd",** pero a diferencia del cliente este sí debe ser iniciado y configurado para que el cliente puede conectarse y dar uso a la herramienta.

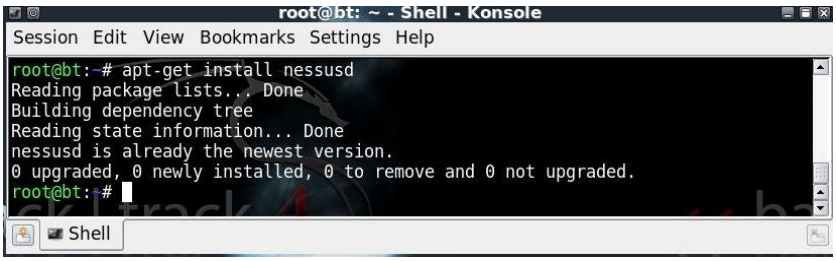


Figura 4.31: Instalación del servidor Nessus mediante el comando "apt –get install".
Fuente: Autor de tesis.

Lo primero será generar un usuario cliente el cual se creará con el comando:

 # nessus-adduser

Como se puede visualizar en la siguiente figura, el usuario que se configurará será "root", en el cual se ingresarán datos de password y sistemas de reglas.

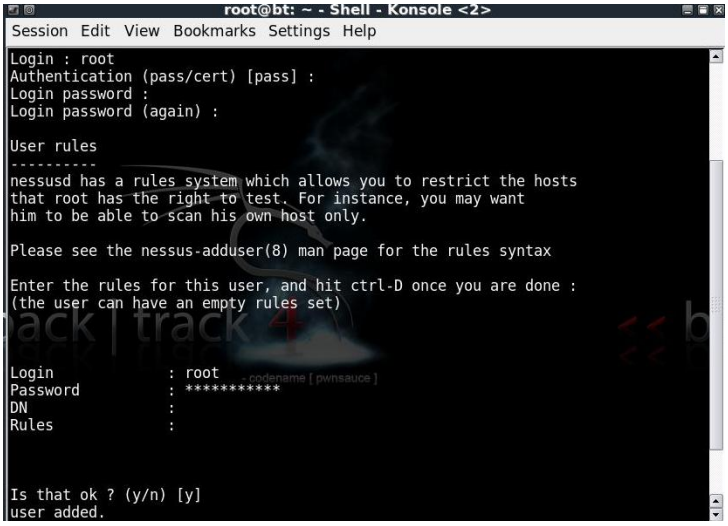


Figura 4.32: Configuración de usuarios cliente desde el servidor Nessus instalado.
Fuente: Autor de tesis.

En este momento se puede ejecutar el cliente de Nessus para comenzar el ataque desde BackTrack.

De la misma forma que se utilizó en entorno Windows, se debe indicar el equipo al que se va a realizar el ataque ya sea por el nombre de host o por la dirección IP. Como se explicó anteriormente esta herramienta se basa en ataques con plugins, los cuales pueden ser escogidos para cada análisis de vulnerabilidades.

Los reportes generados por la herramienta no son tan amigables como en Windows pero la ventaja es que el escaneo que realiza es mucho más minucioso y preciso, ya que el informe de resultados provee de información que si cae en malas manos podría ser perjudicial al equipo remoto.

Ejemplo → Target: http://201.219.3.16/

En el ejemplo se puede observar las diferentes vulnerabilidades que posee el servidor escogido como objetivo de ataque, con esta información y con la ayuda de páginas que aprovechan estas debilidades de seguridad se puede obtener acceso a servicios e información sin autorización.

Estas herramientas al parecer son inofensivas, pero si se las conoce a fondo pueden generar muchos problemas a los administradores de red y seguridad si el equipo objetivo de ataque fue uno de ellos.

La única forma de evitar estos ataques es conociendo los problemas de seguridad que existen en un determinado servidor para de esta manera modificar las configuraciones tomando las medidas preventivas necesarias para que no ocurran estas situaciones.

5. CAPÍTULO: ADMINISTRACIÓN Y MANEJO DE LA INFORMACIÓN.

5.1. PROBLEMAS COMUNES EN EL MANEJO DE LA INFORMACIÓN.

En la actualidad existen instituciones que no poseen un manejo adecuado de la información que se genera en todos sus procesos.
Esto genera problemas de procesamiento en cuanto a la velocidad de respuesta, facilidad de acceso y disponibilidad del recurso.
Además cuando se cometen errores en cuanto al almacenamiento y procesamiento de la misma se obtendrá información poco útil ya que no estará en condiciones de generar los reportes requeridos.

5.1.1. INFORMACIÓN LIMITADA.

Cuando no se posee información necesaria de algún proceso en particular, la funcionalidad y productividad de la empresa o institución se va retrasando a medida que pasa el tiempo. Se puede decir que al tener una base de datos con pocos registros que cuenta con información generalizada, el procesamiento de la misma se vuelve manejable, no es así cuando la base de datos a crecido considerablemente y para poder manejarla se necesitan de las herramientas adecuadas para procesar miles de registros en cada transacción.

Ejemplo:
Para este ejemplo se muestra que la información que posee la institución se reduce a 7 campos, que si bien muestran información general sobre los beneficiarios, no describe detalladamente ni específicamente los parámetros de calificación, aprobación, seguimiento de cada una de las personas que recibieron el bono.

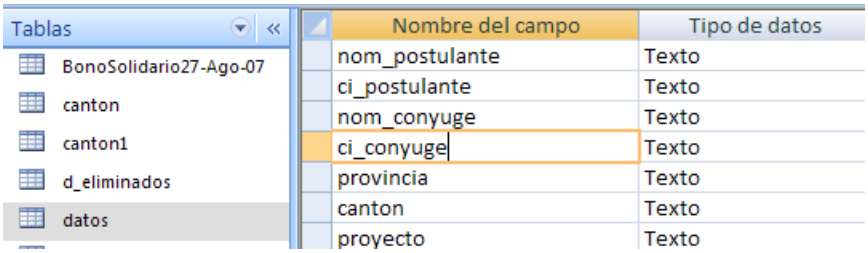


Figura 5.1: Vista modo diseño de la base de beneficiarios del bono de vivienda en Microsoft Access.
Fuente: Autor de tesis.

Como se aprecia en la siguiente figura, se procesan alrededor de 400000 registros aproximadamente pero con datos que no permiten generar reportes estadísticos, gerenciales, tabulares y detallados. El principal problema es que no existe un sistema que controle y administre una base de datos centralizada de los beneficiarios.

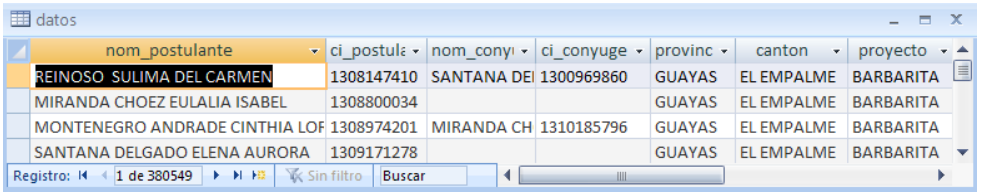


Figura 5.2: Detalle de tabla "datos", que muestra el número de registros que posee la tabla.
Fuente: Autor de tesis.

5.1.2. INFORMACIÓN CONFIDENCIAL SIN PROTECCIÓN.

La información confidencial sobre los beneficiarios del bono de la vivienda debería estar almacenada y respaldada en un equipo que cuente con las debidas normas de seguridad.

Si no se cuenta con un DBA (Administrador de Base de Datos), que se dedique exclusivamente al resguardo y cuidado de la misma, tarde o temprano la empresa o institución estará lamentándose por posibles pérdidas o alteraciones de información.

Ejemplo:

En el MIDUVI existe información sobre los beneficiarios que han recibido el bono de vivienda, estos registros se alojan en un computador que no cuenta con las medidas de seguridad adecuadas.

Si esta “base de datos” llegase a ser cambiada o alterada por alguna persona que tenga fines maliciosos causaría un gran problema a la institución pues actualmente es la única fuente de información en cuanto a personas que han recibido el beneficio.

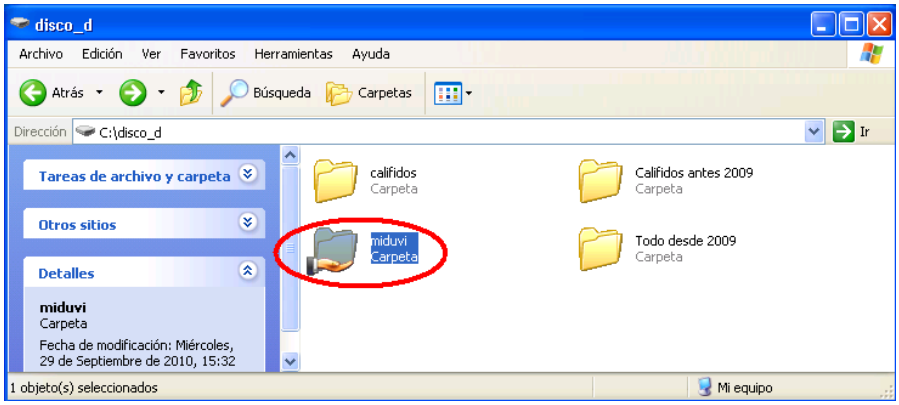
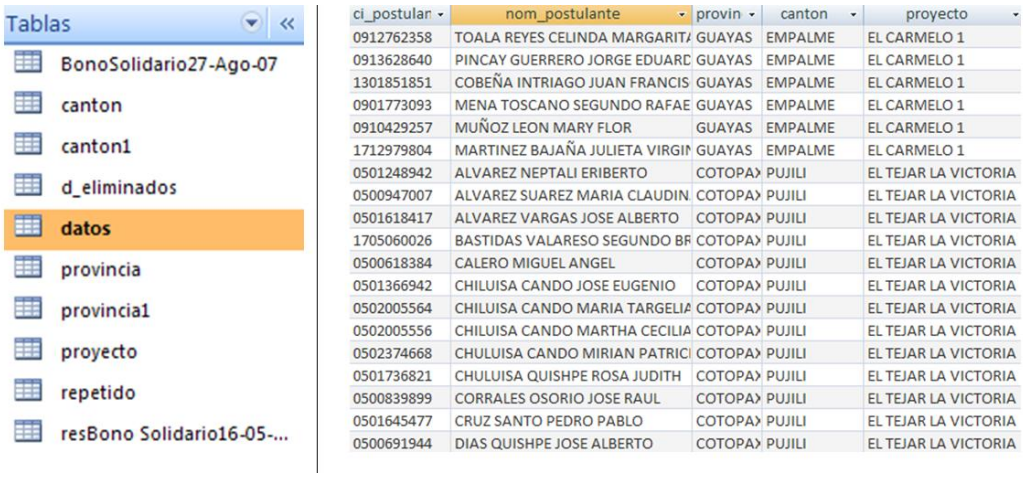


Figura 5.3: Carpeta de Windows que aloja la base de datos de beneficiarios del bono de vivienda.
Fuente: Autor de tesis.

En la figura anterior, se aprecia una carpeta de Windows en la cual se aloja la base de Access con la tabla “nacional” y una pequeña aplicación desarrollada en Visual Basic, la cual carga automáticamente la información sobre los beneficiarios del bono de la vivienda, y estos datos son la referencia para saber que las nuevas postulaciones no se dupliquen y se emita doble beneficio a una persona.



ci_postular	nom_postulante	provin	canton	proyecto
0912762358	TOALA REYES CELINDA MARGARITA	GUAYAS	EMPALME	EL CARMELO 1
0913628640	PINCAY GUERRERO JORGE EDUARD	GUAYAS	EMPALME	EL CARMELO 1
1301851851	COBEÑA INTRIAGO JUAN FRANCIS	GUAYAS	EMPALME	EL CARMELO 1
0901773093	MENA TOSCANO SEGUNDO RAFAE	GUAYAS	EMPALME	EL CARMELO 1
0910429257	MUÑOZ LEON MARY FLOR	GUAYAS	EMPALME	EL CARMELO 1
1712979804	MARTINEZ BAJAÑA JULIETA VIRGI	GUAYAS	EMPALME	EL CARMELO 1
0501248942	ALVAREZ NEPTALI ERIBERTO	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0500947007	ALVAREZ SUAREZ MARIA CLAUDIN	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0501618417	ALVAREZ VARGAS JOSE ALBERTO	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
1705060026	BASTIDAS VALARESO SEGUNDO BR	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0500618384	CALERO MIGUEL ANGEL	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0501366942	CHILUISA CANDO JOSE EUGENIO	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0502005564	CHILUISA CANDO MARIA TARGELIA	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0502005556	CHILUISA CANDO MARTHA CECILIA	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0502374668	CHULUISA CANDO MIRIAN PATRICI	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0501736821	CHULUISA QUISHPE ROSA JUDITH	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0500839899	CORRALES OSORIO JOSE RAUL	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0501645477	CRUZ SANTO PEDRO PABLO	COTOPAX	PUJILI	EL TEJAR LA VICTORIA
0500691944	DIAS QUISHPE JOSE ALBERTO	COTOPAX	PUJILI	EL TEJAR LA VICTORIA

Figura 5.4: Registros de Microsoft Access donde se almacenan los registros de beneficiarios.
Fuente: Autor de tesis.

Estos datos son cargados automáticamente a una tabla “datos” la cual va añadiendo los registros que son enviados por las unidades técnicas provinciales de todo el país y la cual sirve como “base nacional” para validar duplicidad con cualquier otro beneficio que otorga en MIDUVI.

5.1.3. BASE DE DATOS NO RELACIONAL SIN CODIFICACIÓN.

Las bases de datos relacionales proveen de varias ventajas si se las compara con matrices de datos planas que actualmente se utilizan en algunas instituciones.
Es cierto que herramientas como el Excel permiten manejar datos de una manera ordenada y organizada, pero si los datos aumentan rápidamente según los procesos que se lleven en una empresa o institución se vuelve realmente difícil y problemático tener un control mediante hojas planas o matrices de datos no relacionales.

Es así que en el MIDUVI, se tiene una base plana o matriz de datos no relacional sin codificación, y esta es la causa del problema al tratar de generar reportes tabulados por provincia, cantón y parroquia.

Para ver con un ejemplo este problema se realizará una consulta SQL a la tabla “datos”, en la cual consta la información sobre los incentivos de vivienda que otorga el MIDUVI.

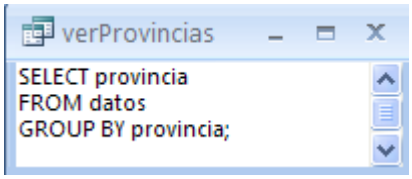


Figura 5.5: Vista de diseño de la consulta SQL a ser generada para extraer las provincias.
Fuente: Autor de tesis.

Como se aprecia en la figura anterior se realizó un SELECT a la tabla datos agrupándolos por provincia. Para un caso normal el resultado sería los nombres de las 24 provincias que contiene el Ecuador.

El resultado que devolvió la consulta es la siguiente:

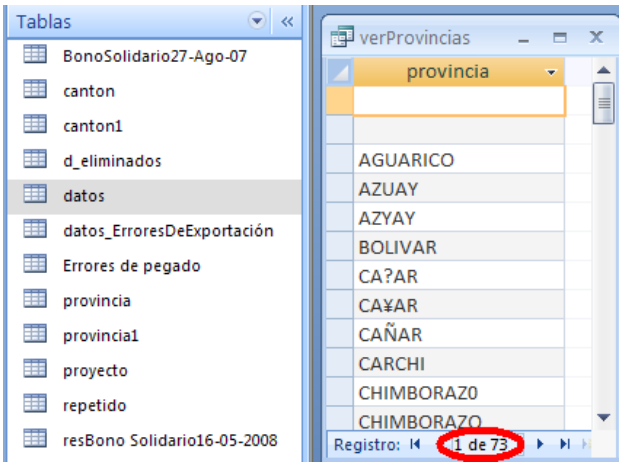


Figura 5.6: Resultado de la consulta SELECT agrupada por provincias de la tabla datos.
Fuente: Autor de tesis.

El número de registros fue de 73 nombres de provincias, cada una de ellas difiere por algún carácter especial, números, orden de letras, tildes, abreviaturas y hasta se visualiza nombres de cantones que han ingresado en la columna de provincias. Otro ejemplo se aprecia en la siguiente figura, que para la provincia de SANTO DOMINGO DE LOS TSACHILAS, se tiene una variedad de nombres al ser la provincia entre todas del Ecuador que posee más caracteres en su nombre.

nom_postulante	ci_postula	nom_conyuge	ci_conyug	provincia	canton	pr
PALACIOS COLON ASISCLO	1709839078	LUCAS PALACIOS	1308069945	SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	CHILA RIO BUA
PARDO JULIA AMANDA	1707699871			SANTO DOMINGO	SANTO DOMINGO	LAS MERCEDES GRU
PAREDES HOLGUER RENE	1708991441			SANTO DOMINGO	SANTO DOMINGO	EL ESFUERZO I / 09
PAREDES MARIA LIVIA AMERICA	1801050004	RAMOS MAYORG	1800429209	SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	SANTA MARIANITA
PINARGOTE ROSA RAMONA	1711073724			SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	LUZ DEL DIA
SALAZAR HILDA GLORIA	1710397413			SANTO DOMINGO	SANTO DOMINGO	BELLAVISTA I-09 SA
SIGUENZA BLANCA ROSA	1705364949	BALSECA CASTEL	1706114509	SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	ALLURIQUIN
TUBAY GABRIEL PATRICIO	1301586135			SANTO DOMINGO	SANTO DOMINGO	EL ESFUERZO I / 09
ULLAGUARI MARIA LASTENIA	1709704249	CHEZA TARAPUE	1001310547	SANTO DOMINGO DE LOS TSÁCHILAS	STO.DOMING	LOS PALMITOS
VEGA MARIA CARMEN	1101833901			SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	LUZ DEL DIA
VERA MERCEDES EDILMA	1305814707			SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	LA VILLEGAS G#1 -2
VITERI VICTOR MANUEL	1701845784	CHIPANTIZA ASE	1706150578	SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	LA VILLEGAS G#1 -2
ABAD CORREA LUZ AMERICA	1707942437			SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	SANTA MARIANITA
ABRIL NARANJO NANCY MARIBEL	1714181037			SANTO DOMINGO DE LOS	SANTO DOMINGO	URBANA CORTE2 2(
ABRIL PARCO EVA MARIA	1717052771	MONAR YANEZ J	1719617670	SANTO DOMINGO	SANTO DOMINGO	BELLAVISTA I-09 SA
ACARO AREVALO ANGELA	1703222222			SANTO DOMINGO	SANTO DOMINGO	EL PLACER DEL TOA
ACARO COFRE MARIANA DE JESU	1709967200	ORDOÑEZ MORA	1101971065	SANTO DOMINGO	SANTO DOMINGO	EL PLACER DEL TOA
ACOSTA VEGA LERIDA MERCEDES	1306407675	BASURTO GILER	1305172866	SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	LUZ DEL DIA

Figura 5.7: Tabla nacional mostrando los errores en la provincia de Santo Domingo de los Tsachilas.
Fuente: Autor de tesis.

Este problema se genera principalmente por 2 razones, la primera es que no existe un procedimiento de validación de datos y la segunda es porque no existe un sistema de gestión y control que trabaje con códigos y tablas relacionales como se aprecia en la siguiente figura.

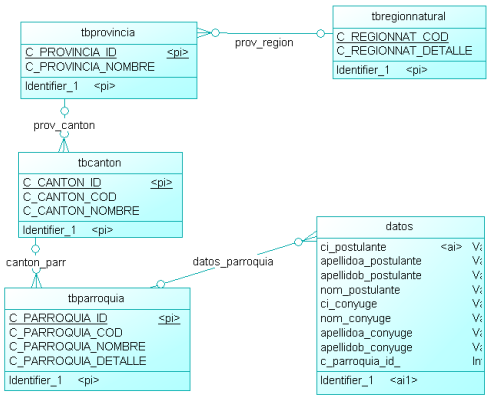


Figura 5.8: Diagrama entidad relación que se debería implementar en la tabla datos.
Fuente: Autor de tesis.

Para el caso de bonos de vivienda, se debería trabajar con la DPA (División Política Administrativa) actualizada por el INEC, para la codificación de provincias, cantones y parroquias. La figura anterior muestra el esquema que se podría adoptar para solucionar el problema actual.

En la siguiente tabla, se muestra un resumen detallado con los nombres de provincias que existen en la tabla “datos”, en la cual se visualizan registros distintos que se refieren a una misma provincia.

CAMPO PROVINCIA	CAMPO CANTON	CAMPO NOMBRE DEL PROYECTO
AGUARICO	MUSHU RUNA	
AZUAY	CUENCA	MAYANCELA/2009
AZYAY	CUENCA	SIV-MAGISTERIO-2009-NP
BOLIVAR	GARANDA	QUIVILLUNGO
CA?AR	AZOGUEZ	SIV-VIVIENDA NUEVA
CAÑAR	LA TRONCAL	COCHANCAY
CARCHI	MIRA	URBANO4TOCORTE08
CA¥AR	CA□AR	SIV
CHIMBORAZ0	COLTA	ROEOPAMBA CENTRO
CHIMBORAZO	GUAMOTE	SAN ANTONIO DE GUAMOTE
COTOPAXI	PUJILI	EL TEJAR LA VICTORIA
DAULE	GUAYAS	LA PATRIA ES DE TODOS
EASMERALDAS	QUININDE	VILLEGAS I
EL ORO	BALSAS	BELLAMARIA
ESMERALDAS	ESMERALDAS	SANCARLOS
FRANCISCO DE ORELLANA	LORETO	HUATICOCHA
FRCO. DE ORELLANA	ORELLANA	URBANO4TOCORTE08
GALAPAGOS	SANTA CRUZ	UNION DEL PUEBLO
GUAYAQUIL	NARANJAL	TAURA 1
GUAYAS	EMPALME	EL CARMELO 1
GUAYAS.	YAGUACHI	UNIDOS VENCEREMOS
IMBABURA	COTACACHI	DOMINGO SABIO 2
LOJA	PALTAS	EL TRIUNFO-NARANJILLO
LOS RIO	PUEBLOVIEJ	RAFAEL CORREA
LOS RIOS	MOCACHE	EL TRIUNFO MACULILLO
M.SANTIAGO	PALORA	16-Ago
MANABI	PORTOVIEJO	FIDEICOMISO - ORQUIDEAS I
MANBI	CHONE	FIDEICOMISO - SEIS DE DICIEMBRE
MORONA	LOGROÑO	SANTIAGO TUKUP
MORONA SANTIAGO	HUAMBOYA	PURIZIMA
MORONA S	SANTIAGO	TAYUSA
MORONA S.	MORONA	MUSAP
MORONA SAN	MORONA	UNT WICHIM
MORONASANT	MORONA	RIO BLANCO II
MORONA SANTIAGO	SUCUA	URBANO4TOCORTE08

Tabla 5.1: Detalle de provincias existentes en la tabla datos. Parte 1.
Fuente: Autor de tesis.

CAMPO PROVINCIA	CAMPO CANTON	CAMPO NOMBRE DEL PROYECTO
NAPO	EL CHACO	URBANO4TOCORTE08
NO DELIMITADAS	LA CONCORDIA	SIV-MEJORAMIENTO
ORELLANA	FCO. DE OR	DAYUMA 2
PASTAZA	PASTAZA	CONVENIO-HUAORANI
PICHICHA	MEJIA	TESALIA 2
PICHICHINCHA	MEJIA	SAN IGNACIO DE CUTUGLAHUA
PICHINCCHA	CAYAMBE	CASHAPAMBA
PICHINCHA	CAYAMBE	OLMEDO
QUININDE	ESMERALDAS	LAS MALVINAS
SAN ISIDRO	COLTA	GUACONA
SANTA ELEN	SALINAS	BARRIO NUEVO
SANTA ELENA	SANTA ELENA	SAN ISIDRO
SANTAELENA	LALIBERTAD	GALICIA DE LA LIBERTAD
SANTO DOMINGO	SANTO DOMINGO	PARROQUIA PUERTO LIMON
SANTO DOMINGO DE LOS	SANTO DOMINGO	URBANO4TOCORTE08
SANTO DOMINGO DE LOS TSACHILAS	STO.DOMINGO	ALLURIQUIN
ST.DG.TSA.	SATO. DGO.	COOP. MAYA MONCAYO
ST.DG.TSCH	STO. DGO.	COOP. JORGE MAHUAD G1
ST.DGO. TS	STO. DGO.	COOP. JORGE MAHUAD
STA ELENA	SALINAS	SALINAS EMERGENTE
STA. ELENA	STA. ELENA	LAS BRISAS
STO DGO TS	SATO. DGO.	CONGOMA CHICO G4
STO. DOMINGO DE LOS TSACHILAS	STO.DOMINGO	SIV- MAGISTERIO-2008-P
STO. T. SA	SATO. DGO.	COOP. JORGE MAHUAD G2
STO.DGO.TS	SANTO DOMI	SRA. PAZOS LUZ AMERICA
STO.DOMING	STO.DOMING	RECINTO ZARACAY
SUCUMBIO	LAGO AGRIO	SAN VALENTIN
SUCUMBIOS	LAGO AGRIO	SAN BARTOLO
TSACHILA	STO. DGO.	RECINTO LAS MERCEDES
TUNGUAHUA	PELILEO	SURANGAY-CUBRE CUPOS
TUNGURAHUA	AMBATO	TONDOLIQUE - QUISAPINCHA
ZAMORA	C. CONDOR	TUNTIAK BARRIOS ALEDAÑOS
ZAMORA CH.	EL PANGUI	LA RECTA Y BARRIOS ALEDAÑ
ZAMORA CHINCHIPE	ZAMORA	URBANAPRIMERCORTE2008

Tabla 5.2: Detalle de provincias existentes en la tabla datos. Parte 2.
Fuente: Autor de tesis.

5.2. HERRAMIENTAS PARA PROCESAMIENTO Y MANEJO DE INFORMACIÓN.

Existen varias herramientas y gestores de bases de datos que fueron creadas para trabajar con cientos de tablas con la funcionalidad de manejar relaciones entre ellas.

Entre las principales herramientas para el manejo de bases de datos se mencionarán algunas.

Según el tipo de gestor de base de datos:

MySQL-Front: administración de bases de datos con MySQL.

PgAdmin: administración de bases en PostgreSql.

Aqua Data Studio: administración de bases relacionales en Oracle.

SQL Server Managment Studio: administración de bases en SQL SERVER.

Según su funcionalidad:

SPSS Statistics: Herramienta con múltiples opciones para estadística.

DataAdmin: Herramienta de fácil instalación, muy liviano y de fácil manejo.

DBDesigner: Herramienta de edición, creación y administración de datos.

5.2.1. UTILIZACIÓN DE UN SGDB COMO HERRAMIENTA PRIVATIVA.

En este punto se mostrará de forma general las principales funcionalidades de esta herramienta, con datos de los beneficiarios de los bonos de vivienda.

Se podrá comparar y verificar si el gestor de base de datos de Oracle procesa más rápido la información que un gestor creado con Software Libre.

Las pruebas a realizarse estarán enfocadas al tiempo de ejecución en el procesamiento de datos, ya que al automatizar procesos de una empresa o institución mediante el desarrollo de aplicaciónes web, el tiempo de procesamiento es un factor muy determinante en el sistema.

5.2.1.1 INSTALACIÓN Y CONFIGURACIÓN DE ORACLE 10g EE

Para poder utilizar esta herramienta se instalará la versión de oracle 10g express edition, ya que es más liviana y muestra una interfaz amigable al usuario.

Luego de ingresar con el user y password configurados en la instalación se podrá visualizar las opciones que tiene oracle 10g XE, como se muestra en la siguiente figura.

Figura 5.9: Interfaz principal del menú de Oracle Database Express Edition, luego de instalación.
Fuente: Autor de tesis.

5.2.1.2 PRINCIPALES FUNCIONALIDADES DE LA HERRAMIENTA.

Una de las funcionalidades más importantes es el poder manejar bases de datos que provienen de otros sistemas.

Es así que esta herramienta tienen las opciones de DATA LOAD / UNLOAD, que permitirá migrar datos de un sistema a Oracle 10g EX.

Ejemplo:

El primer paso será importar la sentecia SQL que contiene la estructura de la tabla nacional de los beneficiarios de bonos de vivienda.

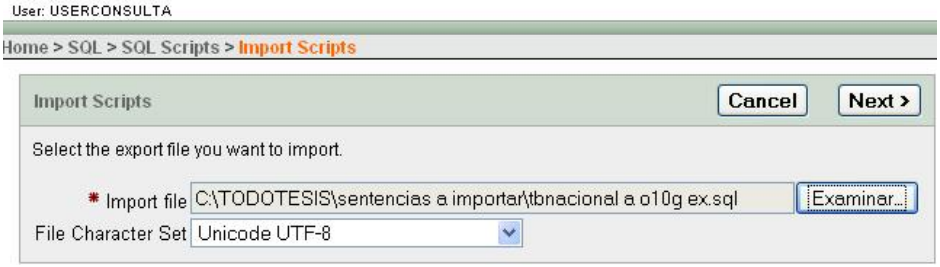


Figura 5.10: Interfaz para generar los scripts de importación de datos.
Fuente: Autor de tesis.

En la siguiente figura se puede apreciar la sentencia SQL que va a ser ejecutada en el gestor de base de datos.

Se creará exactamente el mismo modelo de diseño para la tabla nacional, ya que se requiere obtener todos los registros de los beneficiarios de bonos.

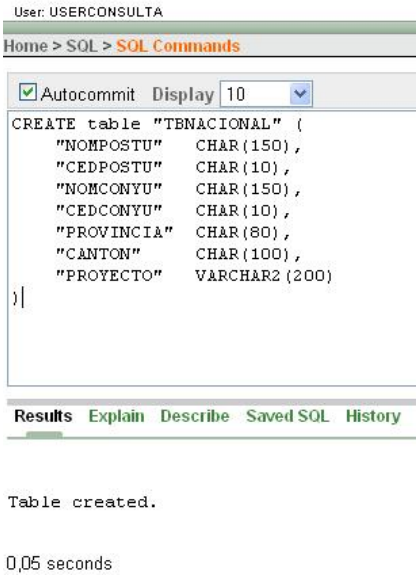


Figura 5.11: Detalle de la consulta SQL generada por Oracle Database Express.
Fuente: Autor de tesis.

Luego de tener la tabla creada, se procederá a realizar el proceso de importación de datos desde un archivo plano.

Se deberá ingresar a la opción Data Load / Unload y escoger la opción "**Load Text Data",** lo que permitirá escoger el archivo a importarse.

Figura 5.12: Menú de opciones de Data Load / Unload al momento de importar archivos.
Fuente: Autor de tesis.

Como se muestra en la figura siguiente, se debe definir también el tipo de separador y si existe un carácter de terminación de línea.

La codificación o Character Set, se debe configurar de acuerdo al archivo que se va a importar, ya que si se escoge la opción equivocada se generará errores en el proceso y no se obtendrá una carga satisfactoria.

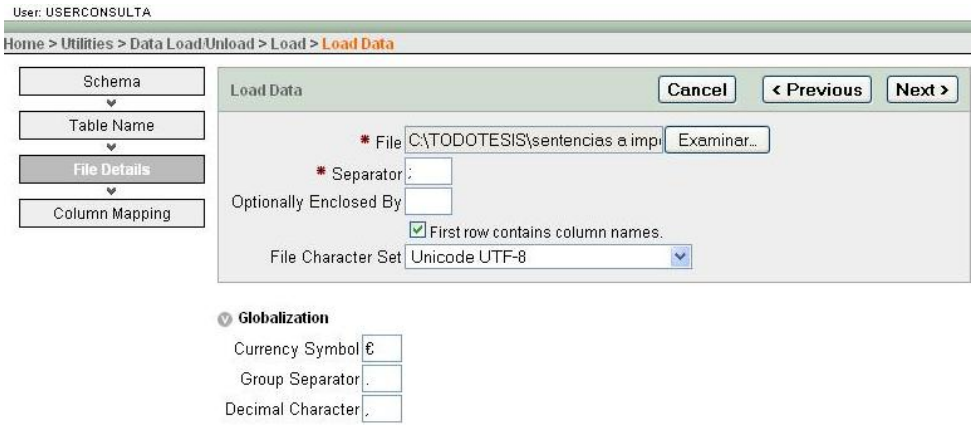
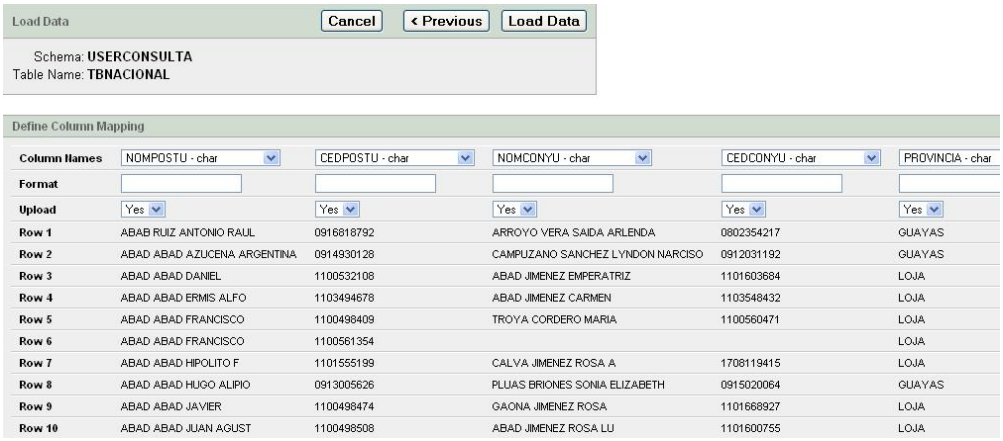


Figura 5.13: Definición del tipo de separador y charset en la pantalla de Load Data.
Fuente: Autor de tesis.

Luego antes de presionar el botón "Load Data", se debe verificar por última vez que todos los parámetros estén de acuerdo a los requerimientos.

El tiempo de importación estará de acuerdo a el número de registros que tenga el archivo plano, existen archivos muy livianos que pueden estar en el rango de los KBytes y otros que su contenido es tan grande y su tamaño varía entre 1 y 2 GB.



Column Names	NOMPOSTU - char	CEDPOSTU - char	NOMCONYU - char	CEDCONYU - char	PROVINCIA - char
Format					
Upload	Yes	Yes	Yes	Yes	Yes
Row 1	ABAB RUIZ ANTONIO RAUL	0916818792	ARROYO VERA SAIDA ARLENDA	0802354217	GUAYAS
Row 2	ABAD ABAD AZUCENA ARGENTINA	0914930128	CAMPUZANO SANCHEZ LYNDON NARCISO	0912031192	GUAYAS
Row 3	ABAD ABAD DANIEL	1100532108	ABAD JIMENEZ EMPERATRIZ	1101603684	LOJA
Row 4	ABAD ABAD ERMIS ALFO	1103494678	ABAD JIMENEZ CARMEN	1103548432	LOJA
Row 5	ABAD ABAD FRANCISCO	1100498409	TROYA CORDERO MARIA	1100560471	LOJA
Row 6	ABAD ABAD FRANCISCO	1100561354			LOJA
Row 7	ABAD ABAD HIPOLITO F	1101555199	CALVA JIMENEZ ROSA A	1708119415	LOJA
Row 8	ABAD ABAD HUGO ALIPIO	0913005626	PLUAS BRIONES SONIA ELIZABETH	0915020064	GUAYAS
Row 9	ABAD ABAD JAVIER	1100498474	GAONA JIMENEZ ROSA	1101668927	LOJA
Row 10	ABAD ABAD JUAN AGUST	1100498508	ABAD JIMENEZ ROSA LU	1101600755	LOJA

Figura 5.14: Vista previa de resultados antes de finalizar la importación.
Fuente: Autor de tesis.

Esta herramienta es muy amigable al usuario y en cuanto a la velocidad de procesamiento de datos se puede asegurar que funciona muy rápidamente, es decir, que tiene un rendimiento alto si se quisiera implementar con un sistema tipo web.

5.2.2. UTILIZACIÓN DEL SGBD COMO HERRAMIENTA OPEN SOURCE.

Para mostrar la herramienta open source de gestión de base de datos, se escogió PgAdmin III, muy conocida en la actualidad, ya que fue una de las pioneras en lo que respecta al procesamiento de bases de datos con Postgres.

Las principales características al utilizar PgAdmin III son las siguientes:

- Es un proyecto OperSource, por lo tanto, un grupo grande de desarrolladores trabaja para mejorar este SGBD.
- Trabaja con bases relacionales orientada a objetos y es multiplataforma.
- Es un motor de alta concurrencia, ya que permite el acceso a una tabla de diferentes fuentes para realizar diferentes acciones.
- Variedad de tipos de datos, un gran avance es PostGIS, para datos espaciales y georeferenciados.
- Posee gran acoplamiento con funciones, triggers, vistas, claves foráneas.

5.2.2.1 CONFIGURACIÓN DE PgAdmin III Y EMS Data Import for Postgres.

La instalación de PgAdmin se mostrará en una forma resumida, indicando las configuraciones más importantes que se deben tomar en cuenta.

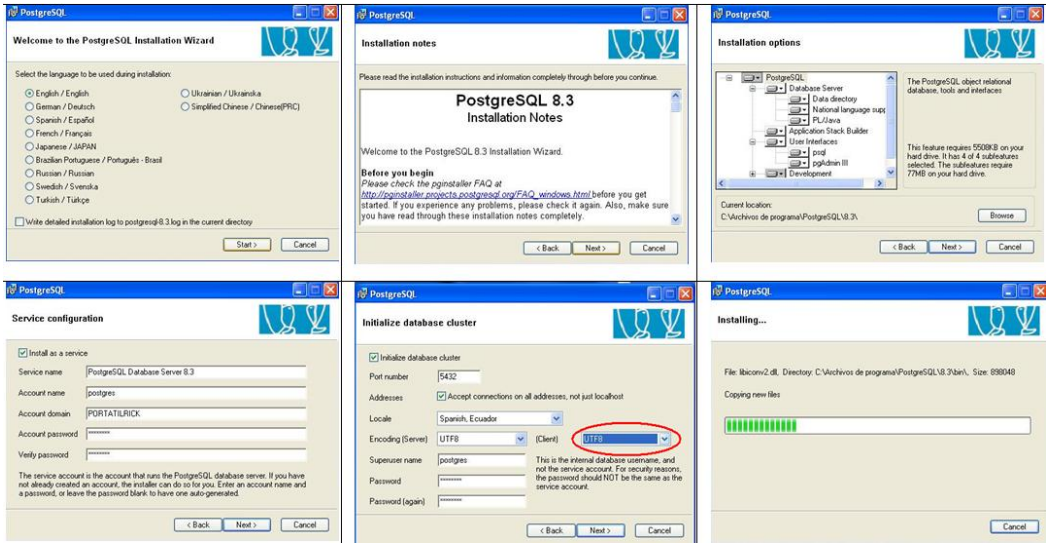


Figura 5.15: Proceso de instalación y configuración de la herramienta Postgres.
Fuente: Autor de tesis.

Se recomienda utilizar la codificación UTF-8 tanto para el cliente y el servidor, ya que la utilización de caracteres especiales, letra “ñ”, tildes y demás caracteres propios del lenguaje castellano, no se presentarán correctamente si no se utiliza esta codificación.

Luego de finalizada la instalación de Postgres, se procederá a la instalación de la herramienta PgAdmin III.

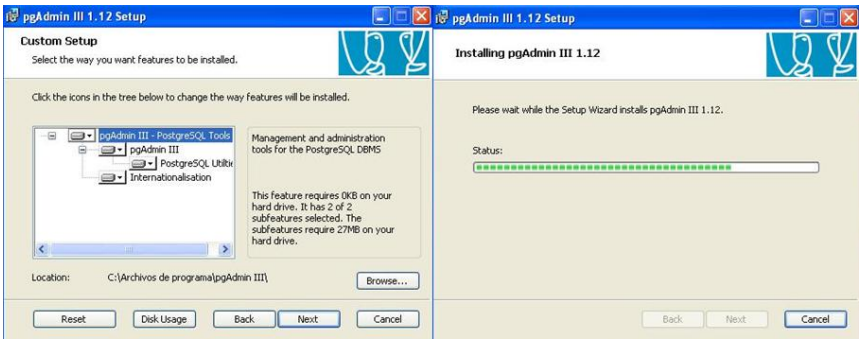


Figura 5.16: Selección de paquetes a instalarse con PgAdmin.
Fuente: Autor de Tesis.

Como se aprecia en la figura, se instalan las principales utilidades de esta herramienta. Luego finalizará la instalación y se procederá a ejecutarla.

5.2.2.2 PRINCIPALES FUNCIONALIDADES DE LA HERRAMIENTA.

Luego de instalar PgAdmin III, se procederá a abrir la herramienta para poder ingresar la contraseña y así poder iniciar la conexión.

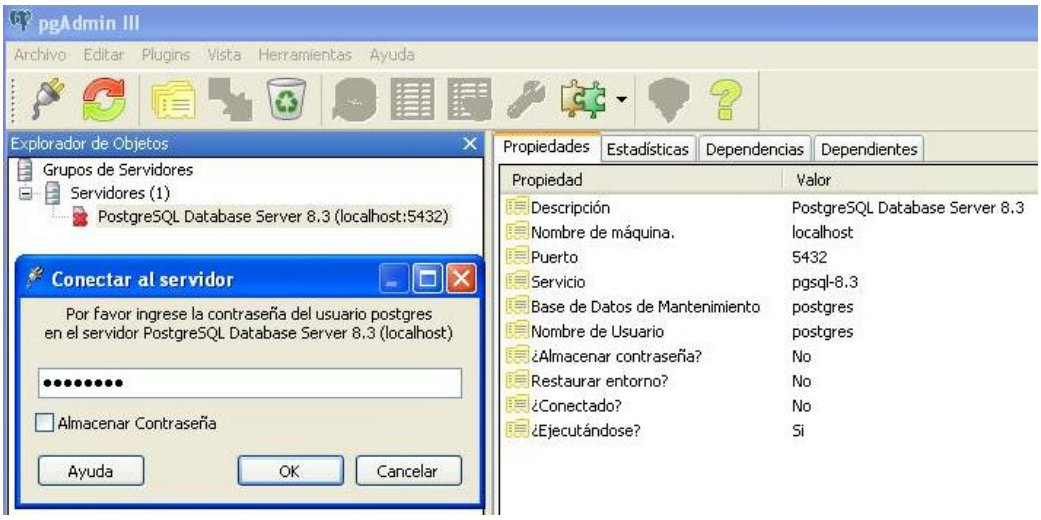


Figura 5.17: Ingreso de contraseña para iniciar la conexión con el servidor postgres desde Pgadmin III. Fuente: Autor de tesis.

Para probar el funcionamiento con Postgres, se procederá a realizar un ejemplo de importación de datos con la tabla de los beneficiarios de bonos.

Ejemplo:

Para este ejemplo se procederá a crear la tabla nacional para iniciar la importación de datos que se manejan en la tabla de Microsoft Access. Luego de obtener los datos en PgAdmin, se probará el rendimiento y funcionamiento.

5.2.2.3 INSTALACIÓN Y MIGRACIÓN DE DATOS CON EMS Data Import .

La instalación de esta aplicación es esencial para realizar el proceso de importación de datos, EMS data import es una poderosa aplicación que permite realizar imports desde varias fuentes de datos. El único inconveniente es que tiene costo de licencia para su completo funcionamiento.

Como se aprecia en la siguiente figura, la pantalla muestra el wizard para la conexión a las bases de datos creadas.

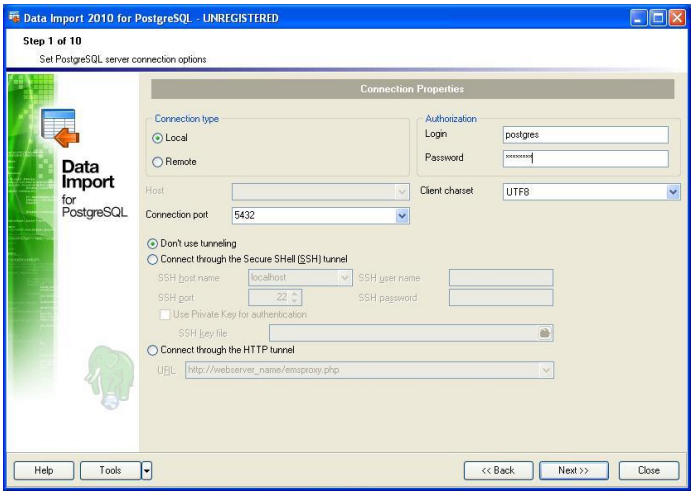


Figura 5.18: Configuración inicial para la importación de datos utilizando Data Import.
Fuente: Autor de tesis.

Se define el puerto de conexión, el password y el charset que es muy importante definirlo correctamente.

En la siguiente figura se selecciona la tabla a la cual serán importados los datos del archivo texto que contiene los datos de beneficiarios del bono.

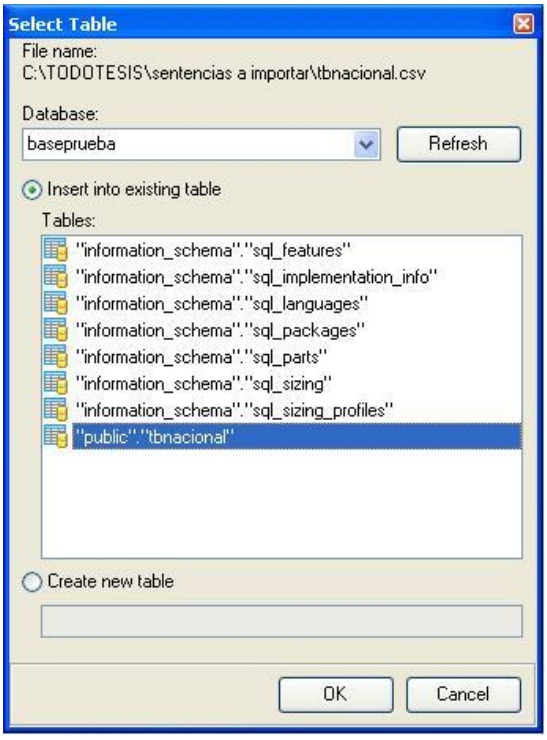


Figura 5.19: Selección de "tbnacional" en el listado de tablas que presenta Data Import.
Fuente: Autor de tesis.

En la siguiente figura se define el delimitador y el Enconding, éste último es muy importante ya que si no se escoge correctamente los datos serán importados con errores, tal como se aprecia en la siguiente figura.

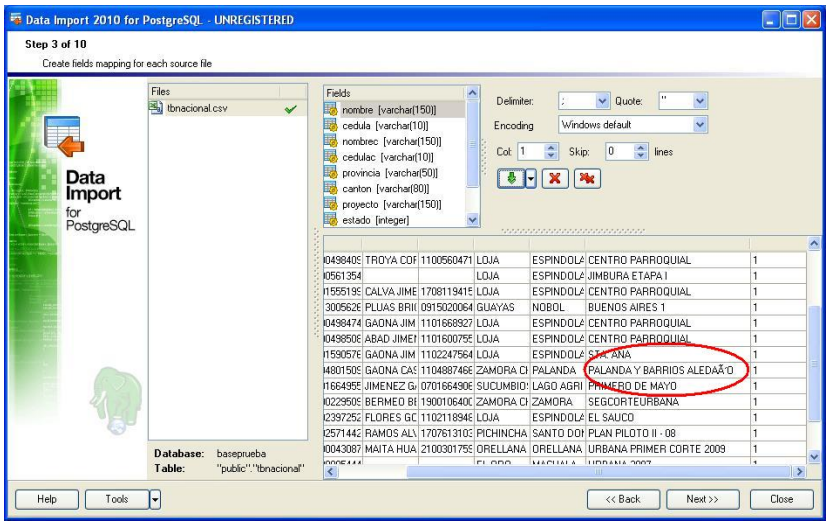


Figura 5.20: Vista previa de los registros a importarse utilizando un encoding incorrecto.
Fuente: Autor de tesis.

Para solucionar este problema se debe escoger el Encoding “Unicode UTF-8”, ya que el archivo plano del cual se importan los datos viene en ese formato.
Como se visualiza en la figura, ya no existen errores de importación.

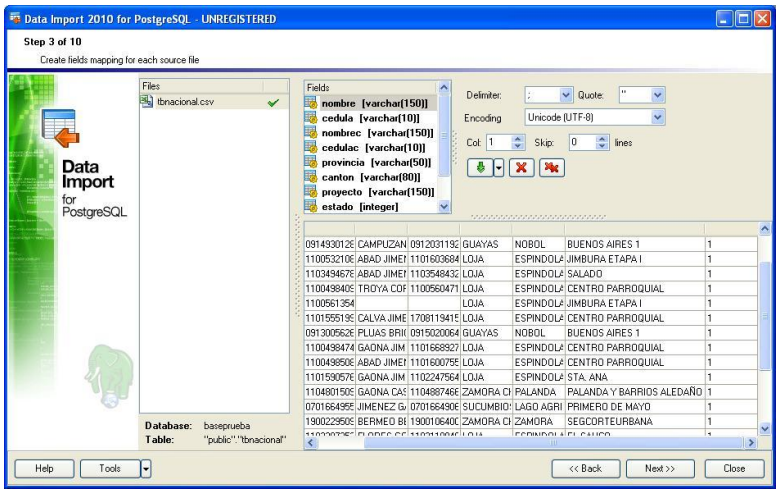


Figura 5.21: Vista previa de los registros a importarse utilizando un encoding correcto.
Fuente: Autor de tesis.

Se debe seguir con el Wizard y al final mostrará un mensaje de “Finalizada la importación”. Este pequeño ejemplo muestra una forma fácil y rápida de migrar datos de un formato a PgAdmin III, y de esta manera obtener todas las ventajas que tiene la herramienta.

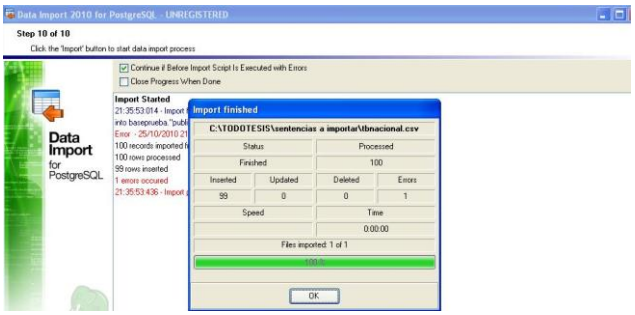


Figura 5.22: Pantalla de finalización del proceso de importación con Data Import.
Fuente: Autor de tesis.

5.2.3. UTILIZACIÓN DE UN HERRAMIENTA ORIENTADA A LA ESTADÍSTICA, SPSS STATISTICS.

Para este punto se estudiará y analizará las principales bondades de la herramienta SPSS Statistics, que es un software enfocado mayormente a los cálculos estadísticos.

La razón por la cual se presenta la herramienta es porque la estadística ha adquirido, de manera progresiva, una mayor relevancia en varios sectores de la sociedad. En el caso del MIDUVI, se requiere generar reportes con estas características y es por esto que se pretende ahondar un poco sobre este tema.

5.2.3.1 PRINCIPALES OPCIONES Y FUNCIONES DE SPSS

La ventana principal se presenta en la siguiente figura, y es muy fácil explorar sus menús y opciones ya que se asemeja mucho a un procesador de texto, como es el Excel.Una particularidad de esta herramienta es que las columnas tienen un nombre común “var”, pero puede ser cambiado según se requiera.

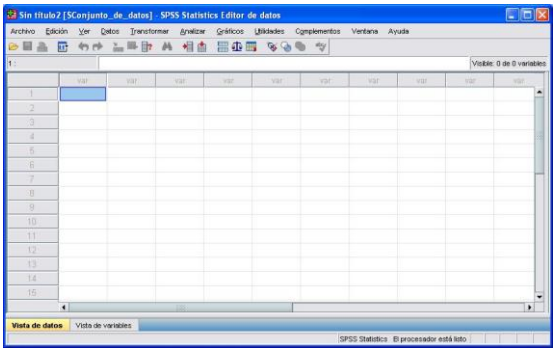


Figura 5.23: Pantalla principal de la herramienta SPSS.
Fuente: Autor de tesis.

5.2.3.2 MIGRACIÓN DE DATOS AL FORMATO DE SPSS.

Para el proceso de migración a SPSS se utilizará el programa StatTransfer 8.0, esta aplicación es muy fácil de utilizar y exporta los datos al formato requerido.

Ejemplo:

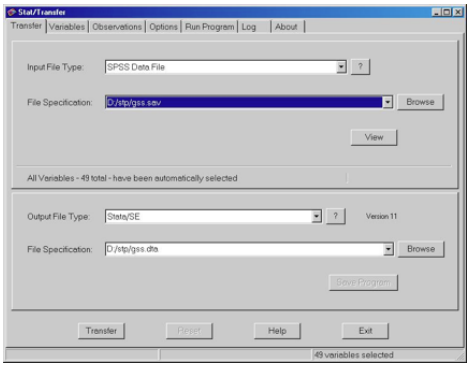


Figura 5.24: Pantalla principal de stat transfer para la migración de datos al formato .SAV.
Fuente: Autor de tesis.

Como se aprecia en la figura en tan solo 2 pasos se pudo obtener el archivo "BASECALIFIDOS.SAV", la cual se abrirá con la herramienta SPSS y se podrá realizar algunas acciones interesantes.

5.2.3.3 FUNCIONES MAS UTILIZADAS DEL SPSS.

Al abrir el archivo con la herramienta, se presenta la siguiente figura, con la cual se debe escoger la opción Abrir un origen de datos existente.

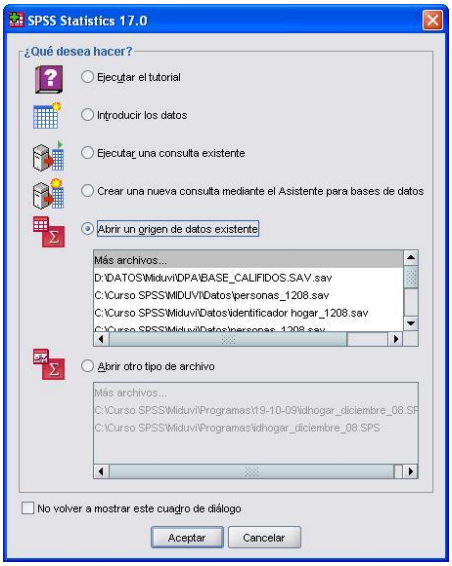
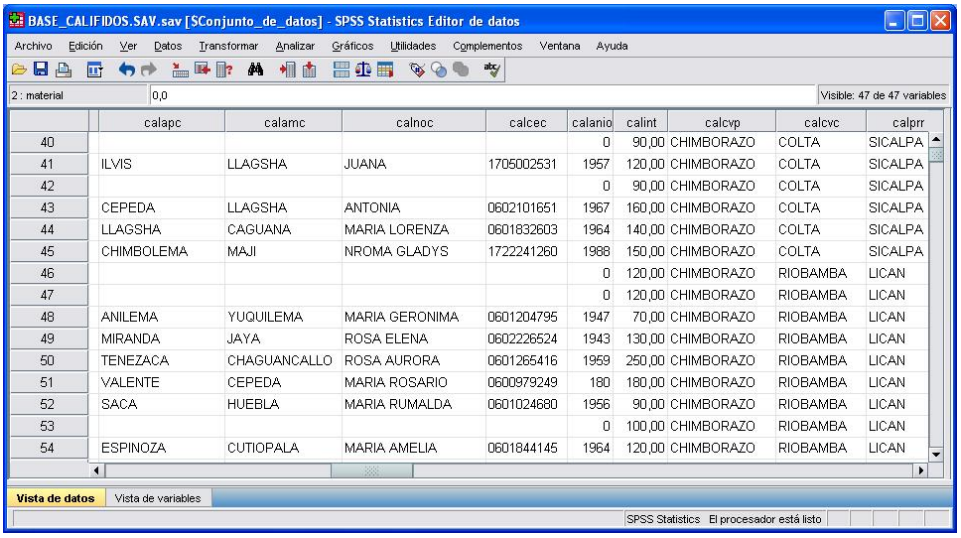


Figura 5.25: Ventana de opciones al momento de abrir un archivo existente en SPSS.
Fuente: Autor de tesis.

Luego de seleccionar la opción, se presentará ya los datos y registros que contiene el archivo BASECALIFIDOS, donde consta información sobre los beneficiarios de bonos de vivienda.



	calapc	calamc	calnoc	calcec	calanio	calint	calcvp	calcvc	calprr
40					0	90,00	CHIMBORAZO	COLTA	SICALPA
41	ILVIS	LLAGSHA	JUANA	1705002531	1957	120,00	CHIMBORAZO	COLTA	SICALPA
42					0	90,00	CHIMBORAZO	COLTA	SICALPA
43	CEPEDA	LLAGSHA	ANTONIA	0602101651	1967	160,00	CHIMBORAZO	COLTA	SICALPA
44	LLAGSHA	CAGUANA	MARIA LORENZA	0601832603	1964	140,00	CHIMBORAZO	COLTA	SICALPA
45	CHIMBOLEMA	MAJI	NROMA GLADYS	1722241260	1988	150,00	CHIMBORAZO	COLTA	SICALPA
46					0	120,00	CHIMBORAZO	RIOBAMBA	LICAN
47					0	120,00	CHIMBORAZO	RIOBAMBA	LICAN
48	ANILEMA	YUQUILEMA	MARIA GERONIMA	0601204795	1947	70,00	CHIMBORAZO	RIOBAMBA	LICAN
49	MIRANDA	JAYA	ROSA ELENA	0602226524	1943	130,00	CHIMBORAZO	RIOBAMBA	LICAN
50	TENEZACA	CHAGUANCALLO	ROSA AURORA	0601265416	1959	250,00	CHIMBORAZO	RIOBAMBA	LICAN
51	VALENTE	CEPEDA	MARIA ROSARIO	0600979249	180	180,00	CHIMBORAZO	RIOBAMBA	LICAN
52	SACA	HUEBLA	MARIA RUMALDA	0601024680	1956	90,00	CHIMBORAZO	RIOBAMBA	LICAN
53					0	100,00	CHIMBORAZO	RIOBAMBA	LICAN
54	ESPINOZA	CUTIOPALA	MARIA AMELIA	0601844145	1964	120,00	CHIMBORAZO	RIOBAMBA	LICAN

Figura 5.26: Modo en vista de datos que presenta la herramienta SPSS.
Fuente: Autor de tesis.

Sobre esta base de datos se pueden realizar un sin número de acciones, y generar reportes para la toma de decisiones.

Para el ejemplo siguiente se tomará una base de 80000 registros aproximadamente, los cuales serán sometidos a una consulta de beneficiarios de bono con frecuencia de hombres vs mujeres.

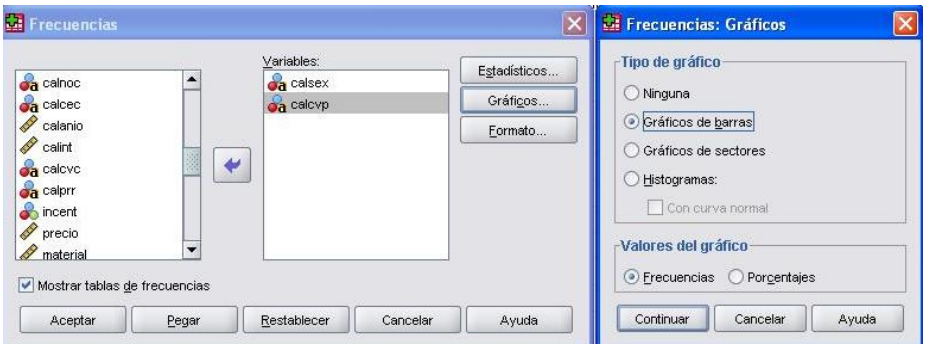


Figura 5.27: Ventanas de opción para el cálculo de frecuencias con gráficos de barras en SPSS.
Fuente: Autor de tesis.

Como se presentó en la anterior figura, se presionó en la barra de menú, la opción Analizar -- > Frecuencias.

En este caso se escogió la variable “calsex”, que contiene la variable del sexo de la persona beneficiaria. Adicionalmente se pueden escoger opciones de estadística, gráficos y el formato en el cual se generarán los reportes.

Para el ejemplo se escogió que además de los resultados de frecuencia, el programa genere un gráfico representando el reporte.
La siguiente figura expone los resultados arrojados por SPSS, en el cual la primera tabla se refiere a los datos con los cuales la herramienta proceso la información.

Frecuencias

[$Conjunto_de_datos] D:\DATOS\Miduvi\DPA\BASE_CALIFIDOS.SAV.sav

Estadísticos

		calsex	calcvp
N	Válidos	80999	80999
	Perdidos	0	0

Tabla de frecuencia

calsex

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos		23	,0	,0	,0
	F	40965	50,6	50,6	50,6
	M	40011	49,4	49,4	100,0
	Total	80999	100,0	100,0	

Figura 5.28: Resultado del reporte de frecuencias emitido por SPSS.
Fuente: Autor de tesis.

Para finalizar, la siguiente figura muestra un gráfico de barras con la frecuencia de F (Mujeres) vs M (Hombres), en el cual se puede apreciar de manera general el porcentaje de personas que recibieron el bono de vivienda.
Como se puede visualizar la herramienta SPSS muestra reportes muy claros y explicativos, que ayudan a entender de mejor manera los resultados finales.

Esta es una de las tantas bondades que brinda la herramienta SPSS, existen muchas más que podrían servir para generar proyecciones a futuro para tratar de focalizar y entregar incentivos de vivienda a las personas más pobres y que más lo necesitan.

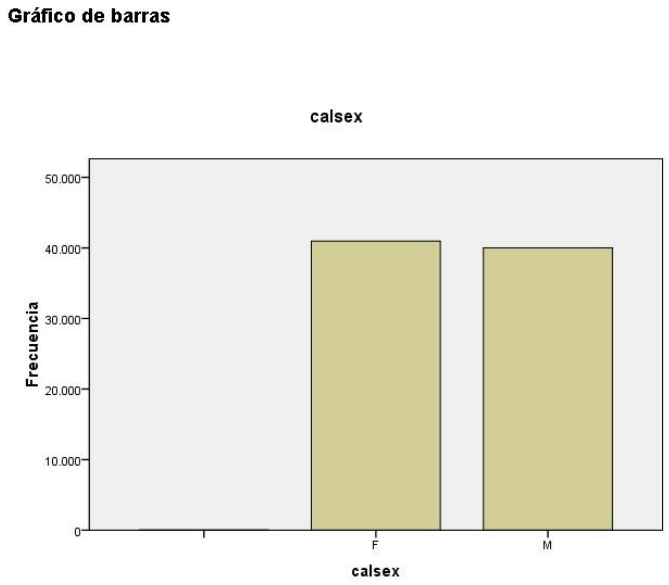


Figura 5.29: Gráfico de barras con la frecuencia de Mujeres v.s Hombres como beneficiarios.
Fuente: Autor de tesis.

5.3. GESTIÓN DE ALMACENAMIENTO Y COPIAS DE SEGURIDAD PARA EL MEJOR ALOJAMIENTO DE LA INFORMACIÓN

La función de un sistema informático además de proporcionar aplicaciones para automatizar procesos eficientemente, debe proveer del espacio suficiente de almacenamiento de la información para que los usuarios puedan realizar su trabajo diario.

Hay que tomar en cuenta que los usuarios no solamente guardan archivos de texto que varían entre los 100 y 200 KB, sino también que un usuario común trabaja con aplicaciones que generan archivos muchos más pesados como ARCGIS, Autocad, Corel X5, etc.

Si a todo esto se le suma algunos gigabytes del correo acumulado que guarda de algunos años atrás, los servidores fácilmente podrían colapsar.

Para este subcapítulo se presentará algunas alternativas para gestionar de mejor manera al crecimiento de la información y además conocer algunas de las técnicas para realizar copias de seguridad efectivas.

5.3.1. INSTALACIÓN Y CONFIGURACIÓN DE LVM.

Este ejemplo se lo realizará en Debian, para mostrar cómo se crea un LVM (Gestión de Volúmenes Lógicos).

INSTALACIÓN DEL PAQUETE LVM

La sintaxis utilizada es:

aptitude install –y lvm2

El comando anterior descarga los paquetes y complementos necesarios e instala el paquete lvm2, como se aprecia en la figura.

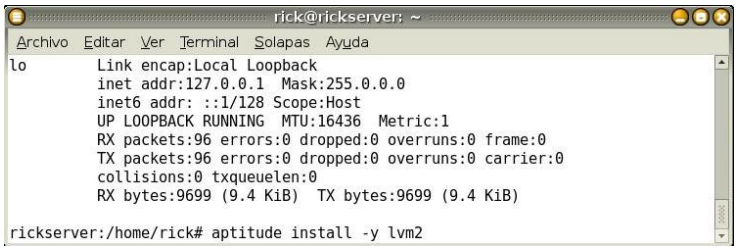


Figura 5.30: Instalación de lvm2 mediante la consola de Debian, utilizando el comando aptitude.
Fuente: Autor de tesis.

Luego de esto, si el proceso de instalación continúa sin errores saldrá la siguiente figura indicando que se completó la instalación.

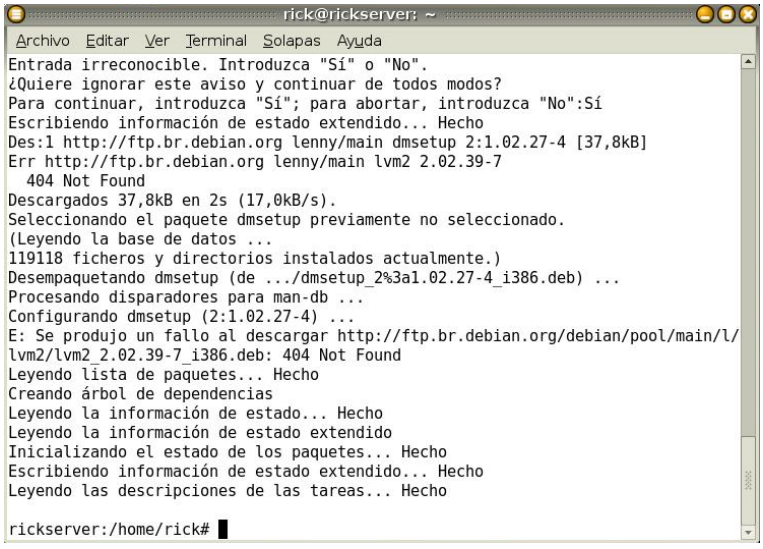


Figura 5.31: Configuración de la herramienta en el proceso de instalación de lvm2.
Fuente: Autor de tesis.

Con el paquete instalado ya se puede empezar a configurar el disco duro para tener un LVM y así gestionar de mejor manera el espacio de almacenamiento de discos y por lo tanto la capacidad de la base de datos que está instalada en el servidor.

Figura 5.32: Configuración del disco duro, donde se indica el tipo de disco en el cual se trabajará.
Fuente: Autor de tesis.

En la figura anterior, se ha iniciado la configuración con el paquete, para preparar al disco duro a tener: el volumen físico, el grupo de volúmenes y el volumen lógico.

El siguiente comando ingresado, muestra las particiones de discos actuales.

```
Orden (m para obtener ayuda): p

Disco /dev/sda: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cilindros of 16065 * 512 = 8225280 bytes
Disk identifier: 0x0009aaf2

Disposit. Inicio    Comienzo      Fin      Bloques  Id  Sistema
/dev/sda1               1         196     1574338+  82  Linux swap / Solaris
/dev/sda2             197        1305     8908042+  83  Linux

Orden (m para obtener ayuda): 
```

Figura 5.33: Visualización de las propiedades de los discos actuales con el comando "p".
Fuente: Autor de tesis.

Se tienen 2 particiones, pero se piensa agregar un disco más para poder crear 2 particiones adicionales, 1 extendida y 1 física más, quedando de la siguiente forma:

/dev/sda1	Partición Swap
/dev/sda2	Raíz / Linux
/dev/sda3	Partición Extendida
/dev/sda4	Partición LVM

Tabla 5.3: Tabla resumen de las particiones del equipo servidor donde se aplicará la herramienta.
Fuente: Autor de tesis.

Para finalizar se debe cambiar el identificador a la partición /sda4, con la tecla “t” y guardar toda la configuración con la letra “w”. Luego de reiniciado el equipo se tendrá un LVM estable para la gestión óptima del almacenamiento de datos.

5.3.2. CLONACIÓN DE SISTEMAS.

Una vez que se tiene una máquina configurada adecuadamente, en la cual se esté alojando información importante y que se necesite tener respaldos por cualquier anomalía que pueda suceder, la solución es clonar ese sistema.

INSTALACIÓN DE PARTIMAGE

Este paquete es parecido a Ghost de Symantec, el cual proporciona soporte integrado para transferir el sistema de ficheros comprimido o las imágenes de disco, enviados a servidores centrales usando FTP.

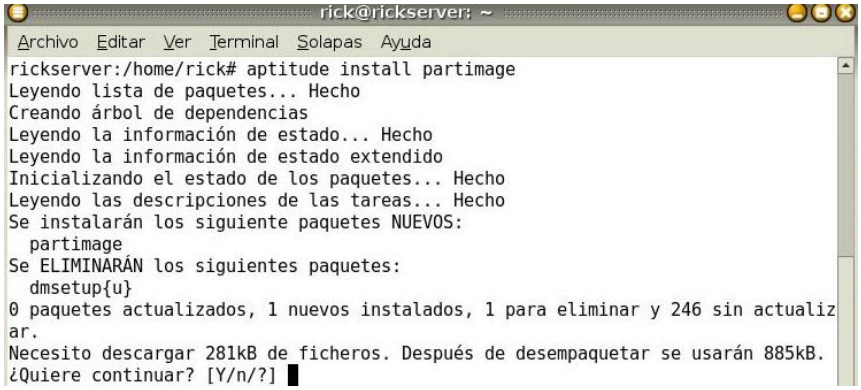


Figura 5.34: Instalación del paquete partimage mediante el comando aptitude.
Fuente: Autor de tesis.

Como se aprecia en la figura anterior, la instalación de partimage empezará y descargará todos los complementos necesarios.

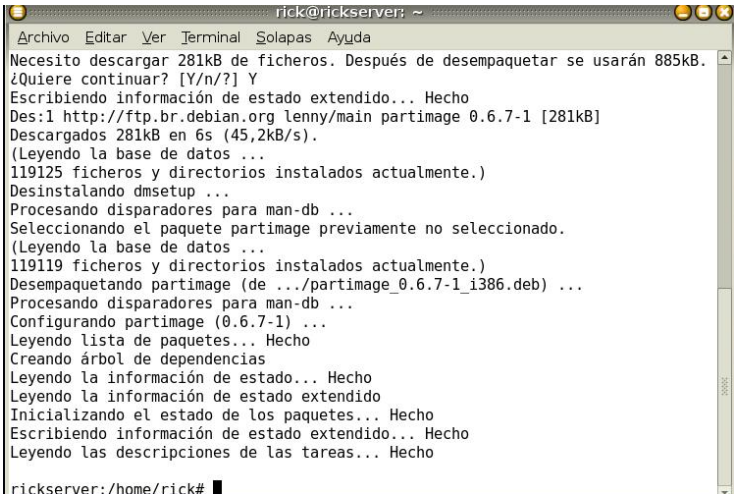


Figura 5.35: Proceso y finalización de la instalación del paquete partimage.
Fuente: Autor de tesis.

Luego de finalizada la instalación se procede a ejecutar el programa.

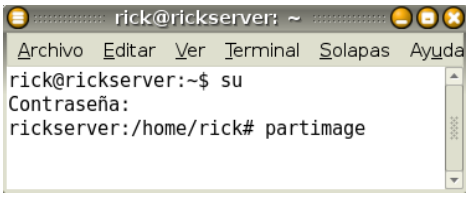


Figura 5.36: Acceso al super usuario root para ejecutar e iniciar la herramienta.
Fuente: Autor de tesis.

Este comando ejecutara lo siguiente:

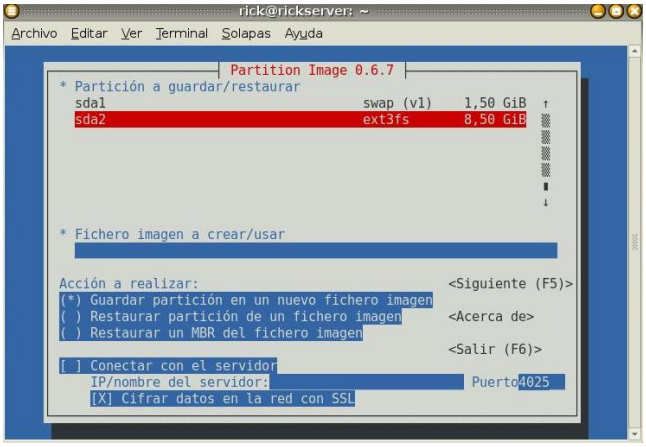


Figura 5.37: Pantalla principal de la herramienta Patition Image luego de haberla iniciado.
Fuente: Autor de tesis.

Y este es el programa que servirá para realizar clonaciones de sistemas de una forma fácil y rápida.

Ejemplo:

Luego de escoger la partición que no esté montada aún, y que se requiera copiar como una imagen se debe configurar algunos parámetros, como por ejemplo el nombre y ruta del archivo imagen a crearse, nivel de compresión, modo de imagen dividida, sobrescribir sin preguntar, etc.

Para seguir con el proceso se debe presionar la tecla F5, como se aprecia en la siguiente figura.

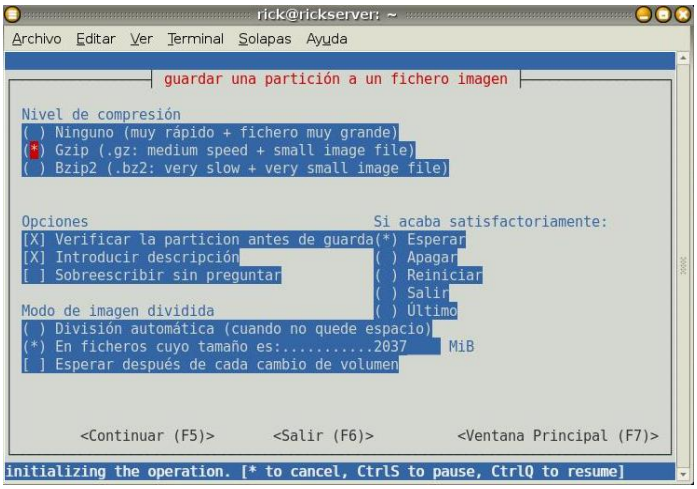


Figura 5.38: Pantalla de opciones y niveles de compresión disponibles.
Fuente: Autor de tesis.

Antes de iniciar el proceso se presenta una pantalla con un resumen de la unidad a copiar para verificar si todo esta correcto.

Figura 5.39: Resumen de parámetros con los cuales se iniciará el proceso de creación de la imagen.
Fuente: Autor de tesis.

Luego de terminado el proceso, se puede verificar en la ruta que se estableció en las primeras pantallas de partimage, que se encuentra la imagen creada.

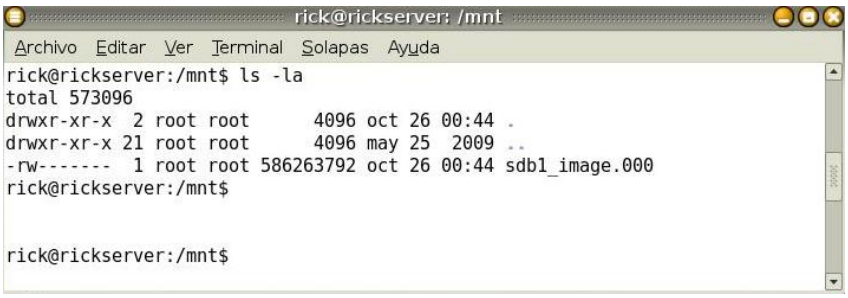


Figura 5.40: Ejecución de comando ls para mostrar los ficheros obtenidos con la herramienta.
Fuente: Autor de tesis.

Para restablecer esta imagen basta cambiar la opción en la parte de “acción a realizar”, logrando restablecer todo el contenido de la unidad.

5.3.3. COPIAS DE SEGURIDAD.

En este último punto del capítulo se pretende hacer conocer una alternativa para las copias de seguridad de grandes discos y que contengan información de gran contenido.
La idea también es evitar que se demore demasiado tiempo en generar respaldos de discos grandes, ya que una empresa no puede esperar varios días para obtener una copia de seguridad.

Para el siguiente ejemplo, se realizará bajo un sistema Linux y con un disco de unos 2TB. El procedimiento a ejecutarse requiere escoger el comando adecuado para facilitar la creación de la copia de seguridad.

#cp –dpRux /home /mnt/home-backup

El comando anterior, posee propiedades y parámetros bien definidos, para obtener una copia segura y confiable.

Pero no tendría sentido utilizar el mismo comando para grandes y pequeños discos, es así, que se podría crear un script pensando en crear un respaldo mucho más personalizado y seguro.

Código Script para realizar un respaldo más personalizado y seguro:

```
#! /bin/bash
# Backup script using cp
#
If [ $#  !=  2 ] ; then
        echo " Uso: script_backup partition backup-device"
        echo " Ejemplo: script_backup  /home / dev / sda1 "
        exit
fi

VERBOSE="no"
STDOPTS="-dpRux"
LOGFILE="/var/log/Backup/simple.log"
TARGETBASE = 'echo $i  | sed  -e  's;^\ / ; ; '  -e  's; \ / ; -  ; g ' '
FULLTARGET = "/mnt/"$TARGETBASE"-backup "
DATE = 'date'
Export BACKUPTASK = " $1 to $2 "
Trap cleanup 1  2  3  6

Cleanup (  ){
Echo  "Ha ocurrido un error,  Se ordenara " | tee  -a  $LOGFILE
DATE = 'date'
umount  $FULLTARGET
echo  "Se aborto el proceso de backups de "  $BACKUPTASK $DATE " | tee –a LOGFILE
exit 1
}

if [ !  -d  /var/log/backup ] ; then
        mkdir  -p  /var/log/Backup
fi
echo "  Inicio simple de backups con " $BACKUPTASK  at  $DATE "  | tee  -a  $LOGFILE

if [ !  -d $FULLTARGET ] ; then
        echo  " Creando punto de montaje $FULLTARGET " |  tee  -a  $LOGFILE
        mkdir  -p  $FULLTARGET
fi
MOUNTED = ' df  |  grep  $FULLTARGET '

if [ "x$MOUNTED" != "x" ] ; then
        echo " Existe una unidad montada en $FULLTARGET -exiting"| tee  -a  $LOGFILE
        exit
fi
mount $2  $FULLTARGET

if [ x$? != "x0" ] ; then
        echo "Montaje del volumen Backup $2 fallido -exiting"| tee  -a  $LOGFILE
        exit
fi
#Este bloque guarda copias de archivos importantes de sistema en todos sus #volúmenes de backups, en especial en el directorio llamado .123_admin.
if [  ! –d  $FULLTARGET"/.123_admin" ] ; then
        mkdir  -p  $FULLTARGET"/.123_admin/conf"
fi
```

```
echo " Respaldando los archivos de sistema en $FULLTARGET/.123_admin " | tee –a $LOGFILE
cd /etc
cp -u passwd group shadow $FULLTARGET"/.123_admin"
if [ -d sysconfig ] ; then
        cp -uR sysconfig $FULLTARGET"/.123_admin"
fi
find . –name "*.conf" -print | while read file ; do
        cp -u $file $FULLTARGET"/.123_admin/conf"
done
# En este momento se está actualizando los backups.
DATE = 'date'
echo " Comenzando el backup actual of $BACKUPTASK en $DATE " | tee -a $LOGFILE
cd $1

if [ x$VERBOSE != "xno" ] ; then
        cp $STDOPTS"v" . $FULLTARGET
else
        cp $STDOPTS . $FULLTARGET
fi
umount $FULLTARGET
DATE = 'date'
echo " Se ha completado el script para Backup de $BACKUPTASK en $DATE " | tee –a $LOGFILE
```

Modo de utilizar:

Si por ejemplo se quisiera copiar la carpeta /mnt/videos al disco duro de la PC, se debería utilizar el siguiente comando:

 # /usr/local/bin/script_backup /mnt/videos /dev/sda1

Y se podría tener un control más específico de todo el proceso de creación de una copia de seguridad personalizada y creada mediante un script.

6. CAPÍTULO: PROPUESTA DE SEGURIDAD PARA EL MIDUVI.

El capítulo final se enfocará a las soluciones prácticas que se han analizado y se han puesto a prueba en los servidores que manejan las bases de datos de beneficiarios de bonos que otorga el Ministerio de Desarrollo Urbano y Vivienda.
Todas estas soluciones experimentales han sido cuidadosamente estudiadas previamente y con la ayuda de herramientas de virtualización que existen en la actualidad se ha podido generar ambiente de pruebas que se asemeja al funcionamiento de los servidores que trabajan en producción.

La idea de presentar las siguientes soluciones es que se pueda analizar cada una de ellas y al final se proponga aplicarlas e implementarlas, ya que están pensadas para que el MIDUVI pueda explotar estas herramientas tecnológicas a su beneficio y que gracias a la variedad de funcionalidades que brindan, se pueda llegar a entregar un servicio de calidad.

6.1. SOLUCIÓN 1: MIGRACIÓN DE DATOS DE LOS BENEFICIARIOS DE BONOS DE VIVIENDA PARA UNA MEJOR ADMINISTRACIÓN

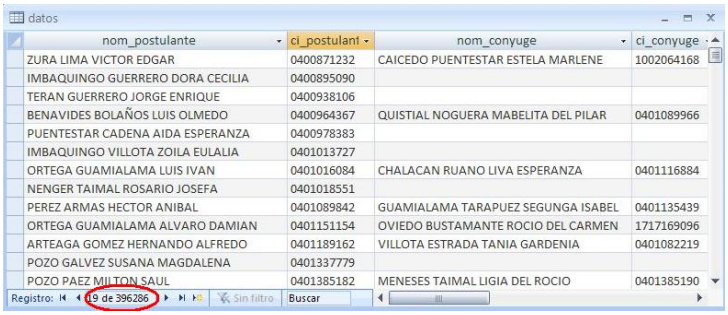
La solución Nº 1, consiste en migrar las tablas de Microsoft Access que contienen registros de beneficiarios de bonos de vivienda a una base de datos relacional MySQL que permite interoperabilidad con aplicaciones web.

Existe un gran problema en la migración de estas tablas ya que toda la información histórica que posee la institución ha sido ingresada con la ausencia de un sistema informático que gestione una base de datos centralizada. Si se resume el problema se puede decir que existen 24 bases de datos ya que existen 24 provincias en el Ecuador que registran información de bonos de vivienda.

6.1.1. ANÁLISIS DE LA MATRIZ DE DATOS DE BENEFICIARIOS.

Para tratar de comprender con que información se debe trabajar se puede mostrar la tabla de Microsoft Access que aloja los registros de beneficiarios que recibieron el bono de vivienda otorgado por el MIDUVI.

Como se visualiza en la siguiente figura, existen aproximadamente 400000 registros, de toda la historia de incentivos de vivienda entregados a las personas ecuatorianas por parte del Ministerio de Vivienda.



datos

nom_postulante	ci_postulant	nom_conyuge	ci_conyuge
ZURA LIMA VICTOR EDGAR	0400871232	CAICEDO PUENTESTAR ESTELA MARLENE	1002064168
IMBAQUINGO GUERRERO DORA CECILIA	0400895090		
TERAN GUERRERO JORGE ENRIQUE	0400938106		
BENAVIDES BOLAÑOS LUIS OLMEDO	0400964367	QUISTIAL NOGUERA MABELITA DEL PILAR	0401089966
PUENTESTAR CADENA AIDA ESPERANZA	0400978383		
IMBAQUINGO VILLOTA ZOILA EULALIA	0401013727		
ORTEGA GUAMIALAMA LUIS IVAN	0401016084	CHALACAN RUANO LIVA ESPERANZA	0401116884
NENGER TAIMAL ROSARIO JOSEFA	0401018551		
PEREZ ARMAS HECTOR ANIBAL	0401089842	GUAMIALAMA TARAPUEZ SEGUNGA ISABEL	0401135439
ORTEGA GUAMIALAMA ALVARO DAMIAN	0401151154	OVIEDO BUSTAMANTE ROCIO DEL CARMEN	1717169096
ARTEAGA GOMEZ HERNANDO ALFREDO	0401189162	VILLOTA ESTRADA TANIA GARDENIA	0401082219
POZO GALVEZ SUSANA MAGDALENA	0401337779		
POZO PAEZ MILTON SAUL	0401385182	MENESES TAIMAL LIGIA DEL ROCIO	0401385190

Registro: 19 de 396286 | Sin filtro | Buscar

Figura 6.1: Análisis de la tabla "datos" de Microsoft Access, mostrando los registros de beneficiarios.
Fuente: Autor de tesis.

Este repositorio de datos se alimenta de datos enviados de las 24 provincias de Ecuador, mediante un proceso de carga de información y validación de duplicidad con la ayuda de una aplicación desarrollada en Visual Basic, que se presenta en la siguiente figura.

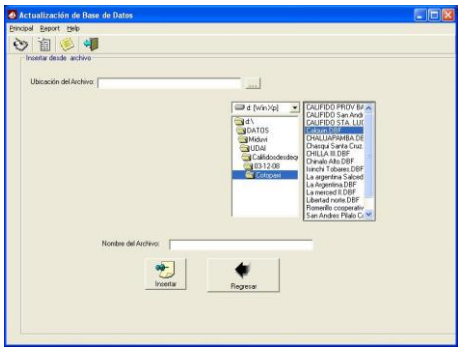


Figura 6.2: Aplicación desarrollada en Visual Basic con la cual se realiza la carga automática de datos.
Fuente: Autor de tesis.

Este aplicativo posee un algoritmo de búsqueda que verifica si los nuevos datos que serán cargados no se repitan o se dupliquen. Además luego de realizar este primer filtro, los registros serán insertados al repositorio de Microsoft Access, que se lo conoce como BASENACIONAL.

Es así que en la actualidad se llega a tener 396286 registros de beneficiarios de bonos de vivienda, los cuales pueden ser migrados a una base de datos relacional, en este caso MySQL para analizar, validad, verificar y depurar ciertos errores que posee la tabla “BASENACIONAL”.

6.1.2. CORRECCIÓN DE ERRORES DE ALMACENAMIENTO DE DATOS.

Los principales errores que se encontraron en la “BASENACIONAL”, son los siguientes:

- Caracteres especiales Ç, à, è, ì, ò, ù, À, È, Ì, Ò, Ù, `, ´ ,-, = , +.
- Espacios en blanco
- Ubicación geográfica (Provincia - Cantón) sin codificación.

En la siguiente figura se pueden apreciar algunos de los errores que se encontraron en la BASENACIONAL, es la aparición de caracteres especiales y hasta operadores matemáticos, son algunas de las inconsistencias más comunes que aparecen en los nombres de los beneficiarios así como en el de sus cónyuges.

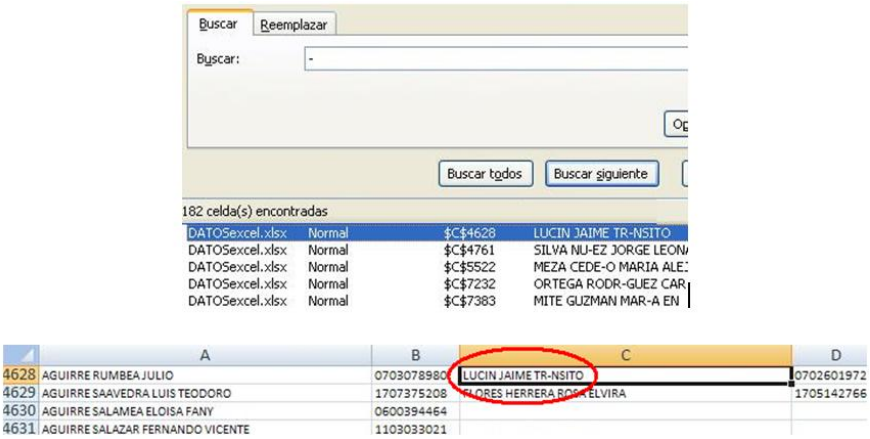


Figura 6.3: Se puede apreciar que el caracter ’ - ’ (guión), reemplazó a la letra A. Se aprecian 182 errores encontrados.

Fuente: Autor de tesis.

En la siguiente figura se muestra que existen errores de digitación muy notables y que afectan al momento de realizar búsquedas personalizadas o filtros específicos de un determinado grupo familiar o persona en específico.

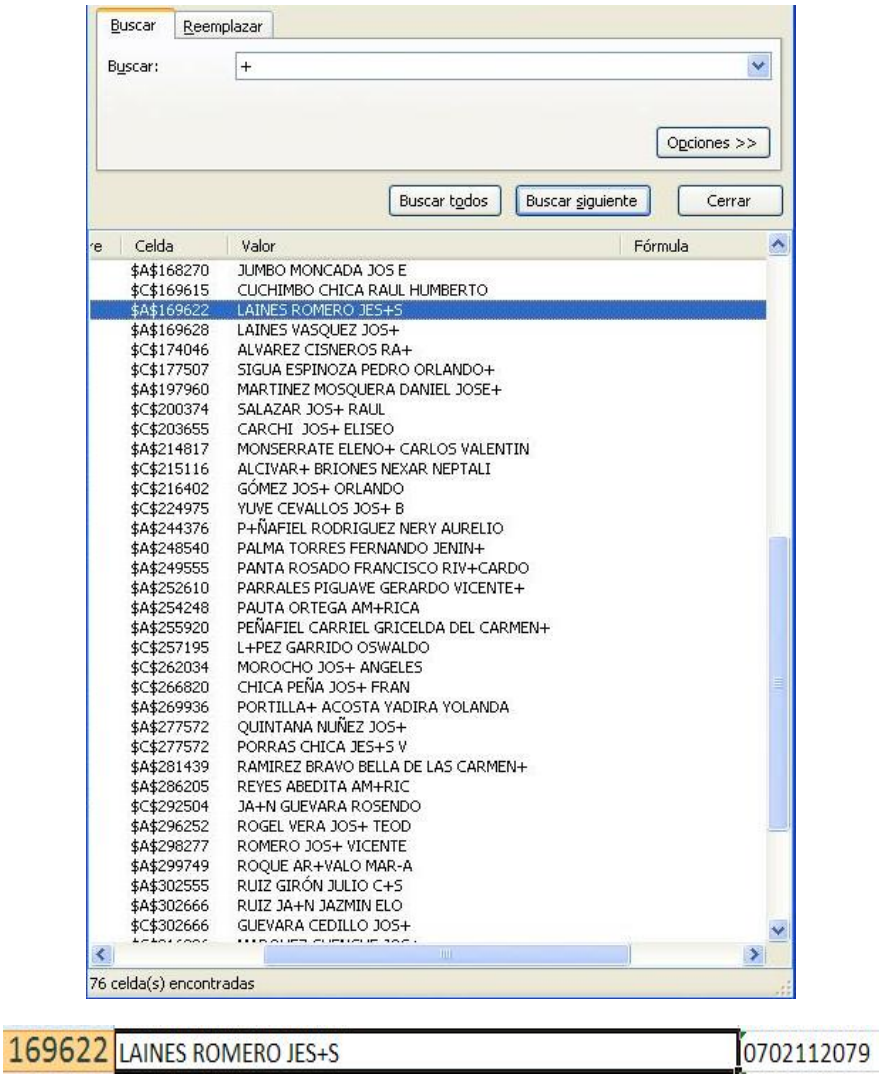


Figura 6.4: Resultado de búsqueda del carácter + (más), se aprecian 76 errores similares. Fuente Autor de tesis.

Todos estos errores se han ido corrigiendo poco a poco, ya sea de forma manual o automática. Se pretende seguir realizando más depuraciones hasta contar con una matriz de datos con la menor cantidad de errores posibles.

6.1.3. CREACIÓN DE LA BASE DE DATOS EN MYSQL.

Para poder migrar los registros de la BASENACIONAL a una base en MySQL, se procedió a instalar la versión 5.0 y la herramienta de administración MySQL.Front.v3.1.4.24, que permitirá trabajar con muchas utilidades para el correcto manejo de la información.

6.1.3.1 CREACIÓN DE LA BASE “miduvi” Y TABLA “tbnacional”

El primer paso será crear el script SQL para la creación de la tabla **tbnacional**, tal como se presenta en la siguiente figura. Se puede especificar el charset a UTF-8 y el tipo de tabla InnoDB.

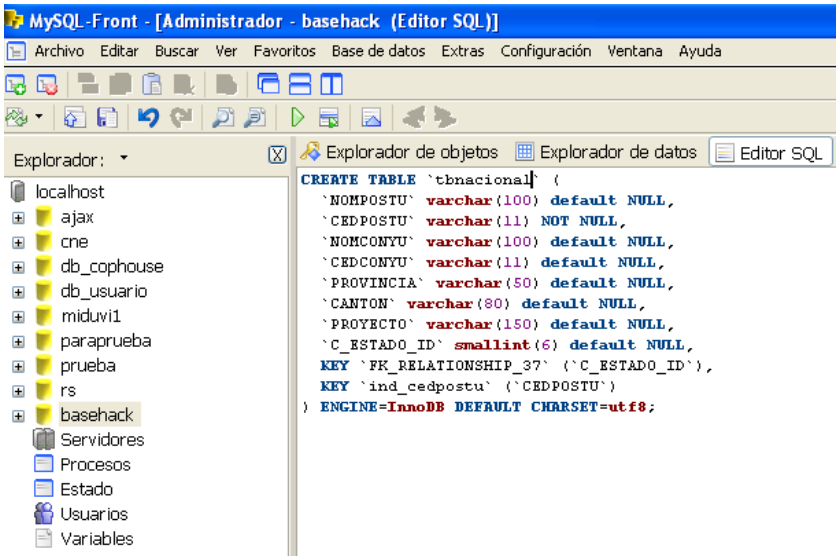


Figura 6.5: Vista de la ventana explorador y Editor SQL en la herramienta MySQL Front.
Fuente: Autor de tesis.

Para ejecutar la consulta sobre la base de datos seleccionada se debe presionar la tecla F9, si la consulta no tiene ningún error en sintaxis, la tabla requerida será creada satisfactoriamente.

En la siguiente figura se podrá visualizar la tabla con sus respectivos campos, así como el tipo de dato de cada uno de los mismos.

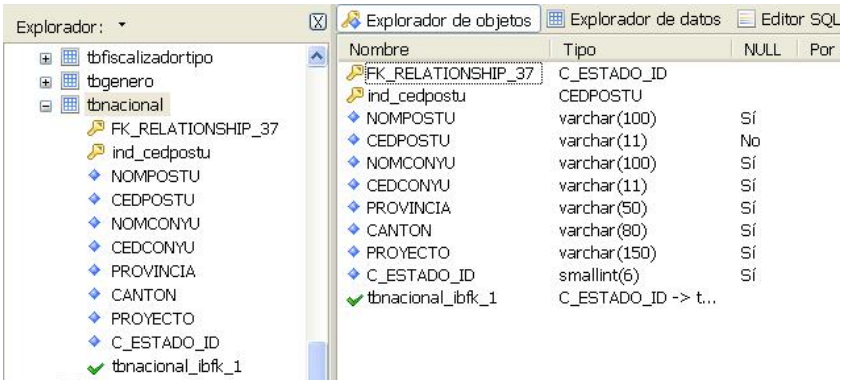


Figura 6.6: Detalle de campos y tipos de campo de la tabla tbnacional desde MySQL Front.
Fuente: Autor de tesis.

Siguiendo el procedimiento de importación, se debe generar el archivo plano a partir de la tabla datos del archivo nacional de Microsoft Access, tal como se muestra en la siguiente figura.

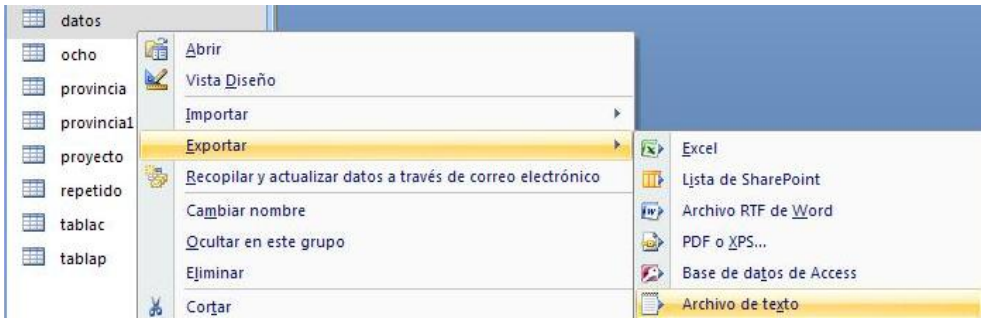


Figura 6.7: Opción de Microsoft Access para importar una tabla a archivo de texto.
Fuente: Autor de tesis.

Se debe escoger el delimitador y tipos de datos a exportar y luego poner un nombre que en este caso será “datos.txt”.

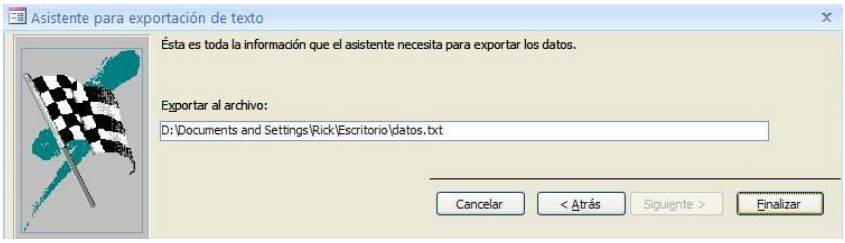


Figura 6.8: Pantalla de finalización del proceso de exportación al archivo texto de nombre “datos.txt”.
Fuente: Autor de tesis.

Luego de tener el archivo creado, se procede a cambiar la codificación a **UTF-8**, caso contrario, al momento de importar no reconocerá los caracteres especiales, así como tildes y letra “ñ”.

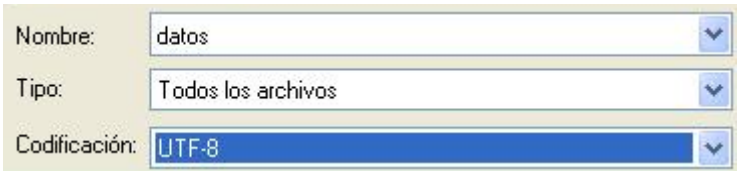


Figura 6.9: Selección de la codificación UTF-8 en el proceso de exportación del archivo.
Fuente: Autor de tesis.

El archivo final “datos.txt”, estará listo para el proceso de importación a MySQL, este proceso se lo realiza debido a la gran rapidez del gestor de base de datos al momento de cargar datos de archivos planos.

6.1.4. PROCESO DE IMPORTACIÓN DE DATOS.

Este es el último paso para completar el proceso de importación, lo primero que se debe realizar es clic derecho en la tabla "**tbnacional**", creada anteriormente. Luego seleccionar la opción Importar --> Archivo CSV, como se muestra en la siguiente figura.

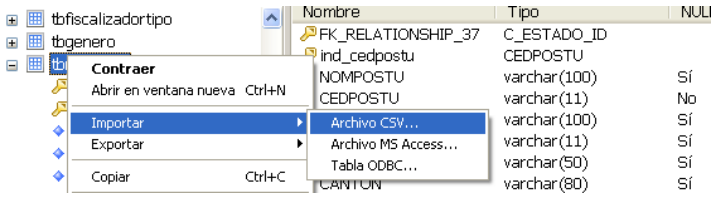


Figura 6.10: Selección de la opción "Achivo CSV", en el proceso de importación del archivo texto.
Fuente: Autor de tesis.

Siguiendo con el proceso, se debe configurar el caracter separador (;), así como el uso de comillas para cadenas tipo texto.

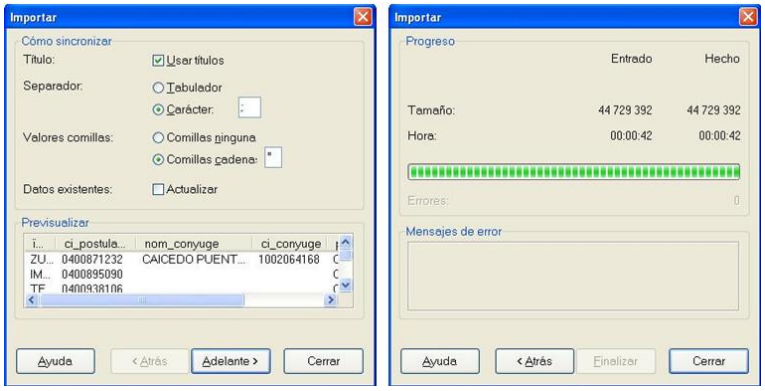


Figura 6.11: Selección de criterio de sincronización previo a la importación de datos.
Fuente: Autor de tesis.

Si el proceso se completó satisfactoriamente, la tabla en MySQL "**tbnacional**" alojará los datos de los beneficiarios de bonos de vivienda, permitiendo en este momento pensar en desarrollar una interfaz web, para luego poder acceder desde el internet a este repositorio y realizar consultas sobre cualquier registro relacionado con los bonos de vivienda.

Al poseer un motor MySQL se pueden realizar comparaciones sobre la rapidez de consulta que este gestor ofrece frente a otros, como ejemplo se realizó una consulta a la tabla recién importada obteniendo un tiempo de 0.03 segundos al realizar la consulta a 396286 registros, como se aprecia en la siguiente figura.

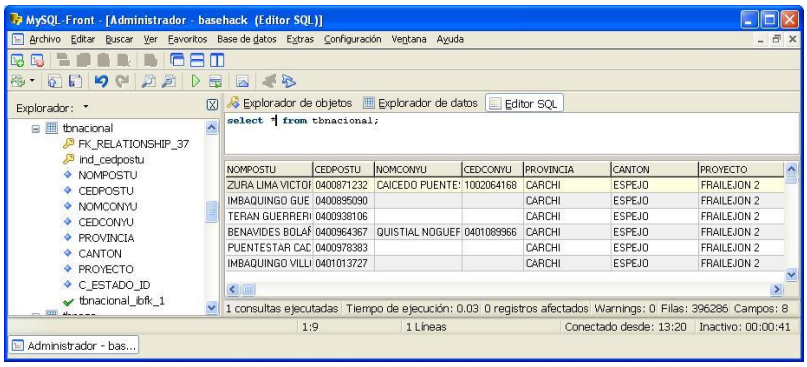


Figura 6.12: Verificación del tiempo de consulta que se demora MySQL al devolver todos los registros de la tabla nacional importada de Microsoft Access.
Fuente: Autor de tesis.

6.2. SOLUCIÓN 2: MEJORES ALTERNATIVAS PARA EVITAR ATAQUES DE RED.

6.2.1. ERRORES COMUNES QUE SE DEBE EVITAR.

No importa la experiencia ni el conocimiento que tenga un administrador de sistemas o experto en seguridad de redes informáticas, los errores estarán presentes en algún momento.

Algunos serán muy simples de solucionarlos, pero otros pueden ser realmente graves, que con suerte tomarán todo un fin de semana para solucionarlo.

La recomendación y la clave para el éxito al administrar servidores es mitigar el riesgo, teniendo un buen plan de salida que asegure que el daño causado por potenciales errores sea limitado.

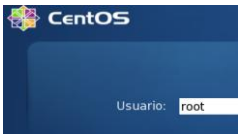
EVITAR EL USO DEL "súper-usuario" EN COMANDOS COMUNES

Un administrador sólido, trata de olvidarse que existe el súper-usuario, para configurar y administrar los servidores.

El error más común de los jóvenes administradores es realizar lo siguiente:

Figura 6.13: Ejecución de comandos de inicio de servicio de red, sin estar como usuario root.
Fuente: Autor de tesis.

Como se aprecia en la anterior figura, el administrador poco experimentado requiere realizar una actualización del repositorio, pero al ejecutar un comando sin ser súper usuario se presentan mensajes de error, y la solución más práctica es logearse desde el inicio de sesión como **root**, muy grave error.



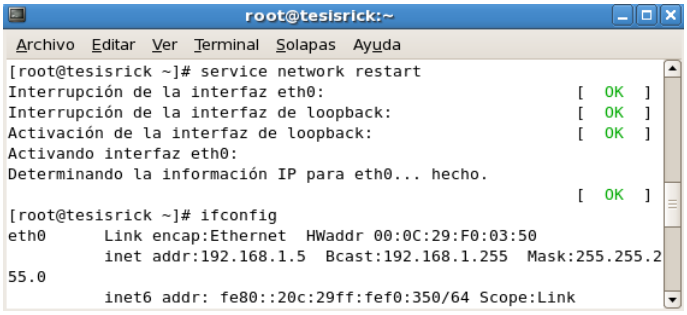


Figura 6.14: Login como root y ejecución del comando de inicio de servicio de red satisfactorio.
Fuente: Autor de tesis.

Como se puede apreciar en la figura anterior, los comandos **service network restart** y **ifconfig** funcionan perfectamente, ya que se ha iniciado la sesión con el super-usuario. Este error se debe evitar utilizando los comandos de la siguiente manera, para evitar accesos a la consola del sistema.

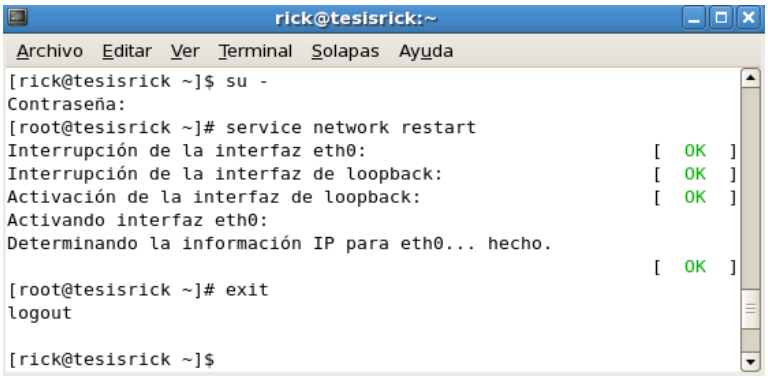


Figura 6.15: Ejecución de comandos de inicio de servicios sin alterar la seguridad del sistema.
Fuente: Autor de tesis.

VERIFICACIÓN DE COMANDOS PARA SERVIDORES EN PRODUCCIÓN.

Una recomendación muy importante en la configuración y administración de servidores es verificar 2 y 3 veces el conjunto de scripts que se ejecutarán en un determinado servidor puesto en producción.

Al realizar modificaciones directamente sobre un servidor en producción resulta una forma más práctica arreglar un determinado problema, pero al mismo tiempo es algo riesgoso si los resultados no son los esperados.

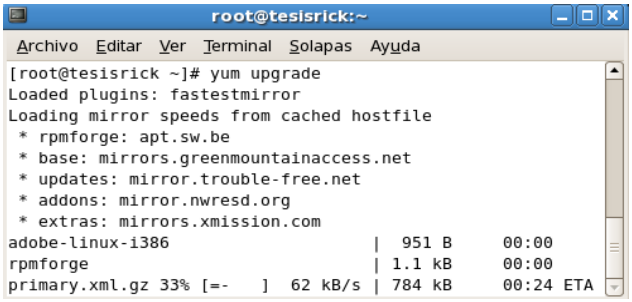


Figura 6.16: Ejecución del comando "upgrade" para la actualización del servidor en producción.
Fuente: Autor de tesis.

Realizar una actualización al servidor web que aloje una aplicación importante para una empresa o institución sin haber programado un procedimiento de reversa, podría causar un desastre y en ocasiones la baja de todo el servicio.

La siguiente figura es un ejemplo de una actualización común de servidor, que guardará los nuevos repositorios y modificará algunas configuraciones.

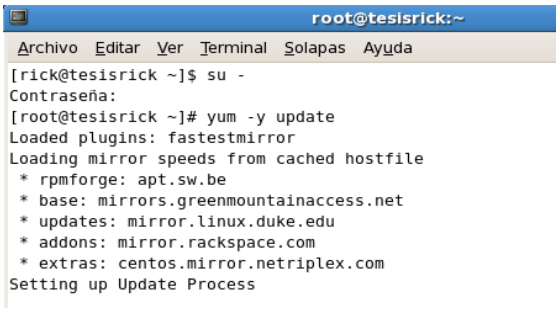


Figura 6.17: Error común al tratar de actualizar directamente sobre el servidor en producción con el comando yum update.
Fuente: Autor de tesis.

Al ejecutar el comando **# yum –y update** se iniciará el proceso de actualización y podría ocurrir que luego de reiniciar el servidor web no trabaje correctamente, y no desempeñe las mismas funciones que antes realizaba.

Como conclusión, si no se posee un servidor de pruebas y se requiera ejecutar directamente nuevos scripts en el equipo de producción, se deben realizar como mínimo 2 procedimientos:

- Procedimiento programado de ejecución.- donde estén los nuevos scripts comprobados y con controles de verificación de errores.
- Procedimiento de marcha atrás.- este procedimiento consiste en tener un plan de reversa, donde los archivos y configuraciones que serán modificados podrán ser restaurados en el momento que no se consiga el resultado esperado.

6.2.2. TÉCNICAS PARA AUMENTAR LA SEGURIDAD.

La responsabilidad de todo administrador de sistemas es asegurar que los sistemas sean seguros y no sean un potencial objetivo de los atacantes de red.

Activar servicios indispensables y mantener abiertos únicamente los puertos necesarios, es una gran solución, para que los servidores trabajen establemente y no sean una víctima más de los intrusos de la red.

Si se resume un poco, en este punto se mostrará un amplio espectro de aplicaciones y técnicas de seguridad de los sistemas que ayudan a minimizar o eliminar intrusiones.

6.2.2.1 DESACTIVAR SERVICIOS INCESARIOS.

Muchos de los servicios de red pueden estar activados por defecto, pero son tan innecesarios como inseguros. Un buen administrador debería analizar cuáles son los servicios que necesita una determinada aplicación.

Los 3 lugares estándar desde los cuales los servicios de sistema pueden iniciarse son los siguientes:

- **# /etc/inittab**

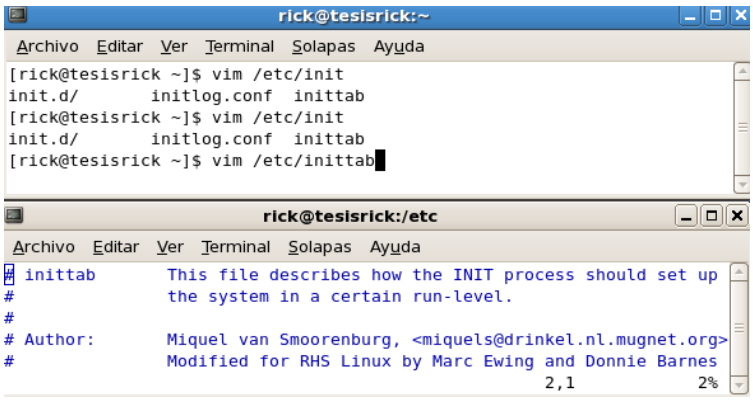


Figura 6.18: Configuración del fichero etc/initab para verificar los servicios activos.
Fuente: Autor de tesis.

- Los scripts en los directorios **/etc/rc.d/rc*.d**

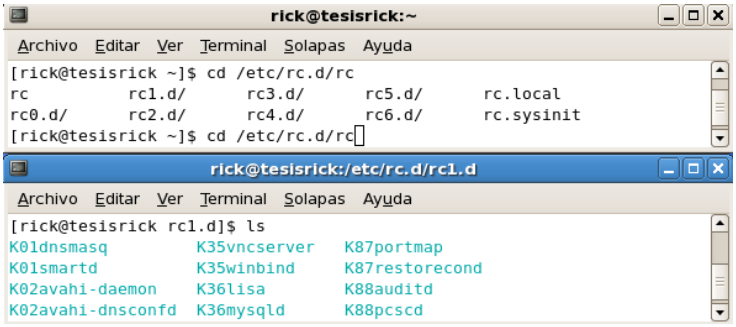


Figura 6.19: Configuración de ficheros etc/rd.d/rc.* para verificar los servicios activos.
Fuente: Autor de tesis.

- A través del demonio de internet **inetd** ó **xinetd**

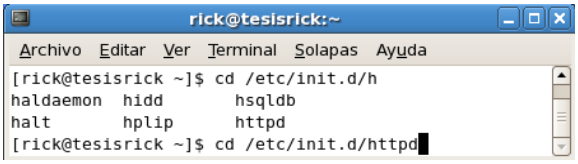


Figura 6.20: Configuración de servicios sobre los demonios inetd o xinetd.
Fuente: Autor de tesis.

Paso 1: EXAMINAR /etc/inittab

El fichero /etc/inittab arranca la secuencia estándar de script de inicio, como se puede apreciar en la siguiente figura, donde se ejecutan los comandos que arrancan la secuencia de inicialización para cada nivel.

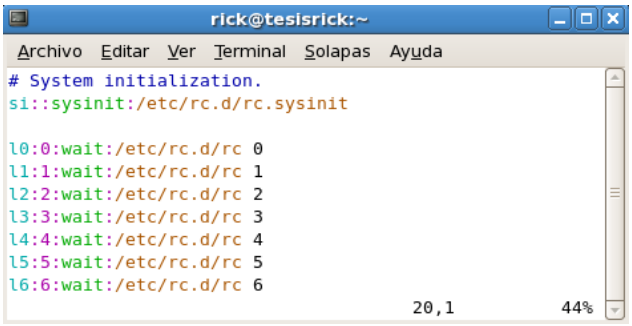


Figura 6.21: Comandos que utiliza initab para arrancar la secuencia de iniciación para cada nivel.
Fuente: Autor de tesis.

Paso 2: Optimizar los scripts de inicio por nivel de ejecución

Los directorios rc*.d que se mostraron anteriormente, corresponden a los niveles de ejecución según el número que posean.

El directorio para cada nivel de ejecución contiene enlaces simbólicos a los script reales que inician y finalizan diversos servicios, los cuales residen en /ect/rc.d/init.d, como se visualiza en la siguiente figura.

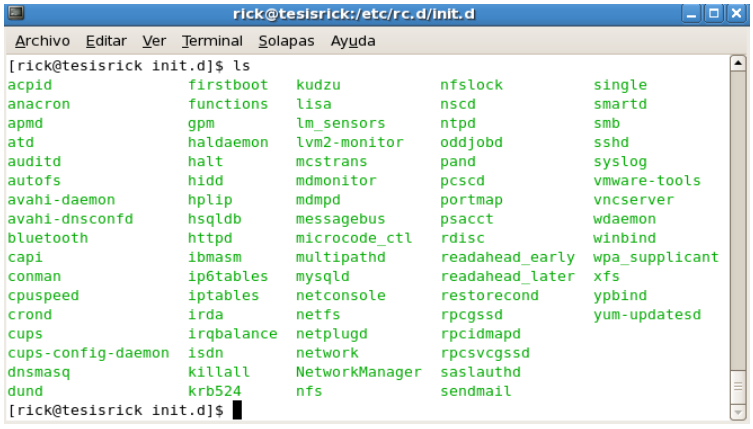


Figura 6.22: Ficheros de /etc/rc.d/init.d donde constan los servicios del sistema.
Fuente: Autor de tesis.

Los enlaces que comienzan por “S” se iniciarán cuando se entre en ese nivel de ejecución, mientras que los enlaces que comienzan por “K” serán finalizados cuando se abandone el nivel.

La forma rápida para desactivar un servicio es eliminar el script “S” asociado, pero una buena solución es crear un directorio DESABILITADO en cada directorio de nivel de ejecución y mover ahí los enlaces simbólicos que inician o finalizan servicios y que no se desea que se ejecuten en este directorio.

Paso 3: Hacer los servicios más eficientes ejecutados desde "inetd".

Uno de los script del directorio antes mencionado, inicia el demonio **inetd** en distribuciones Linux antiguas y **xinetd** en distribuciones más recientes. Para desactivar algunos servicios con **inetd** se debe configurar el archivo /etc/inetd.conf, comentando los no deseados. De la misma manera con el archivo /etc/xinetd.conf, para desactivar un servicio específico, se debe dar el valor de "yes" a la entra "disable" y reiniciar las entradas para estos demonios.

6.2.2.2 PERMITIR O DENEGAR SERVICIOS POR IP

Esta solución es muy práctica al momento de bloquear sistemas maliciosos que puedan perjudicar un servidor que aloje información confidencial. Tener un procedimiento que permita habilitar y deshabilitar el acceso a ciertas personas desde sus PCs hace un sistema estable y seguro.

Una alternativa sería configurar iptables o ipchains para implementar restricciones de acceso, pero la idea es tener otro método mucho más fácil y práctico, con la ayuda de la configuración apropiada de los ficheros /etc/hosts.allow y /etc/hosts.deny.

- **CONFIGURACIÓN DE LOS FICHEROS hosts.allow y hosts.deny**

Todo el tráfico de paquetes entrantes TCP que un servidor Linux procesa, son filtrados por medios de las reglas en hosts.allow, y luego si no existen coincidencias, con las reglas hosts.deny.
En la forma más simple, las líneas de cada fichero tiene el siguiente formato:

nombre-demonio: nombre-equipo o dirección-ip

Ejemplo:

sshd: 192.168.0.143, 192.168.5.25

Para entender el ejemplo si esta línea es insertada en hosts.allow, el tráfico SSH del equipo estaría permitido para las direcciones IP 192.168.0.143 y 192.168.5.25. De igual manera si se incluye la línea anterior expuesta en el fichero host.deny, ninguna de las 2 direcciones IP podrán acceder desde SSH.

El demonio TCP de Linux proporciona un excelente lenguaje y sintaxis para configurar restricciones de control de acceso en los ficheros hosts.allow y hosts.deny.

Ejemplo:

#hosts.allow

sshd: .foo.bar

En el ejemplo anterior se puede apreciar el punto (.) precedente. Esto permite aceptar cualquier cosa que contenga ".foo.bar" en su nombre de sistema.

- **CONFIGURACIÓN DE hosts.allow - hosts.deny EN SU UTILIZACIÓN.**

Para poder configurar correctamente estos ficheros, si se piensa en el funcionamiento de un servidor en producción se deben tomar ciertas recomendaciones.

Lo que se va a realizar es configurar el servidor en el fichero hosts.allow que permita conexiones web HTTP desde cualquier parte y restrinja el tráfico por SSH a determinadas IPs con privilegios para modificar ciertos parámetros. Además, como parte de una buena configuración de seguridad, se denegará el acceso por TELNET ya que la información que podría generarse en este protocolo no está encriptada.

Ejemplo:

Se edita hosts.allow como se muestra en la siguiente tabla:

hosts.allow	***hosts.deny***
sshd: LOCAL, 192.168.0.143, 192.168.5.25	**telnet:** ALL
httpd: ALL	

Tabla 6.1: Tabla resumen de la configuración para el fichero host.allow y host.deny.
Fuente: Autor de tesis.

6.2.3. SISTEMA DE DETECCIÓN DE INTRUSOS – SNORT.

Los sistemas de detección de intrusos son indispensables que existan en toda red con un nivel de seguridad alto y que trabaje con sistemas complejos y de alta concurrencia de usuarios y clientes.

Estos sistemas buscan patrones previamente definidos que impliquen cualquier tipo de acción maliciosa o sospechosa sobre la red de datos.

Los IDS aportan a la seguridad con una capacidad de prevención y de alerta anticipada ante cualquier ataque, aunque no están diseñados para detenerlos si pueden generar acciones de respuesta a estos. Además los IDS aumentan la seguridad de los sistemas, monitorean el tráfico de la red, examinan los paquetes y detectan las primeras fases de los ataques comunes a las redes de datos.

6.2.3.1 HERRAMIENTA SNORT

Esta es una herramienta de seguridad para detectar y monitorizar los eventos ocurridos en un determinado sistema o red de datos que afecten a la seguridad de los mismos.

Snort es un sistema de detección de intrusiones basado en red, implementa un motor de detección de ataques y barrido de puertos sobre los cuales se generan registros y alertas para responder a posibles vulnerabilidades o intentos de ataques a la red.

CARACTERÍSTICAS:

- Es una herramienta bajo licencia GLP, gratuito.
- Multiplataforma Windows y UNIX/Linux
- Posee gran cantidad de filtros y patrones predefinidos.
- Implementa un lenguaje de creación de reglas flexibles.
- Multifunción (sniffer y IDS a la vez).

Ejemplo:

Este ejemplo se enfoca a un sistema IDS, que probará las principales funcionalidades como el monitoreo de las peticiones de red entrantes a un determinado sistema, la generación de alertas frente a cualquier actividad que parezca falsa, y generación de logs como resultados.

INSTALACIÓN Y CONFIGURACIÓN DE SNORT

El primer paso es instalar la herramienta Winpcap, que sirve como librería de bajo nivel que utilizará Snort. Se procede también a instalar Snort como se muestra en la siguiente figura.

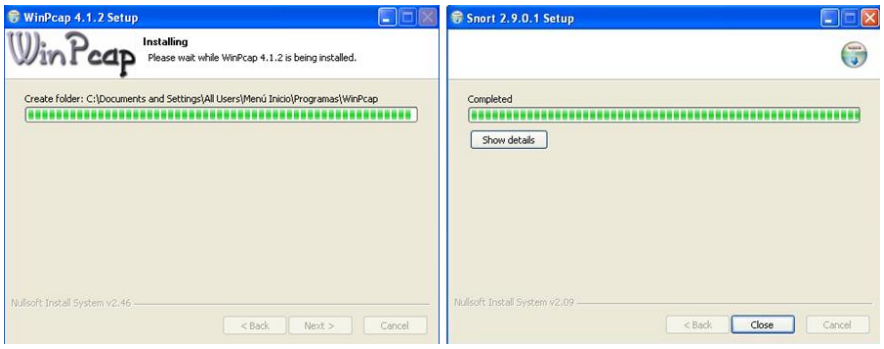


Figura 6.23: Proceso de instalación de la herramienta WinCap sobre Windows.
Fuente: Autor de tesis.

Luego de terminada la instalación, se procederá a configurar la herramienta, para lo cual se accederá a la capeta **C:\Snort\etc**, en este directorio se encuentra un fichero llamado **snort.conf** que será el archivo de configuración en el cual se realizará las modificaciones.

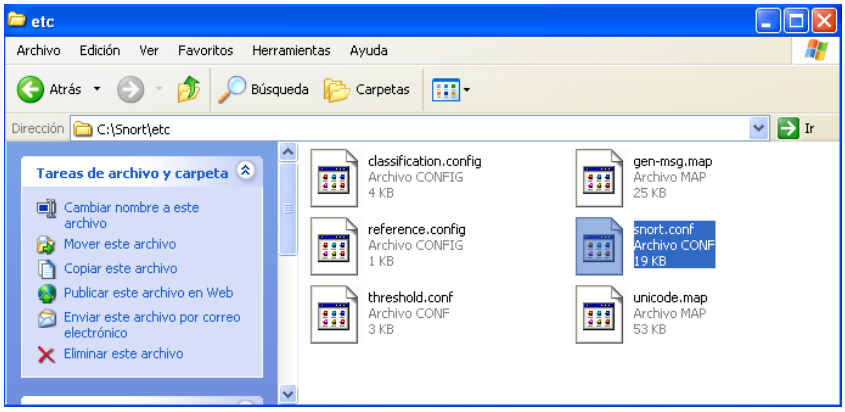


Figura 6.24: Búsqueda y selección del archivo de configuración de la herramienta Snort.
Fuente: Autor de tesis.

Luego se deberá ingresar al archivo para iniciar la configuración de la herramienta, en la cual se ingresará la información de la red o hosts a protegerse como se muestra en la siguiente figura.

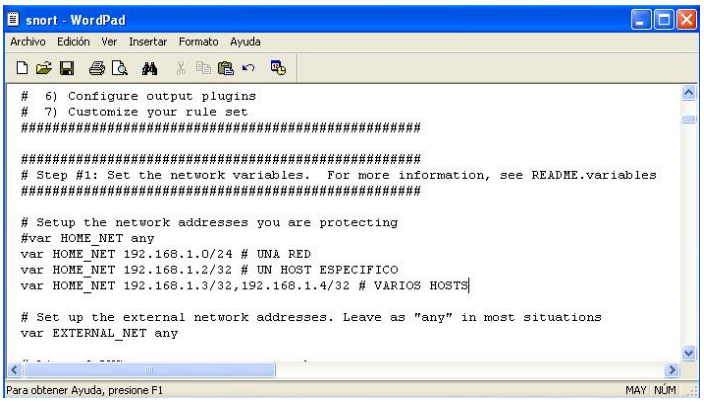


Figura 6.25: Configuración de la dirección de red o host para comprobar el funcionamiento de Snort.
Fuente: Autor de tesis.

Además se deberá descargar las reglas de la página oficial de Snort (http://www.snort.org), para luego copiarlas en el directorio "**C:\Snort\rules**"

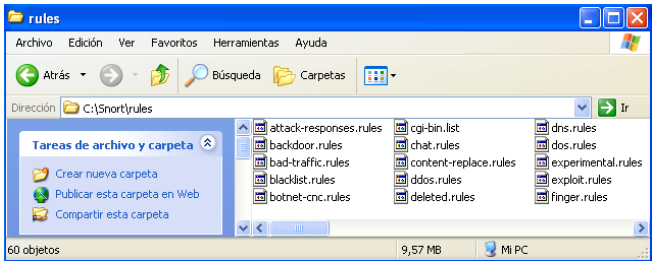


Figura 6.26: Directorio C:\Snort\rules\ luego de copiar reglas descargadas de la página oficial de Snort.
Fuente: Autor de tesis.

Para finalizar el proceso quedaría realizar 2 cambios en las siguientes líneas las cuales se visualizan en la siguiente figura.

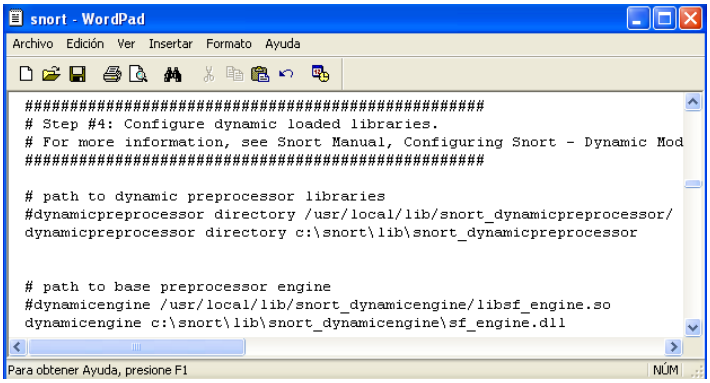


Figura 6.27: Configuración de las librerías (.dll) que se encuentran en el directorio de Windows lib\.
Fuente: Autor de tesis.

Con estos cambios realizados se puede ejecutar la herramienta desde la consola, tal como lo muestra la siguiente figura.

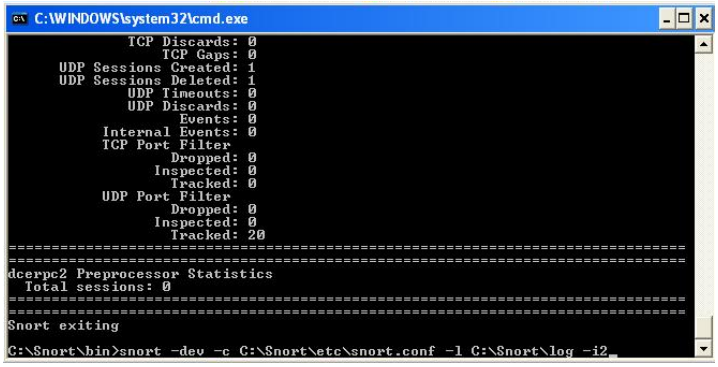


Figura 6.28: Ejecución del comando para iniciar la herramienta Snort, generando un reporte.
Fuente: Autor de tesis.

En este ejemplo se está definiendo el archivo de configuración **snort.conf** y además con el comando " ***-l*** " se indica el directorio para guardar las alertas y logs que servirán para que el administrador de seguridad observe y verifique problemas en la red.

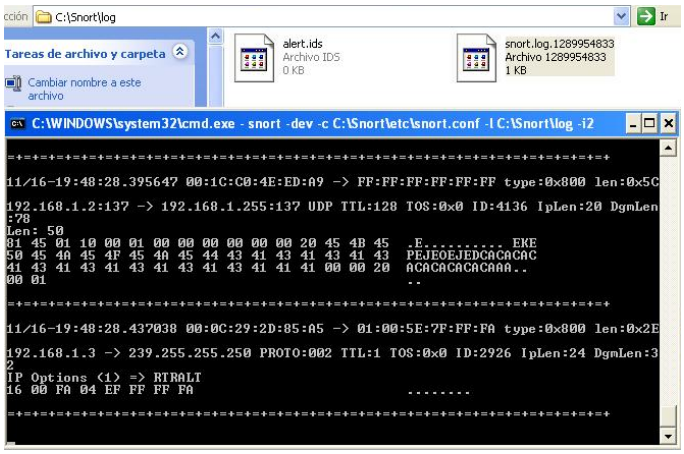


Figura 6.29: Detalle del resultado de alertas obtenido luego de la ejecución de Snort.
Fuente: Autor de tesis.

Como se pudo observar en la figura anterior, la herramienta Snort se ejecutó desde la consola, y también creó 2 archivos en el directorio C:\Snort\log, en los cuales se guarda toda la información generada por Snort. Como conclusión se puede decir que esta herramienta permite detectar intrusos alertando de posibles ataques de un determinado equipo. La buena utilización de este IDS posibilita a un administrador manejar servidores seguros y confiables.

6.3. SOLUCIÓN 3: PLAN DE SEGURIDAD PARA REDES Y GESTIÓN DE LA INFORMACIÓN.

La solución Nº 3, se propone implementarla en el Ministerio de Desarrollo Urbano y Vivienda para brindar una serie de procedimientos y prácticas a seguir que controlen y gestionen de mejor manera, la red de datos, servidores e información importante de la institución.

El recurso crítico que debe poseer controles de seguridad bastante fuertes y herméticos es la información de beneficiarios de bonos de vivienda, ya que si algún intruso logra acceder a los servidores que alojan a la misma, causarían un grave daño si no se tienen estrategias claras y efectivas para evitar este tipo de ataques.

Es por esto que se presenta una serie de ejercicios prácticos que pueden ser tomados en cuenta al momento de evitar algún ataque o fallo de red que pueda perjudicar a las bases de datos que alojan información confidencial.

6.3.1. FUNCIONAMIENTO Y DEFENSA CONTRA SNIFFERS.

Los Sniffers se pueden definir como aplicaciones o programas de monitorización oculta que tienen la función de recoger la mayor cantidad de información del tráfico de una red. Se los conoce como analizadores de protocolos.

6.3.1.1. COMO ACTUAN LOS SNIFFERS

Las estaciones de trabajo escuchan y responden solamente a los paquetes que van dirigidos a ellas. Sin embargo, es posible modelar el software que lanza la interfaz de red de una estación de trabajo en algo llamado modo promiscuo.
Con este análisis, la estación de trabajo puede monitorizar y capturar todo el tráfico de red y los paquetes que pasen por ella, independientemente del destino que tengan.

Ejemplo de cabeceras de Sniffers.

```
#include <linux/if.h >
#include <Linux/i_ether.h >
#include <Linux/ip.h >
#include <Linux/socket.h >
#include <Linux/tcp.h >
#include <Linux/stdio.h >
```

La mayoría de los sniffers se han diseñado con estos archivos de cabecera. Cada uno de ellos gestiona un aspecto distinto de la escucha, grabación y generación de informes sobre el tráfico de TCP / IP.

Lo que hacen los intrusos y piratas de red es poner la interfaz en modo promiscuo utilizando una marca de " ***if.h*** ". Una vez que la interfaz se encuentra en este modo, escucha todos los paquetes de la red, y lo que faltaría es escuchar el tráfico TCP /IP y generar un formato que pueda leerse en la salida estándar o escribirlo en un archivo.

EJEMPLO:

Existen muchos sniffers que realizan tareas diferentes, desde capturar nombres de usuarios y contraseñas hasta grabar todo el tráfico de la interfaz de red.

- **Dsnif**

Es una aplicación sencilla y directa. El propósito principal es capturar nombres de usuarios y contraseñas, y esta es una función en la que sobresale.

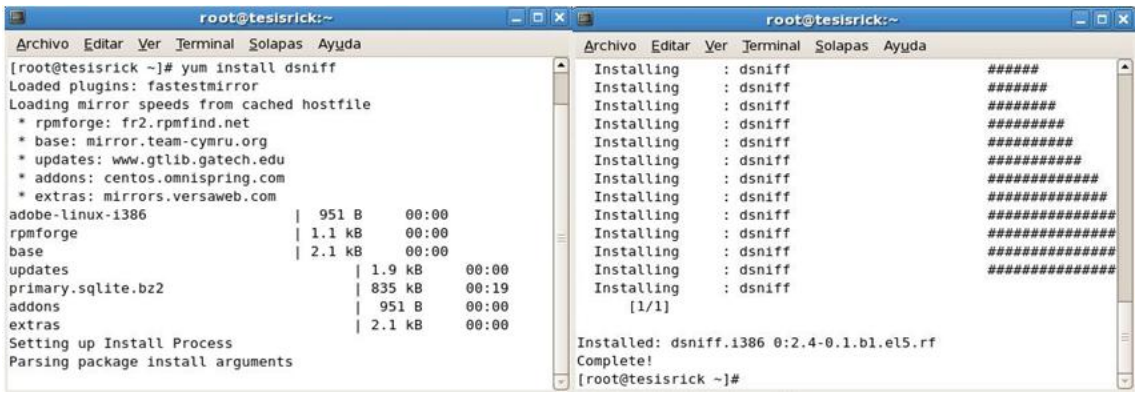


Figura 6.30: Descarga e instalación del paquete dsniff en Linux.
Fuente: Autor de tesis.

Para probar la herramienta se configurará un router con la dirección 192.168.1.1, la víctima 192.168.1.4 y el atacante 192.168.1.6. Luego de esto se procede a ejecutar el primer comando necesario para que el tráfico pueda pasar por el computador atacante, como se muestra en la siguiente figura el **ip_forward** es el que permite que los paquetes lleguen a su destino sin importar quien está en medio de la conexión.

Figura 6.31: Utilización de ip_forward para permitir el tráfico por el computador atacante.
Fuente: Autor de tesis.

La siguiente figura muestra la utilización de "**arpspoof**", lo que permitirá realizar un envenenamiento al cache ARP para hacerse pasar como un destinatario real.

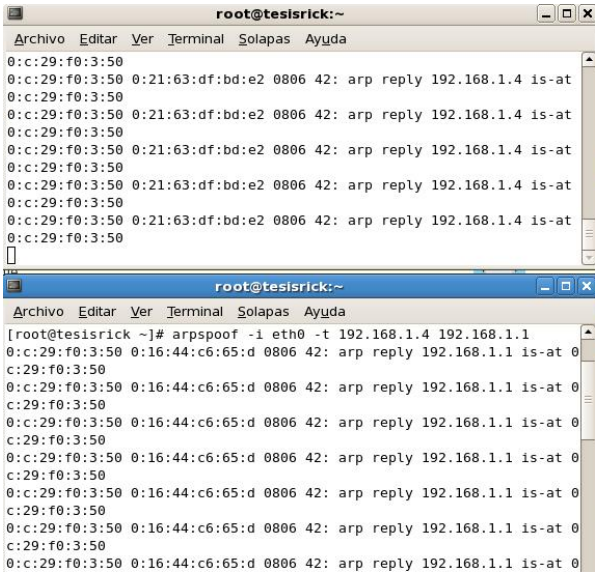


Figura 6.32: Ingreso del comando arpspoof para realizar la modificación al cache ARP.
Fuente: Autor de tesis.

Por último queda ejecutar dsniff a la interfaz eth0, que será en la cual se interceptarán los paquetes, de esta forma se puede capturar datos de usuarios y contraseñas que la víctima este enviando desde una página web de correos o login normal.

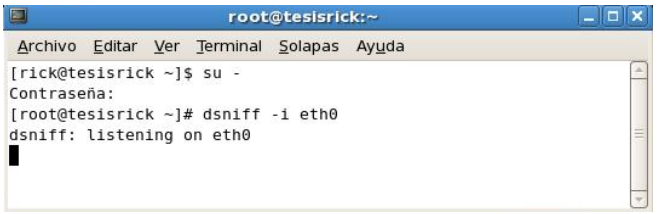


Figura 6.33: Ingreso del comando "dsniff –i eth0" a la interfaz Ethernet logrando el ataque deseado. Fuente: Autor de tesis.

6.3.1.2. COMO DEFENDERSE DE LOS SNIFFERS.

Los ataques de sniffers son difíciles de detectar y combatir, ya que son programas pasivos que no generan rastros, y cuando se configuran correctamente, no utilizan muchos recursos de discos y de memora.

La solución al problema es ir directo al origen, es decir, a la interfaz de red por la cual se están enviando los datos y paquetes. Lo que se debe verificar es que si esa interfaz se encuentra en modo promiscuo, para lo cual se puede utilizar las siguientes herramientas:

- Ifconfig
- Ifstatus

Ifconfig

Con ifconfig es posible detectar de forma rápida cualquier interfaz del host local que se encuentre en modo promiscuo. Al ejecutar **ifconfig** en la consola, la herramienta informará el estado de todas las interfaces, y para detectar que se encuentra en estado promiscuo se debe identificar las siguientes líneas, como se muestra en la figura.

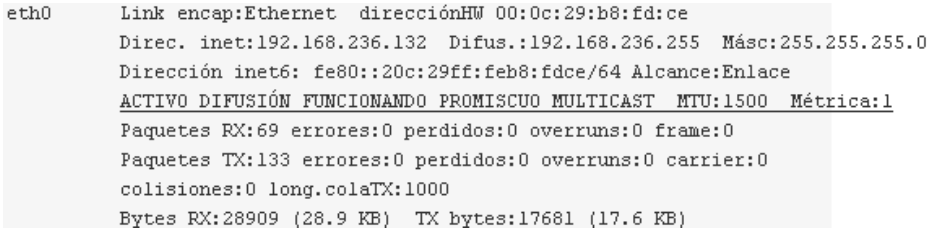


Figura 6.34: Detalle del uso del comando ifconfig al detecta una interfaz eth0 en modo promiscuo. Fuente: http://www.linuxcostarica.org/component/content/article/44-10-ejemplos-practicos/71-10-ejemplos-practicos-de-ifconfig.html.

Ifstatus

Esta herramienta comprueba todas las interfaces de red del sistema e informa si alguna se encuentra en modo de depuración o promiscuo.

Ifstatus detecta sniffers en el host local. Luego de descargarse se recomienda configurarlo como se muestra en la siguiente figura para que cumpla con las funciones de detección de sniffers.

```
OSNAME=     SUNOS55
LIBS=     -lkvm -lelf -lnsl -lsocket
por éstas:
OSNAME=     BSD
#LIBS=     -lkvm -lelf -lnsl -lsocket
```

Figura 6.35: Configuración de OSNAME y LIBS para el funcionamiento de ifstatus.
Fuente: http://www.sfr-fresh.com/unix/misc/old/ifstatus2.2.tar.gz:a/ifstatus/RCS/Makefile,v.

La figura anterior muestra las líneas que se deben editar en el archivo Makefile de configuración de **ifstatus**.

De la misma manera se procede a detectar el sniffer con ésta nueva herramienta y muestra si la interfaz de red está en modo promiscuo y con esto el administrador puede tomar una decisión para evitar que más sniffers puedan seguir atacando a los equipos de la red.

6.3.2. FUNCIONAMIENTO Y DEFENSA CONTRA SCANNERS.

Los Scanners son herramientas de seguridad que detectan los puntos vulnerables de un determinado sistema, podría decirse que un scanner rudimentario es un script en el cual se escribe comandos para rastrear passwords escritos en un login de correo electrónico en busca de espacios vacios, que son posibles puntos débiles en la seguridad.

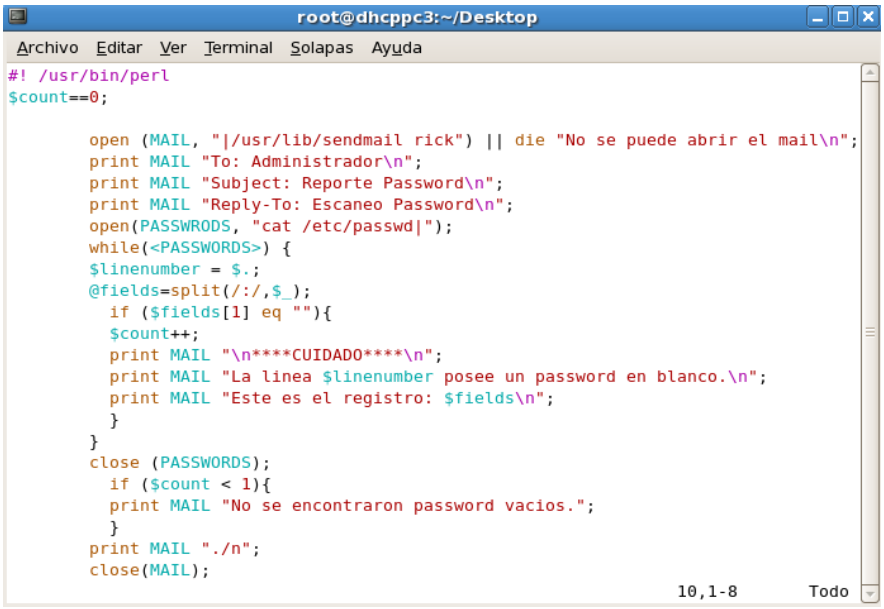


Figura 6.36: Script básico que actúa como scanner y a la vez como defensa a los sniffers.
Fuente: Autor de tesis.

Los scanners de acuerdo a su funcionalidad se dividen en:

- **Scanner de sistema**

Son aquellos que rastrean host locales en busca de los puntos vulnerables comunes y no comunes de la seguridad que aparecen a causa de descuidos, poco interés, falta de conocimiento, y los problemas de configuración que a veces se pasan por alto, aquí se mencionan algunos ejemplos:

- Permisos erróneos de archivos
- Cuentas predeterminadas
- Entradas de UID erróneas o duplicadas.

- **Scanner de red**

Por el contrario, los scanners de red verifican y prueban host sobre conexiones de red, de forma similar a como lo haría un atacante o intruso. Examinan los servicios y puertos disponibles en busca de debilidades y vulnerabilidades a equipos remotos, y se los crea para realizar las siguientes acciones:

- Rastrear sesiones telnet de equipos.

- Adivinar el nombre de dominio NIS.
- Explorar puntos vulnerables de protocolos.
- Comprobar si existen login anónimos para el ingreso sin autorización

6.3.2.1. COMO ACTUAN LOS SCANNERS

El proceso lógico que utilizan tanto los scanner lógico como de red es:

- Cargan un conjunto de reglas de ataques.
- Prueban el objetivo con varios parámetros.
- Registran y emiten reportes con los resultados obtenidos.

Ejemplo:

La variedad de scanners que existen hace que los administradores puedan escoger de una amplia gama de herramientas los que mejor se apeguen a las necesidades particulares.

Para este ejemplo se instalará una aplicación llamada SANE(Scanner Access Now Easy), que brinda características de escaneo muy prácticas y funcionalidades que pueden ser aplicadas en cualquier red.

- **INSTALACIÓN DEL SERVIDOR SANE**

Figura 6.37: Descarga e instalación de ficheros de la herramienta SANE.
Fuente: Autor de tesis.

Como se aprecia en la figura anterior se utilizó el comando YUM para completar la instalación del paquete SANE como se muestra en la figura.

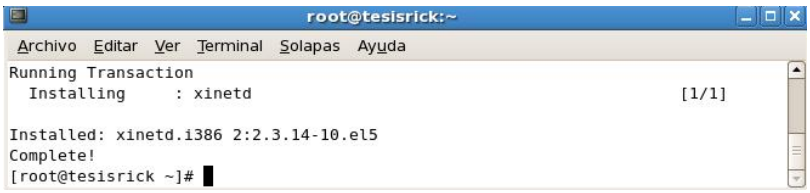


Figura 6.38: Instalación del paquete xinetd para SANE.
Fuente: Autor de tesis.

INSTALACIÓN DEL CLIENTE XSANE

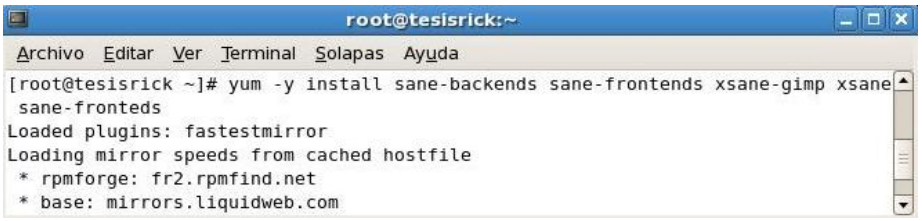


Figura 6.39: Descarga e instalación del paquete para el cliente de Xsane.
Fuente: Autor de tesis.

CONFIGURACIÓN DEL SERVICIO SANED

Se debe verificar que en el fichero **/etc/sane.d/dll.conf** esté habilitada la línea que corresponde al controlador para escáner, es decir, " **net** ".

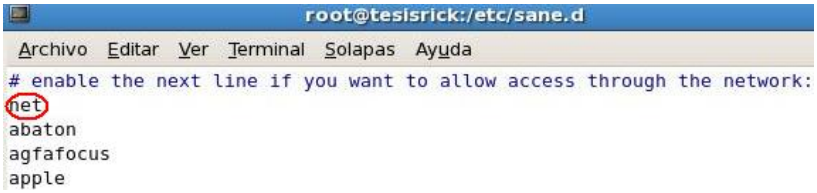


Figura 6.40: Configuración y verificación de NET en el servicio SANED.
Fuente: Autor de tesis.

Además se añade en el fichero **/etc/sane.d/saned.conf** la lista de direcciones IP permitidas la conexión al servicio saned.

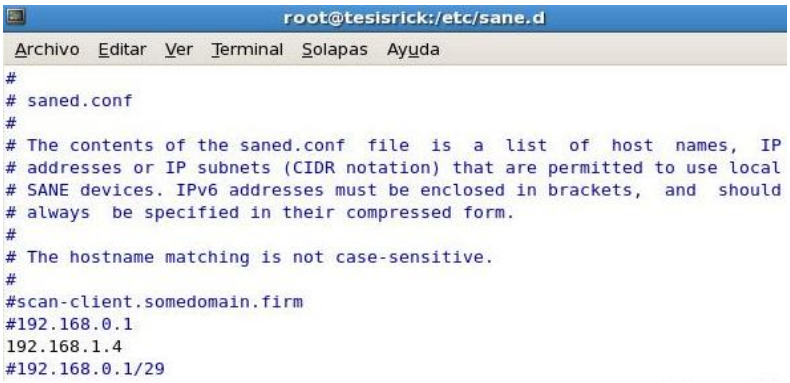


Figura 6.41: Configuración del archivo saned.conf para indicar los host de escaneo.
Fuente: Autor de tesis.

Para que las aplicaciones y servicios puedan proporcionar una identificación para Saned es necesario agregar la siguiente línea con el respectivo puerto.

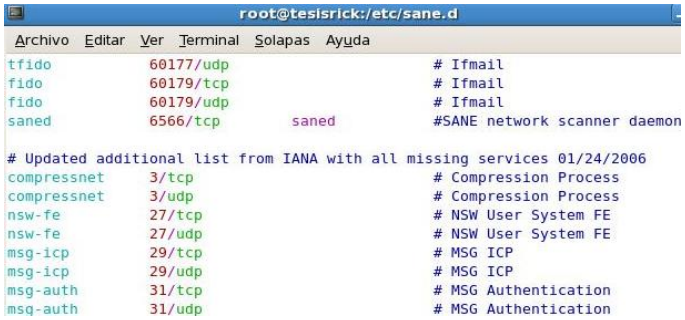


Figura 6.42: Configuración mediante el ingreso del puerto para sane 6566/tcp.
Fuente: Autor de tesis.

Se debe crear el archivo /etc/xinetd.d/saned para dar acceso al servicio mediante Xinetd.

Figura 6.43: Acceso al servicio mediante Xinetd configurando este script.
Fuente: Autor de tesis.

Para activar el servicio de saned se utiliza chkconfig, el cual a su vez notificará al servicio xinetd para que se inicien automáticamente al recibir cualquier petición a través del puerto 6566.

#chkconfig saned on

Si todo salió bien, se puede comprobar el funcionamiento utilizando el comando telnet mediante el puerto 6566 del retorno del sistema, como se muestra en la siguiente figura.

Figura 6.44: Prueba de conexión con el servidor saned mediante el puerto 6566.
Fuente: Autor de tesis.

- **CONFIGURACIÓN DEL CLIENTE XSANED**

El último paso es configurar el cliente Xsane, para esto se debe especificar en el fichero /etc/saned.d/net.conf la dirección IP del servidor recién configurado., como se muestra en la siguiente figura.

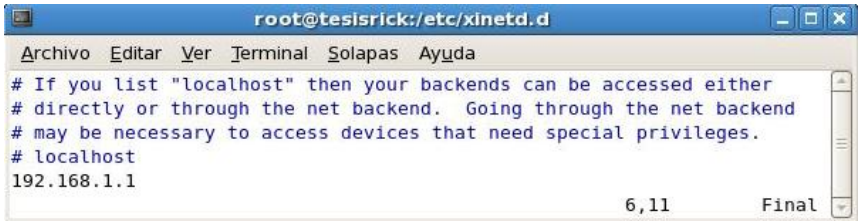


Figura 6.45: Configuración en el fichero net.conf la dirección del servidor al cual se conectará el cliente. Fuente: Autor de tesis.

Una vez realizado esto, los equipos clientes deberán detectar automáticamente el escáner en el servidor.

6.3.2.2. COMO DEFENDERSE DE LOS SCANERS.

Los scanners pueden ser beneficiosos y perjudiciales a la vez, todo depende de quién lo está utilizando. Los scanners seleccionan a que servidores pueden atacar, es por esto, que es conveniente conocer la detección de scanners. De esta manera se podrá saber por lo menos lo que se está realizando en el sistema a pesar de no poder evitar el ataque.

- **courtney (detector de SATAN y SAINT)**

Este script fue creado con lenguaje Perl que, junto con Tcpdump, detecta los rastreos de SATAN y SAINT. Además registra las advertencias en formato syslog ALERT y los reportes se pueden ver en el siguiente PATH:

/var/log/messages.

Para ejecutar courtney, se introduce el siguiente comando:

$ courtney.pl

Para el ejemplo se ejecuta Courtney y se inicia un rastreo de SAINT. A medida que avanza el rastreo, la herramienta guarda cada actividad en la ruta anteriormente descrita.

IcmpInfo (detector de ratreos / bombas ICMP)

Ésta aplicación ayuda a detectar alguna actividad sospechosa en ICMP, como bombas y rastreos. Para utilizarlo se procede a instalar la herramienta y luego configurarlo.

Para ejecutar la herramienta se ingresa el siguiente comando:

#icmpinfo -vv

De esta manera se logra vigilar tanto el tráfico entrante como el saliente y es muy fácil de configurar.

Como conclusión se agrega que los scanners son valiosas herramientas de evaluación de hosts, pero tienen 2 riesgos principales que se deberían evitar, estos son:

- Que los atacantes pueden utilizarlos para determinar las debilidades de un sistema de seguridad
- Se puede confiar demasiado en los scanners.

- **Psad**

Es un grupo de 3 demonios para sistemas escritos en Perl y C que están diseñados para trabajar con el sistema de cortafuegos de Linux “iptables”, la función principal es detectar los port scans y otros tráficos sospechosos.

Tiene la funcionalidad de detectar, alertar y bloquear los port scans. Es una aplicación muy potente si se la sabe utilizar.

INSTALACIÓN

Se debe obtener el fichero psad-2.1.7.tar.bz2, el cual está comprimido y empaquetado. Para descomprimirlo y desempaquetarlo y obtener la carpeta psad-2.1.7 se ejecuta el siguiente comando:

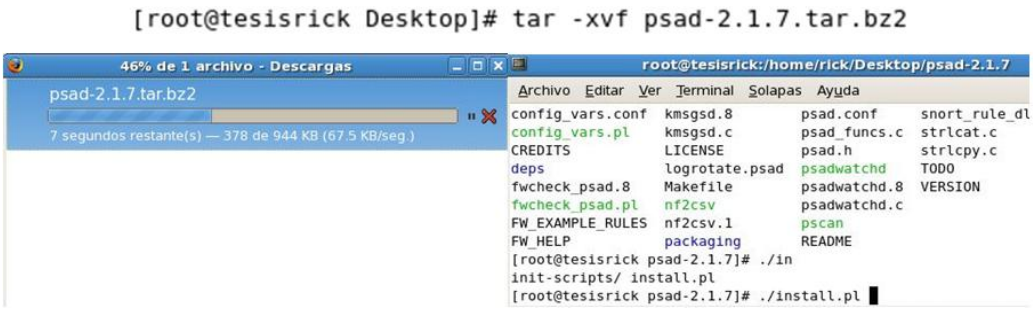


Figura 6.46: Instalación de la herramienta PSAD mediante un fichero tar.bz2.
Fuente: Autor de tesis.

Luego de ejecutar el anterior comando se instalará el paquete Psad, y permitirá configurar los principales parámetros que necesita el demonio para el correcto funcionamiento.

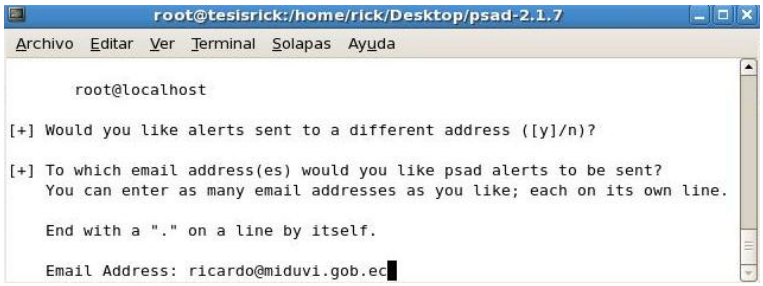


Figura 6.47: Ingreso de mail de reportes y alertas en el proceso de instalación del paquete.
Fuente: Autor de tesis.

Como se visualiza en la figura anterior se está indicando el correo al cual pueden llegar las alertas que se generen en una determinada búsqueda.

Para finalizar la instalación se procede a iniciar y detener el demonio para verificar que puede ser utilizado sin ningún problema.

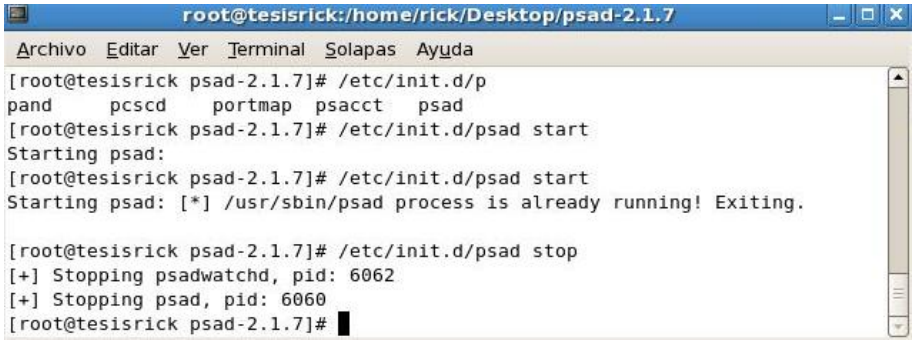


Figura 6.48: Inicio del demonio PSAD para la verificación que la aplicación funciona correctamente.
Fuente: Autor de tesis.

6.3.3. PROTECCIÓN Y RESPALDO DE DATOS.

Muchos son los riesgos que puede correr una red si no se tiene un plan de protección o respaldo de datos en caso de una emergencia.
Además de esto muchos servicios de red pueden resultar vulnerables a las escuchas electrónicas, sniffers, scanners, etc. Esto representa un problema importante, ya que, incluso en un entorno de red cerrado, debe existir un medio seguro para mover archivos, establecer permisos, ejecutar scripts de Shell, etc.
Aquí se presentan algunas alternativas para dar solución a los problemas anteriormente mencionados.

6.3.4.1 SECURITY SHELL PARA INTERCAMBIO DE DATOS

Security Shell es un sistema de inicio de sesión seguro y la evolución efectiva de telnet, rlogin, rsh y rcp.

SSH admite varios algoritmos, entre los cuales se incluyen:

BlowFish: es un esquema de cifrado de 64 bits, se suele utilizar para realizar gran cantidad de cifrados a alta velocidad.

Triple DES: Data Encryption Estándar (Norma de Cifrado de Datos), es un sistema de IBM desarrollado en 1974, es el estándar del gobierno estadounidense para cifrar datos no clasificados.

IDEA: International Data Encryption Algorithm, un eficaz algoritmo de cifrado de bloques que funciona con una clave de 128 bits. Es muy seguro.

RSA: Rivest-Shamir-Adelman, es un sistema criptográfico de claves públicas/privadas ampliamente utilizado.

SSH incorpora la compatibilidad con estos algoritmos, para crear un producto más flexible y ampliable. La arquitectura de ssh se tal que al protocolo básico le da igual el algoritmo que se utilice, por lo tanto es posible cambiar rápidamente de uno a otro sin modificar el protocolo clave y las funciones de ssh.

El cliente ssh permite varias opciones en línea de comandos, éstas son:

OPCION	FUNCION
-a	Especifica que ssh no debe utilizar el envío de autenticacion de agentes.
-c cifrado	Especifica el cifrado que se desea utilizar.
-e car	Especifica un carácter de escape alternativo.
-f	Sirve para que ssh se ejecute en segundo plano una vez que se ha autenticado la sesión.
-i archivo	Especifica un archivo de identidades.
-l usuario	Especifica el usuario que inicia la sesión.
-n	Sirve para redireccionar la entrada desde /dev/null.
-p puerto	Especifica el puerto al que debe dirigirse ssh (22)
-P	Especifica que ssh debe utilizar un puerto de origen sin privilegios.
-q	Se utiliza para enviar ssh al modo quiet.
-t	Sirve para indicar a ssh que abra una tty, aun cuando ya vaya a enviar un solo comando.
-v	Especifica una salida de depuración detallada.
-x	Sirve para desactivar el envio de X11.

Tabla 6.2: Tabla con cuadro de opciones y funciones disponibles en la ejecución de un spofing.
Fuente: Autor de tesis.

Ejemplo: Conexión mediante ssh

La forma de utilizar ssh es realmente fácil, basta con definir la dirección IP a la cual se requiere acceder y se antepone “ssh”, como se muestra en la figura.

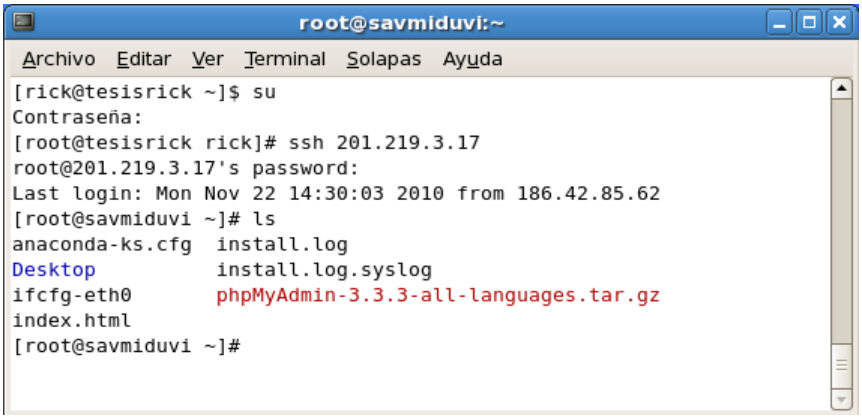


Figura 6.49: Conexión SSH al servidor mediante el comando ssh + dirección IP.
Fuente: Autor de tesis.

Si se puede observar el prompt de la consola, se logró acceder a [root@savmiduvi]#, lo cual provee el control total del servidor.

La solución a esta falla de seguridad es muy simple, sencillamente bloquear o cerrar el puerto 22 que es el que permite iniciar la sesión con SSH.

6.3.4.2. SCP: COPIA SEGURA DE DATOS REMOTOS.

Esta herramienta permite copiar archivos entre hosts utilizando una autenticación y un cifrado transparentes de ssh. Siempre que sea posible se recomienda la utilización de SCP.

Sintaxis

usuario@host1:nombre_de_archivo usuario@host2:nombre_de_archivo

Las opciones para SCP se resumen en la siguiente figura.

OPCION	FUNCION
-A	Desactiva las estadísticas de los archivos individuales.
-a	Activa las estadísticas de los archivos individuales.
-c cifrado	Especifica el cifrado que se va a utilizar para la transferencia.
-i archivo	Especifica un archivo de identidades alternativo.
-L puerto	Especifica que scp debe utilizar un puerto de origen sin privilegios.
-o opciones ssh	Sirve para pasar las opciones extendidas de ssh a ssh.
-P puerto	Especifica el puerto de host remoto al que se dirige scp.
-q	Desactiva las estadísticas de la sesión.
-Q	Activa las estadísticas de la sesión.
-r	Especifica que scp debe copiar los directorios recursivamente.
-v	Especifica que scp debe ejecutarse en modo personalizado.

Tabla 6.3: Tabla con cuadro de opciones y funciones con Shell Secure.
Fuente: Autor de tesis.

La ventaja de la herramienta es que es multiplataforma y que en la actualidad existen interfaces muy amigables para lograr una conexión de Shell segura.

En la siguiente figura se puede apreciar la conexión desde un equipo Windows a un servidor Linux, en el intercambio de archivos de un servidor web. Se realiza muy fácilmente y en pocos segundos se transfiere los ficheros.

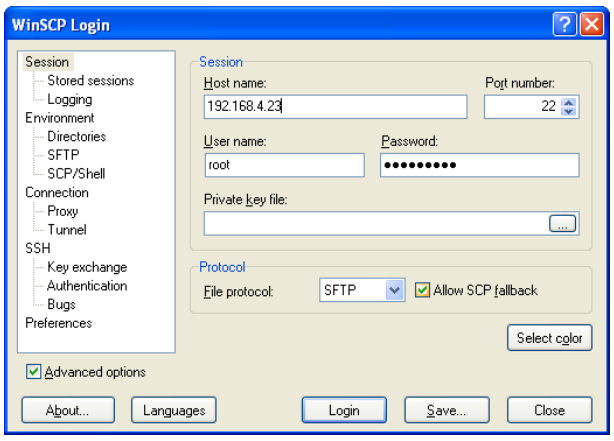


Figura 6.50: Pantalla principal de la herramienta WinSCP al momento de realizar una conexión.
Fuente: Autor de tesis.

En la siguiente figura, en la columna izquierda se encuentra los directorios de Windows, mientras que en la parte derecha se encuentra el servidor web bajo Linux, el cual recibe los ficheros cuando existen cambios o actualizaciones en el servidor.

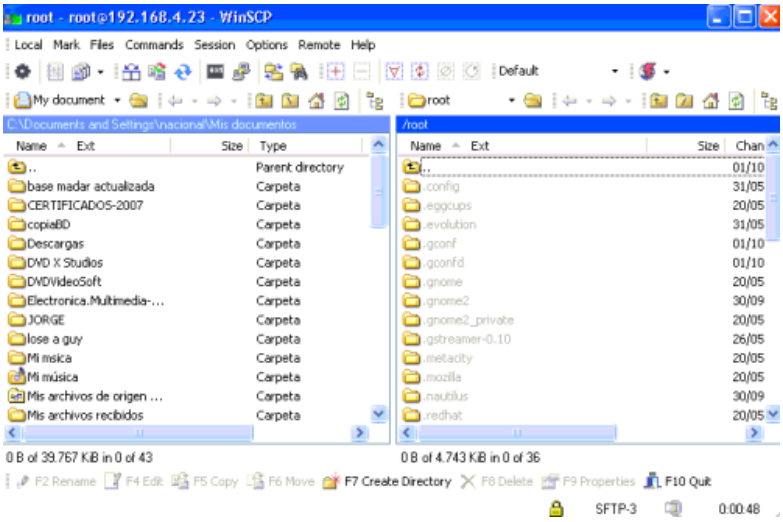


Figura 6.51: Transferencia de archivos de Windows a Linux utilizando WinSCP.
Fuente: Autor de tesis.

Como se puede observar, en los 2 equipos se tiene la misma estructura para los directorios que alojarán las aplicaciones web instaladas en el servidor, cada vez que se realizan nuevas modificaciones se deberán arrastrar de izquierda a derecha con los archivos correspondientes para reemplazarlos en el servidor.

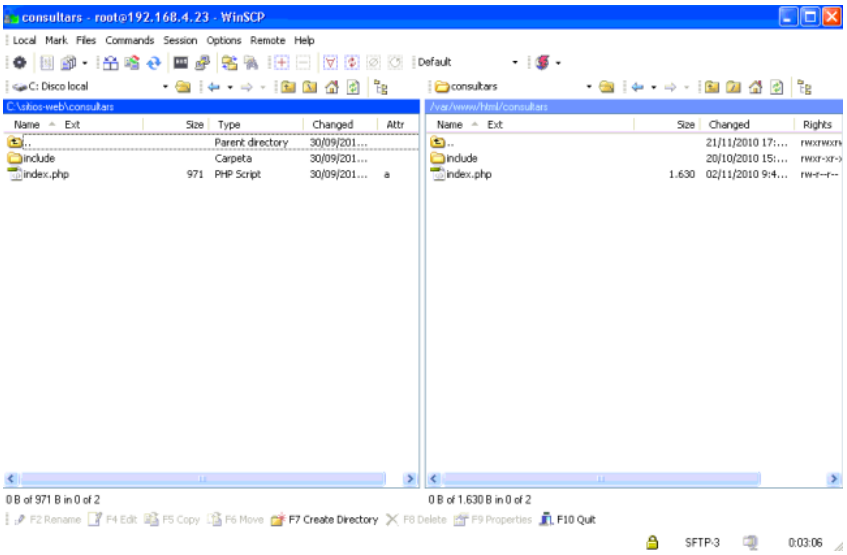


Figura 6.52: Envío de archivos al servidor web.
Fuente: Autor de tesis.

6.3.4.3. COPIAS DE SEGURIDAD COMO PLAN DE CONTINGENCIA

Es muy importante tener un plan de respaldo y copias de seguridad de datos en cualquier institución o empresa, ya que existen una variedad de causas para que la información alojada en los servidores pueda dañarse o aún perderse.

Realizar copias de seguridad de todos los datos importantes de una institución es un seguro económico contra potenciales desastres que pueden suscitarse y a la vez pueden resultar muy costosos solucionarlos o repararlos.

- **RSYNC**

Existen datos muy importantes y vitales en una empresa o institución que necesariamente hay que identificarlos, para poder tomar acción con cualquier herramienta de respaldo y copias de seguridad.

La utilidad Rsync es una copia de un programa diseñado para replicar grandes cantidades de datos. Una de las ventajas es que puede encriptar las transferencias de datos con ssh, haciendo el proceso más rápido y más seguro.

Sintaxis

 # rsync opciones origen destino

En la siguiente lista se describen las principales opciones que se pueden utilizar en la línea de comandos:

OPCION	FUNCION
-a: Archivo	Desactiva las estadísticas de los archivos individuales.
-b	Hace copias de seguridad de todos los archivos destino en lugar de sustituirlos.
-D	Se usa cuando se replican sistemas de archivos. Solo como root.
-g	Preserva los permisos de grupo de los archivos que se estan duplicando.
-H	Preserva los enlaces. Esta opción hace que rsync vaya mas lento.
-l	Copia enlaces simbólicos como enlaces simbolicos. Muy utilizada.
-n	muestra los archivos que se tranferirán, pero no los que se estan tranfiriendo
-o	Preserva la autoría de usuario de los archivos replicados.
-p	Preserva los permisos de archivos.
-r	Activa la recursividad, transfiriendo todos los subdirectorios.
-t	Preserva la hora de modificación de cada archivo. Incluido en -a.
-v	Lista los archivos que se estan transfiriendo.
-vv	Igual que -v, pero además lista los archivos que se ignoran.
-vvv	Igual que -vv, pero imprime información e depuración de rsync.
-z	Activa la compresión, más util sobre Internet que sobre una LAN.

Tabla 6.4: Tabla con el cuadro de opciones y funciones de la herramienta Rsync.
Fuente: Autor de tesis.

Como se visualizó en el cuadro anterior, existen muchas opciones que se pueden utilizar con esta aplicación.

Ejemplo: Script para genera copia de seguridad de usuario.

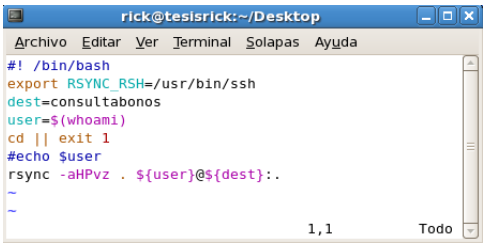


Figura 6.53: Script para realizar una copia de seguridad utilizando Rsync.
Fuente: Autor de tesis.

Lo que se pretende realizar en este ejemplo es un bash script sencillo que genera una copia de seguridad desde el escritorio del usuario al servidor de copias de seguridad. El servidor está definido en la variable "**dest**", la variable user está asignada al nombre del usuario de la cuenta que ejecuta el script, el comando "**cd**" cambia al directorio personal del usuario. La variable de entorno RSYNC_RSH contiene el nombre de la Shell de rsync utilizará.

Al ejecutar el script se generará una réplica de los archivos del directorio personal del usuario que lo ejecutará.

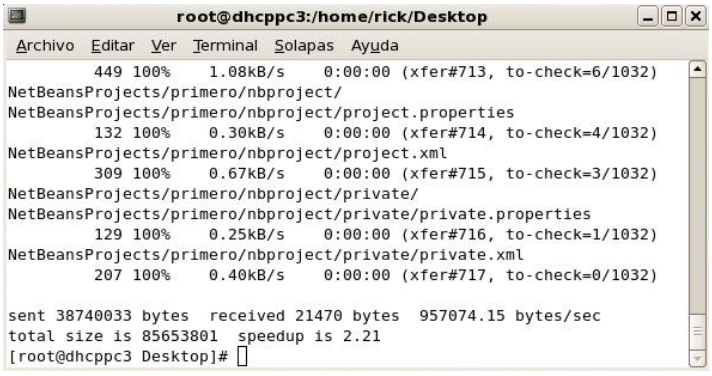


Figura 6.54: Detalle de los resultados luego de la ejecución del script.
Fuente: Autor de tesis.

Rsync indica el número de archivos que considera en la copia, ya que puede o no tomar en cuenta a todos los archivos porque no fueron alterados o modificados. También se indica el progreso de avance para saber si la transferencia tuvo o no éxito.

6.3.4.4. COPIAS DE SEGURIDAD AUTOMATIZADAS.

Es algo elemental que estas copias pueden ser automatizadas utilizando scripts similares, como por ejemplo el demonio **Cron** o mejor aún utilizar el programa **Crontab**.

Además se puede ejecutar un script de tarea en el servidor, para hacer copias de seguridad en otro. Estas copias pueden ser fácilmente transferidas a algún lugar seguro o medio extraíble como CD, DVD, memoria flash, etc.

Ejemplo utilizando "Cron"

El primer paso es verificar si está instalado el servicio con cualquiera de los siguiente comandos: ***# /etc/rc.d/init.d/crond status*** ó ***# service crond status***, al realizar esto debe mostrar el mensaje que el servicio esta ejecutándose como se muestra en la figura.

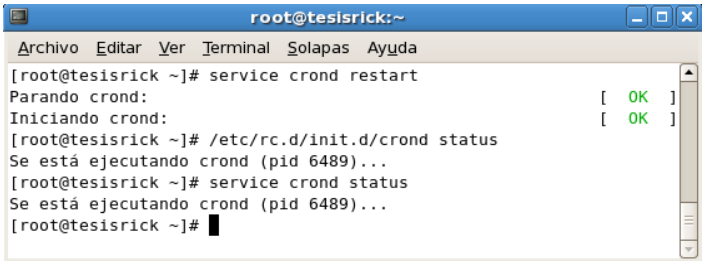


Figura 6.55: Ejecución del comando para la inicialización de cron.
Fuente: Autor de tesis.

Luego de verificar que el servicio está corriendo sin problemas, se debe identificar los archivos **cron.*** que se encuentran en el directorio /etc/ , en los cuales se crearán los scripts a ejecutarse cada hora, cada día, cada semana y cada mes, como se muestra en la siguiente figura.

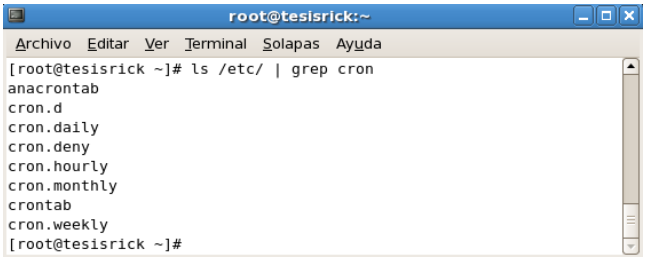


Figura 6.56: Verificación de archivos cron.* en el directorio /etc/
Fuente: Autor de tesis.

Para este ejemplo se creará un script de respaldo para la **página web** de consulta bonos del MIDUVI, en el directorio /etc/cron.hourly/.

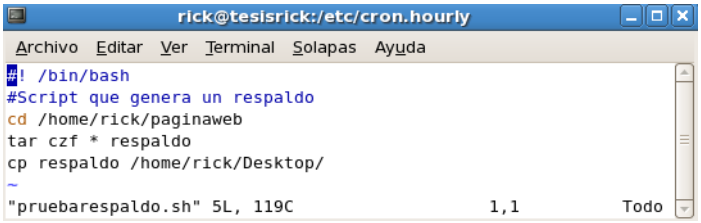


Figura 6.57: Script para generar un archivo de respaldo cada hora.
Fuente: Autor de tesis.

Además se debe dar permisos necesarios para que se pueda ejecutar como tarea programada, así que se procede a utilizar el comando que se muestra en la figura.

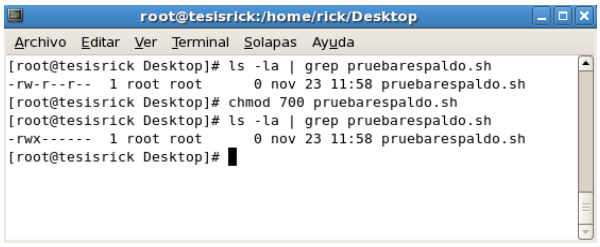


Figura 6.58: Verificación de los archivos creados por el anterior script.
Fuente: Autor de tesis.

Para finalizar se comprueba que el archivo se encuentre en el directorio /etc/cron.hourly/ y luego de una hora un minuto el servicio llamará al script y creará el archivo comprimido para poder generar un fichero de respaldo.

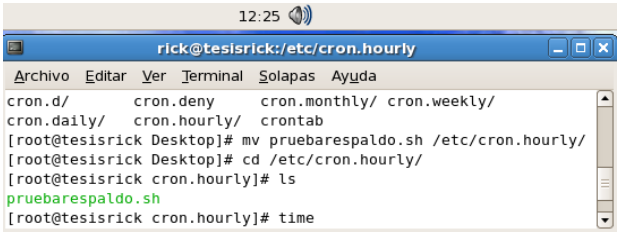


Figura 6.59: Verificación de la hora en que se ejecutó la aplicación.
Fuente: Autor de tesis.

Como se mencionó anteriormente existe una herramienta llamada Crontab que permite realizar muchas más acciones. Para explicar de mejor manera se realizar un script que ejecute un comando para generar un archivo como respaldo de varios archivos que en un ambiente de producción podrían ser bases de datos, directorios, ficheros importantes, etc.

El primer paso será verificar el contenido del archivo **Crontab** como se muestra en la siguiente figura.

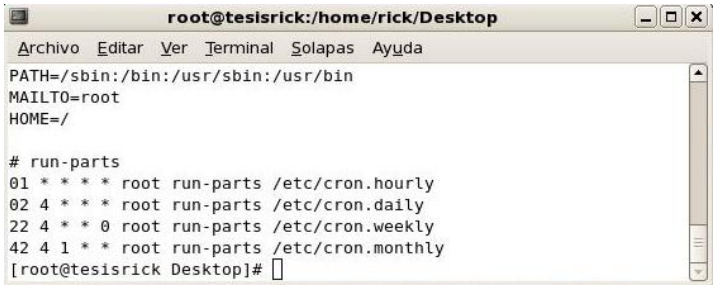


Figura 6.60: Archivo de configuración de Crontab para generar respaldo programados.
Fuente: Autor de tesis.

Como se puede ver, están las llamadas a los archivos " **cron.*** ", que son los que ejecutan los scripts que anteriormente se explicó.

Para realizar una nueva tarea programada se debe añadir una línea que indique el tiempo, el propietario y el comando a ejecutarse. Para entender de mejor forma se expone el siguiente cuadro con las principales opciones de Crontab.

Minuto Hora DiaDelMes Mes DiaDeLaSemana Usuario Comando

Campo	Descripción
Minuto	Controla el minuto de la hora en que el comando será ejecutado, este valor debe de estar entre 0 y 59.
Hora	Controla la hora en que el comando será ejecutado, se especifica en un formato de 24 horas, los valores deben estar entre 0 y 23, 0 es medianoche.
Día del Mes	Día del mes en que se quiere ejecutar el comando. Por ejemplo se indicaría 20, para ejecutar el comando el día 20 del mes.
Mes	Mes en que el comando se ejecutará, puede ser indicado numéricamente (1-12), o por el nombre del mes en inglés, solo las tres primeras letras.
Día de la semana	Día en la semana en que se ejecutará el comando, puede ser numérico (0-7) o por el nombre del día en inglés, solo las tres primeras letras. (0 y 7 = domingo)
Usuario	Usuario que ejecuta el comando.
Comando	Comando, script o programa que se desea ejecutar. Este campo puede contener múltiples palabras y espacios.

Tabla 6.5: Tabla de opciones y descripción de funcionalidades de Crontab.
Fuente: http://www.linuxtotal.com.mx/index.php?cont=info_admon_006.

Luego de verificar que crontab este corriendo en el servidor sin ningún problema, se procede a crear la tarea programada para empaquetar y comprimir un directorio el cual contiene la aplicación web para consulta de bonos de vivienda. La siguiente figura detalla el comando generado.

Figura 6.61: Comando para generar un archivo de resplado de tipo .tar cada hora.
Fuente: Autor de tesis.

Se procede a guardar los cambios y se reinicia el servicio.

Figura 6.62: Reinicio del servicio crontab mediante el comando service crond restart.
Fuente: Autor de tesis.

Ahora en la siguiente figura se pueden verificar los resultados, en la cual se crearán los nuevos ficheros empaquetados y comprimidos en la carpeta /home/rick/backups/, lo que permitirá tener un respaldo de la información más importante que maneje la institución.

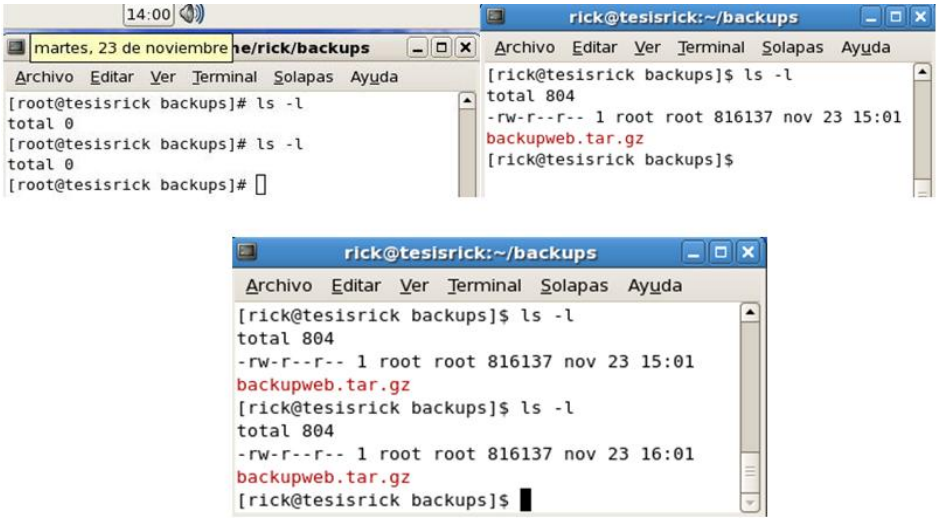


Figura 6.63: Verificación de las copias de seguridad generadas cada hora en el directorio /backups.
Fuente: Autor de tesis.

6.4. SOLUCIÓN 4: DESARROLLO DE UNA APLICACIÓN WEB ENFOCADO A LA SEGURIDAD DE LA INFORMACIÓN.

Al tener las bases de datos de los beneficiarios que recibieron un incentivo de vivienda migradas a MySQL, se puede realizar varias aplicaciones orientadas a la WEB que controlen, administren y gestionen estos datos.

Luego del análisis de requerimientos (véase Anexo B – Análisis de Requerimientos) se definió que es necesario desarrollar 3 aplicaciones que se detallan a continuación:

- **Interfaz de consulta del bono de vivienda.-** Esta aplicación sirve para que entidades financieras, promotores inmobiliarios, oferentes de vivienda y público en general puedan consultar si alguna persona ya recibió algún incentivo de vivienda en el MIDUVI.
- **Interfaz de consulta para la accesibilidad al bono de vivienda.-** La aplicación de accesibilidad está dirigida para las personas que aún no han recibido el bono de vivienda y que necesitan conocer si son aptas para postular al incentivo de vivienda.
- **Módulo para el control y seguimientos de proyectos de vivienda del área rural.-** Este módulo es esencial para el seguimiento de los proyectos que se ejecutan en el Ministerio, ya que abarca desde la emisión del bono hasta el acta entrega recepción del mismo.

6.4.1. INTERFAZ DE CONSULTA DEL BONO DE VIVIENDA.

Este primer aplicativo esta realizado en PHP y comprende la relación con la tabla “tbnacional”, que contiene los registros de beneficiarios del bono de vivienda alojado en el motor de MySQL.

INSTALACIÓN DEL DEMONIO HTTPD Y EL MOTOR MYSQL EN EL SERVIDOR QUE ALOJARÁ LA APLICACIÓN DE CONSULTA BONOS.

La instalación de del servidor web Apache y el motor de base de datos MySQL en el servidor bajo Linux se realizará de la siguiente manera:

Se ejecuta: ***# yum install httpd***

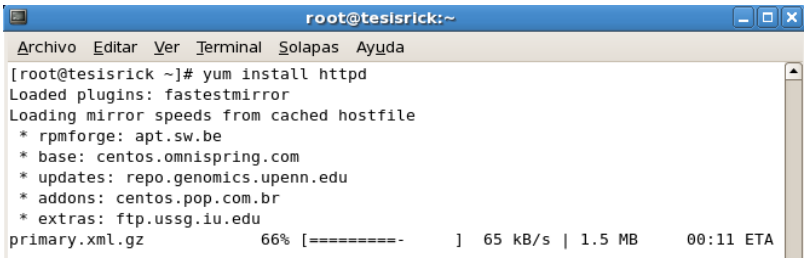


Figura 6.64: Instalación del servicio web con el comando yum install httpd.
Fuente: Autor de tesis.

Luego descargará los complementos y paquetes necesarios y se debe proceder a configurar el servidor web en la siguiente ruta:

 # vim /etc/httpd/conf/httpd.conf

La configuración principal para que el servidor pueda alojar la aplicación de consulta de bonos debe configurarse como se ve en la siguiente figura.

```
User apache
Group apache

#ServerAdmin joinic@localhost
ServerAdmin administrador@miduvi.gov.ec

UseCanonicalName Off

#DocumentRoot "/var/www/"
#DocumentRoot "/var/www/ejemplosphp"
DocumentRoot "/var/www/consultabonos"

#<Directory "/var/www/ejemplosphp/">
<Directory "/var/www/consultabonos/">
```

Figura 6.65: Configuración general del archivo httpd.conf en el cual se determina los directorios web.
Fuente: Autor de tesis

Luego el servidor no está iniciado y por lo tanto en el navegador no se presenta ningún resultado, como se ve en la figura.

Figura 6.66: Comprobación del funcionamiento de la aplicación web antes de iniciar el servicio web.
Fuente: Autor de tesis

Para poder iniciarlo se debe ejecutar el siguiente comando:

 # service httpd restart

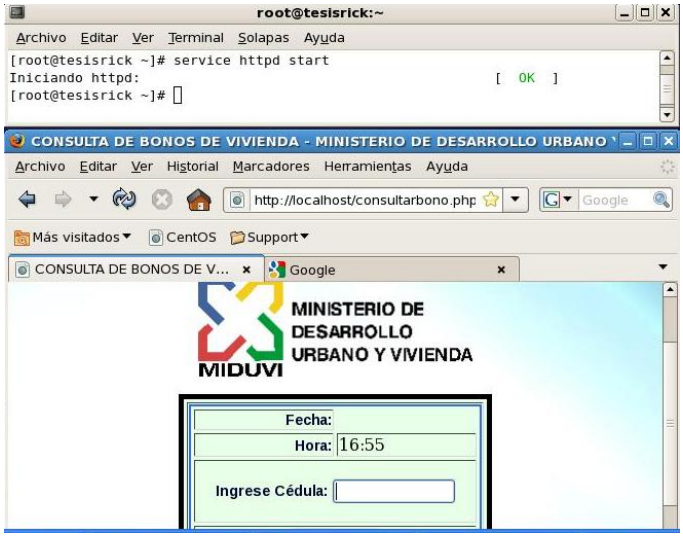


Figura 6.67: Prueba de la aplicación de consulta bonos luego de la ejecución del comando de inicio del servicio web.
Fuente: Autor de tesis.

Para la instalación de MySQL se siguen casi los mismos pasos, es decir, con el comando **# yum install mysql mysql-server** se logra obtener un sistema de gestión de base de datos en el servidor.

Para acceder al servidor se puede utilizar el mismo MySQL-Front ya que soporta conexiones remotas y desde la herramienta se importarán los datos como se mostró en un capítulo anterior.

PANTALLA PRINCIPAL

Figura 6.68: Pantalla principal de la aplicación "consulta bonos" vista en producción desde el internet.
Fuente: Autor de tesis.

Para utilizar este aplicativo se debe ingresar el número de cédula del beneficiario del bono de vivienda.

La consulta está diseñada para buscar tanto en el campo del beneficiario como el del cónyuge, como se presenta en la siguiente figura.

```
$sentencia = "select NOMPOSTU,CEDPOSTU,NOMCONYU,CEDCONYU,
              PROVINCIA,CANTON,PROYECTO,C_ESTADO_DETALLE,C_ESTADO_PORTAL
              from tbnacional n, tbestado e
              where n.c_estado_id = e.c_estado_id and
              (cedpostu = '$cedula' or cedconyu = '$cedula')";
```

Figura 6.69: Sentencia SQL utilizada en la búsqueda de registros desde la aplicación en internet.
Fuente: Autor de tesis.

Luego de ingresar el número de cédula la aplicación presentará la siguiente pantalla, como se muestra en la figura.

Figura 6.70: Prueba del funcionamiento de la aplicación y consulta SQL al devolver datos encontrados.
Fuente: Autor de tesis.

6.4.2. INTERFAZ DE CONSULTA DE LA ACCESIBILIDAD AL BONO.

La funcionalidad de este aplicativo será de indicar e informar a las personas que no han sido beneficiadas del bono de vivienda si pueden o no aplicar al incentivo. Las áreas de consulta serán área urbana y área rural. Cada una de ellas tiene sus propios parámetros de calificación y el aplicativo realizará el proceso de validación de requisitos y mostrará el mensaje que indique si esa persona puede o no postular al bono de vivienda.

Este aplicativo incorpora una base de datos adicional que deberá ser importada desde un archivo plano y que su tamaño es de 1,3 GB.

Figura 6.71: Identificación del archivo del registro social que será importado a la base en MySQL. Fuente: Autor de tesis.

PROCESO DE IMPORTACIÓN DE DATOS DEL REGISTRO SOCIAL

Para este proceso es muy difícil encontrar un procesador de textos que soporte este archivo, razón por la cual no se puede verificar en que codificación están los datos a importarse.

Si se utiliza un método para importar los datos sin conocer la codificación real en la cual fue creado el archivo plano, es posible que los resultados no sean los esperados ya que no se completará correctamente el proceso.

Ejemplo: Importación de la base del registro social.

El primer paso es crear la tabla que alojará a **“miduvipersona”**, luego la tabla **“miduvinucleo”**, que son las dos necesarias para poder realizar la consulta requerida.

En la siguiente figura se puede visualizar el comando SQL para crear la tabla **”tbpersona”** con todos los campos necesarios, luego de esto se procederá a realizar la importación de datos como se realizó anteriormente.

```
CREATE TABLE `tbpersona` (
  `idhogar` bigint(20) NOT NULL,
  `idnucleo` bigint(20) NOT NULL,
  `orden` int(11) NOT NULL,
  `residente` int(11) NOT NULL,
  `apellidos` varchar(255) NOT NULL,
  `nombres` varchar(200) NOT NULL default '',
  `sexo` int(11) NOT NULL,
  `edad` int(11) NOT NULL,
  `edadMes` int(11) NOT NULL,
  `parentesco` int(11) NOT NULL,
  `civil` int(11) NOT NULL,
  `parentescoNucleo` int(11) NOT NULL,
  `tdocumento` int(11) NOT NULL,
  `edocumento` int(11) NOT NULL,
  `nacionalidad` int(11) NOT NULL,
  `cedula` varchar(11) NOT NULL,
  `iessl` int(11) NOT NULL,
  `iess2` int(11) NOT NULL,
  `discapacidad` int(11) NOT NULL,
  `idioma1` int(11) NOT NULL,
  `idioma2` int(11) NOT NULL,
  `matricula` int(11) NOT NULL,
  `asistencia` int(11) NOT NULL,
  `establecimiento` int(11) NOT NULL,
  `instruccion` int(11) NOT NULL,
  `aprobado` int(11) NOT NULL,
  `actividad` int(11) NOT NULL,
  `itrabajo` decimal(11,0) NOT NULL,
  `ialquiler` decimal(11,0) NOT NULL,
  `ipension` decimal(11,0) NOT NULL,
  `ibeca` decimal(10,0) NOT NULL,
  `fnac` datetime NOT NULL,
  `fonetico` varchar(100) NOT NULL,
  `status` varchar(6) NOT NULL,
  `selben` varchar(100) NOT NULL,
  PRIMARY KEY  (`cedula`),
  KEY `idnucleo` (`idnucleo`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;
```

Figura 6.72: Detalle de campos de la tabla persona en la cual se importará los datos del registro social.
Fuente: Autor de tesis

En la siguiente figura se muestra la tabla **“nucleo”** que se relaciona de 1 a varios con la tabla **“persona”** mediante el identificador **idnucleo**, el cual servirá para generar las consultas relacionadas entre las 2 tablas.

```
CREATE TABLE `nucleo` (
  `id` bigint(20) NOT NULL DEFAULT '0',
  `idhogar` bigint(18) DEFAULT NULL,
  `puntaje` varchar(15) DEFAULT NULL,
  `idnucleo` bigint(20) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `idhogar` (`idhogar`,`idnucleo`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;
```

Figura 6.73: Detalle de campos de la tabla núcleo en la cual se importarán los datos del registro social.
Fuente: Autor de tesis.

Luego de importar las tablas antes mencionadas, se procederá a realizar los testing para verificar si los datos se encuentran completos y sin inconsistencias.

TABLA PERSONA

```
select count(*) as totalpersona from tbpersona;
```

totalpersona
4560674

Figura 6.74: Verificación del proceso de importación y conteo de registros en la tabla persona.
Fuente: Autor de tesis.

TABLA NÚCLEO

```
select count(*) as totalnucleo from nucleo;
```

totalnucleo
2421716

Figura 6.75: Verificación del proceso de importación y conteo de registros en la tabla núcleo.
Fuente: Autor de tesis.

DESARROLLO DE LA APLICACIÓN

Para el desarrollo de esta aplicación de acuerdo a los requerimientos de la institución, se presentará una interfaz para el sector urbano y otra para el sector rural.

La característica principal de la interfaz para el sector urbano es que presenta 3 opciones para la selección del tipo de vivienda, que se detallan a continuación:

- Construcción
- Adquisición
- Mejoramiento

CONSULTA_URBANA.PHP

La pantalla para esta consulta es la siguiente:

Figura 6.76: Pantalla principal del aplicativo para la consulta de aspirantes al bono de vivienda del área urbana.

Fuente: Autor de tesis.

Los mensajes que se devuelve la consulta son los siguientes:

Cuando si consta en la base del Registro Social.	ESTIMADO/A: HOYOS SERNA VIRGEN MARIA USTED **SI** PUEDE POSTULAR AL APOYO ECONOMICO POR UN VALOR DE **5000** USD. A UNA VIVIENDA DE HASTA **12000** USD.
Cuando el puntaje es mayor	Usted No califica al apoyo económico para la vivienda Su puntaje es mayor al permitido
Cuando no consta en la base del RS.	No se encuentra registrado en la Base de Datos Si usted desea ser parte de la Base de Datos del Registro Social Haga clic aqui

Tabla 6.6: Tabla de mensajes devueltos por la aplicación de consulta urbana.

Fuente: Autor de tesis.

La validación que se realiza para cada caso de tipo de vivienda se la puede analizar en el código que se muestra en la siguiente figura.

```
//PROCEDEMOS A REALIZAR LA CONSULTA A LA BASE DE DATOS DEL REGISTRO SOCIAL.
$sql = "  select p.cedula, p.apellidos,p.nombres, n.puntaje
          from nucleo n, tbpersona p
          where n.idhogar = p.idhogar and n.idnucleo = p.idnucleo
          and p.cedula = '$cedula__2' ";
$result = mysql_query($sql,$conexion) or die (mysql_error());
$cuantos = mysql_num_rows($result);
if ($cuantos > 0){
  while ($reg=mysql_fetch_array($result)) {
      $ced = $reg['0'];
      $ape = $reg['1'];
      $nom = $reg['2'];
      $pun = $reg['3'];
  }
  //Verificamos que tipo de bono es.
  if ($tipo__2==1){ //CONSTRUCCION
      if ($pun>0 and $pun <= 58.10){
      $bono = 3600;
          if($pun>0 and $pun <=52.90){ $valorviv=1; //valor vivienda hasta 12.000
          }
          else if($pun>52.90 and $pun<=58.10){$valorviv=2;
          }
      }else $bono = 0;
  }else
  if ($tipo__2==2){ //ADQUISICION
      if ($pun>0 and $pun <= 58.10){  $bono = 5000;
          if($pun>0 and $pun<=52.90){ $valorviv=1;
          } else if($pun>52.90 and $pun<=58.10){
              $valorviv=2;
          }
      }else $bono = 0;
  }else
  if ($tipo__2==3){ //MEJORAMIENTO
      if ($pun>0 and $pun <= 52.90){
      $bono = 1500;
      $valorviv=3;
      }else $bono = 0;
```

Figura 6.77: Código fuente en PHP que realiza la consulta SQL y la comparación del rango de puntaje.
Fuente: Autor de tesis.

Según el rango de puntaje que se valide, el bono y el valor de la vivienda serán diferentes, para cada caso existen comentarios en el código php.

Esta aplicación está instalada en el servidor de producción, por lo tanto, desde cualquier parte del mundo se puede acceder sin problemas.

CONSULTA_RURAL.PHP

La pantalla para esta consulta es la siguiente:

Figura 6.78: Pantalla principal del aplicativo para la consulta de aspirantes al bono de vivienda del área rural.

Fuente: Autor de tesis.

Los mensajes que se devuelve la consulta son los siguientes:

Cuando si consta en la base del Registro Social.	DOMINGUEZ PANTA EDGARDO USTED SI PUEDE POSTULAR AL APOYO ECONOMICO POR UN VALOR DE 3960 USD. Y DEBE PONER UN APORTE DE 360 USD.
Cuando el puntaje es mayor	Usted No califica al apoyo económico para la vivienda Su puntaje es mayor al permitido
Cuando no consta en la base del RS.	No se encuentra registrado en la Base de Datos Si usted desea ser parte de la Base de Datos del Registro Social Haga clic aqui

Tabla 6.7: Tabla de mensajes devueltos por la aplicación de consulta rural.

Fuente: Autor de tesis.

La validación que se realiza para este caso es únicamente con el número de cédula y el puntaje del registro social, se puede apreciar en el siguiente código.

```
//PROCEDEMOS A REALIZAR LA CONSULTA A LA BASE DE DATOS DEL REGISTRO SOCIAL.
$sql = "  select p.cedula, p.apellidos,p.nombres, n.puntaje
          from nucleo n, tbpersona p
          where n.idhogar = p.idhogar
          and n.idnucleo = p.idnucleo
          and p.cedula = '$cedula__1' ";
$result = mysql_query($sql,$conexion) or die (mysql_error());
$cuantos = mysql_num_rows($result);
if ($cuantos > 0){
  while ($reg=mysql_fetch_array($result)) {
      $ced = $reg['0'];
      $ape = $reg['1'];
      $nom = $reg['2'];
      $pun = $reg['3'];
  }
  //Calculamos el valor del bono segun el puntaje.
  $bono = 0;
  $aporte = 0;
  if ($pun>0 and $pun < 31.01){
      $bono = 5000;
      $aporte = 0;
  }else
  if ($pun>=31.01 and $pun < 44.52){
      $bono = 5000;
      $aporte = 250;
  }else
  if ($pun>=44.52 and $pun <= 52.90){
      $bono = 3960;
      $aporte = 360;
  }else $bono = 0;
```

Figura 6.79: Código fuente en PHP que realiza la consulta SQL y la comparación del rango de puntaje. Fuente: Autor de tesis.

Como se pudo apreciar, en las condiciones hay 3 categorías que varían de acuerdo al puntaje y según esto varía el aporte que debe realizar el beneficiario.

Se pude finalizar mencionando que estas consultas trabajan con un nivel de velocidad de procesamiento considerable y que los resultados se presentan al usuario de forma inmediata.

6.4.3. MÓDULO PARA EL CONTROL Y SEGUIMIENTO DE LOS PROYECTOS DE VIVIENDA PARA EL AREA RURAL Y URBANO MARGINAL.

La realización de este módulo es esencial en el Ministerio de Desarrollo Urbano y Vivienda, por el área de acción que abarca.

La necesidad de este módulo nace ya que hasta el año 2009 no existía una aplicación que gestione el seguimiento y control de los proyectos de vivienda del área rural – urbano marginal.

Este módulo presenta opciones desde Emisión, Aprobación, Contratación, Pagos, Control de Avance de Obra, Registro de actas provisionales – definitivas y Finalización de la Vivienda.

El manejo de este módulo se lo explica claramente en el Anexo C – Manual de Usuario del Modulo de Control de Proyectos de vivienda.

DICCIONARIO DE DATOS

NOMBRE_TABLA	TIPO_OBJETO	DESCRIPCION
tbtotalcalifidos	Entity	Tabla para almacenar los CALIFIDOS de proyectos de vivienda Rural - Urbano Marginal
tbregion	Entity	Almacena la región segun la codificacion de SENPLADES.
tbprovincia	Entity	Almacena registros de las provincias del Ecuador.
tbcanton	Entity	Almacena registros de cantones del Ecuador.
tbparroquia	Entity	Almacena registros de las parroquias del Ecuador.
tbregionnatural	Entity	Almacena la región natural.
tbproyecto	Entity	Almacena registros de proyectos de vivienda como agrupación de personas que postulan al bono.
tbzonaGeografia	Entity	Almacena la zona o sector en donde se aplicará el beneficio.
tbtiposolucion	Entity	Almacena el tipo de solución del bono.
tbpersona	Entity	Almacena registros de las personas que postulan al bono de vivienda.
tbgenero	Entity	Almacena el sexo de las personas.
tbecivil	Entity	Almacena los tipos de estado civil.
tbcalificacion	Entity	Almacena información de la calificación general de las personas que postularon al bono de vivienda.
tbfiscalizador	Entity	Almacena los registros de fiscalizadores a cargo del proyecto de vivienda.
tbsupervisor	Entity	Almacena los registros de supervisores a cargo del proyecto de vivienda.
tbconstructor	Entity	Almacena los registros de constructores que realizarán los proyectos de vivienda.
tbtransacciones	Entity	Almacena las transacciones que realizan los diferentes usuarios a cargo de la aplicación.
tbusuario	Entity	Almacena los registros de usuarios habilitados para el uso de la aplicación.
tbcontrato	Entity	Almacena los contratos que se generan antes de iniciar la obra de un proyecto de vivienda.
tbestado	Entity	Almacena el estado de las postulaciones de personas que accedieron al bono de vivienda.
tbcarga	Entity	Almacena los registros de las cargas familiares que tiene el postulante.
tbparentesco	Entity	Almacena los tipos de parentesco posibles para la persona que postula al bono de vivienda.
tbtipoproyecto	Entity	Almacena el tipo de proyecto a ejecutarse.
tbcontratomod	Entity	Almacena el tipo de modalidad en contratación para los proyectos de vivienda.
tbfiscalizadortipo	Entity	Almacena los tipos de fiscalizares a cargo de la obra del proyecto de vivienda.
tbpoliza	Entity	Almacena las pólizas que se generan con el pago o financiación de un proyecto de vivienda.
tbpago	Entity	Almacena registros de proyectos que son pagados.
tbfinanciamiento	Entity	Almacena el registro de los diferentes tipos de financiamiento de proyectos de vivienda.
tbtransferencia	Entity	Almacena los registros de proyectos de vivienda que son asignados recursos financieros.
tbnacional	Entity	Almacena los registros historicos de beneficiarios anteriores al año 2009.
tbestadoproy	Entity	Almacena el estado del proyecto de vivienda, desde su inicio hasta la finalización.
tbemitido	Entity	Almacena registros de proyectos que son emitidos.
tbadjudicado	Entity	Almacena los registros de proyectos que son adjudicados.
tbanulado	Entity	Almacena los registros de bonos anulados o devueltos.
tbduplicado	Entity	Almacena los registros de personas que ya recibieron el bono y trataron de postular nuevamente.
tbusuario_a	Entity	Almacena los registros para perfiles y privilegios de usuarios habilitados al uso de la aplicación.
tbdiscapacidad	Entity	Almacena el tipo de discapacidad de las personas, si las tuviere.
tbconyuge	Entity	Almacena registros de los conyuges de postulantes al bono de vivienda.
tbaseguradora	Entity	Almacena registros de aseguradoras para la ejecución de proyectos de vivienda
tbtipopoliza	Entity	Almacena el tipo de póliza a ejecutarse.
tbrenovacion	Entity	Almacena las renovaciones para las pólizas vencidas.
tbavanceobra	Entity	Almacena los registros a nivel de porcentaje de avance de obra de los proyectos de vivienda.

Figura 6.80: Diccionario de Datos (a).
Fuente: Autor de Tesis.

TABLA TBTOTALCALIFIDOS	
NOMBRE DEL CAMPO	**DESCRIPCION**
CALNIN	Código de registro.
FECHA	Fecha de generación de registro.
CALQNTL	Numero de quintil para cada persona.
SOLUCION	Tipo de solución de postulación.
GEOGRAFIA	Area o sector en el que aplica la postulación.
CODPROYECT	Código de proyecto para el comite de vivienda.
NOMPROYECT	Nombre de proyecto para el comite de vivienda.
CALAPP	Apellido paterno del postulante.
CALAPM	Apellido materno del postulante.
CALNOM	Nombres del postulante.
CALEST	Estado civil del postulante.
CALCED	Numero de cedula del postulante.
CALSEX	Sexo del postulante.
CALANO	Año de nacimiento del postulante.
CALOCU	Ocupación del postulante.
CALAPC	Apellido paterno del conyuge.
CALAMC	Apellido materno del conyuge
CALNOC	Nombres del conyuge.
CALCEC	Cedula del conyuge.
CALANIO	Año de nacimiento del conyuge.
CALINT	Valor de ingresos familiares.
CALCVP	Provincia en donde aplicara la postulacion.
CALCVC	Canton en donde aplicara la postulacion.
CALPRR	Parroquia en donde aplicara la postulacion.
INCENT	Valor neto del bono asignado.
PRECIO	Valor total del incentivo.
MATERIAL	Aporte en dólares del postulante.
AREA	Area del terreno en donde se aplicara el bono.
CALEMRG	Valida si el proyecto es emergente.
DSTRCMNT	Calificacion 1 del proyecto emergente.
DSTRMMPS	Calificacion 2 del proyecto emergente.
DSTRPRTA	Calificacion 3 del proyecto emergente.
DSTRVNTN	Calificacion 4 del proyecto emergente.
DSTRTCHO	Calificacion 5 del proyecto emergente.
DSTROTRS	Calificacion 6 del proyecto emergente.
PUNTOPOS	Puntos para postulaciones del postulante.
PUNTOPOS1	Puntos para postulaciones 1 del postulante.
PUNTOPOS2	Puntos para postulaciones 2 del postulante.
PUNTOCON	Puntos para postulaciones del conyuge.
PUNTOCON1	Puntos para postulaciones 1 del conyuge.
PUNTOHIJ	Puntos para postulaciones para los hijos.
PUNTOHIJ1	Puntos para postulaciones 1 para los hijos.
PUNTOPAD	Puntos para los padres adultos.
PUNTOPAD1	Puntos 1 para los padres adultos.
PUNTOANC	Puntos para los ancianos.
PUNTOANC1	Puntos 1 para los ancianos.
PUNTOSFAM	Puntos para la familia.
PUNTONGRFA	Puntos para el grupo familiar 1.
PUNTOGRUFA	Puntos para el grupo familiar 2.
PUNTOSPRO	Puntos del proyecto.
IMPDMTO	Detalles de impedimentos.
IMPDMTO1	Detalle 1 de impedimentos.
IMPNUE	Impedimento para bonos emergentes.
RETIRA	Detalle de retiro de postulación.
CALIFICAPR	Calificacion del proyecto.
CALIFICA	Calificacion del postulante.
CALIFIDOCODIGO	Código identificador para el CALIFIDO.
UBSTENX	Coordenada X en formato WGS84.
UBSTENY	Coordenada Y en formato WGS84.
ZONA	Zona en referencia al meridiano de Greenwich.
ESTADOFINAL	Estado de la postulación.
CE	Código de etnia.
ETNIA	Detalle de Etnia
CT	Código para la tenencia del terreno.
TENENCIATERRENO	Detalle de la tenencia del terreno.
FECHACARGA	Fecha en la que se realiza al carga de datos.
HORACARGA	Hora en la que se realiza la carga de datos.
CODCARGA	Código generado para la carda de datos.
VALIDADO	Condicionante para validar la carda de datos.

TABLA TBREGION	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_REGION_COD	Código de la región.
C_REGION_DETALLE	Región codificada por SENPLADES.

TABLA TBPROVINCIA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_PROVINCIA_ID	Código de la provincia.
C_PROVINCIA_NOMBRE	Nombre de la provincia.

TABLA TBCANTON	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_CANTON_ID	Código del canton
C_CANTON_COD	Id del canton segun la provincia.
C_CANTON_NOMBRE	Nombre del canton.

TABLA TBPARROQUIA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_PARROQUIA_ID	Código de parroquia.
C_PARROQUIA_COD	Id de parroquias según los cantones
C_PARROQUIA_NOMBRE	Nombre de la parroquia.
C_PARROQUIA_DETALLE	Cabecera cantonal de la parroquia.

TABLA TBREGIONNATURAL	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_REGIONNAT_COD	Código de región natural.
C_REGIONNAT_DETALLE	Detalle de la región natural.

TABLA TBZONA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_ZONA_COD	Cód zona o sector de aplicación.
C_ZONA_DETALLE	Nombre de la zona de aplicación

TABLA TBTIPOSOLUCION	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_TIPOSOL_COD	Código del tipo de solución.
C_TIPOSOL_DETALLE	Nombre del tipo de solución.

TABLA TBGENERO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_GENERO_COD	Código para el sexo o genero.
C_GENERO_DETALLE	Nombres para los tipos de sexo.

TABLA TBECIVIL	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_ECIVIL_COD	Código para tipos de estado civil.
C_ECIVIL_DETALLE	Detalle del estado civil.

TABLA TBTRANSACCION	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_TRANSACCION_COD	Código de la transacción.
C_TRANSACCION_FECHA	Fecha de realizacion transacción.
C_TRANSACCION_HORA	Hora realización la transacción.
C_TRANSACCION_NUMO	Número de oficio de transacción.
C_TRANSACCION_FECHA	Fecha del oficio de transacción.
C_TRANSACCION_IP	Ip la cual ejecuta la transacción.
C_TRANSACCION_HOST	Nombre de host que ejecuta.
C_TRANSACCION_OBSER	Observación de la transacción.
C_TRANSACCION_ESTAD	Estado antiguo de la transacción.
C_TRANSACCION_ESTAD	Estado nuevo de la transacción.
C_TRANSACCION_FECHA	Fecha del servidor de transacción.
C_TRANSACCION_PROYE	Proyecto afectado en transacción.

TABLA TBUSUARIO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_USUARIO_COD	Código de usuario registrado.
C_USUARIO_CEDULA	Cédula del usuario registrado.
C_USUARIO_NOMBRES	Nombres del usuario registrado.
C_USUARIO_APELLIDOS	Apellidos del usuario registrado.
C_USUARIO_FECHANAC	Fecha de nacimiento del usuario
C_USUARIO_MAIL	Correo electrónico del usuario
C_USUARIO_USER	Nombre de usuario de acceso
C_USUARIO_PASS	Contraseña del usuario de acceso
C_USUARIO_PERFIL	Perfil de usuario.
C_USUARIO_ESTADO	Estado del usuario.

TABLA TBPROYECTO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_PROYECTO_COD	Código único del proyecto de vivienda.
C_PROYECTO_NOMBRE	Nombre del proyecto de vivienda.
C_PROYECTO_FECHAING	Fecha de ingreso del proyecto de vivienda.
C_PROYECTO_CALIFIDOCOD	Código califido del proyecto de vivienda.
C_PROYECTO_ESTADO	Estado del proyecto de vivienda
C_PROYECTO_PARROQUIA	Parroquia situado el proyecto de vivienda.
C_PROYECTO_CANTON	Canton situado el proyecto de vivienda.
C_PROYECTO_PROVINCIA	Provincia situado el proyecto de vivienda.
C_PROYECTO_VALOR	Valor en dólares del proyecto de vivienda.
C_PROYECTO_VALORAPORTE	Valor en dólares del aporte familiar.
C_PROYECTO_NUMSOL	Número de soluciones del proyecto.
C_PROYECTO_CODIGOCARGA	Código de carga del proyecto de vivienda.
C_PROYECTO_FECHAREALFIN	Fecha real de fin del proyecto de vivienda.
C_PROYECTO_ACTAP	Fecha de registro de acta provisional.
C_PROYECTO_ACTAD	Fecha de registro de acta definitiva.
C_PROYECTO_FECHAREALINICIO	Fecha real de inicio de obra.
C_PROYECTO_AVANCEOBRA	Fecha de visita para avance de obra.

TABLA TBPERSONA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_PERSONA_CEDULA	Cedula de persona.
C_PERSONA_APELLIDOP	Apellido paterno de la persona.
C_PERSONA_APELLIDOM	Apellido materno de la persona.
C_PERSONA_NOMBRES	Nombres de la persona.
C_PERSONA_FECHANAC	Fecha de nacimiento de la persona.
C_PERSONA_TELEFONO	Número de teléfono de la persona.
C_PERSONA_MAIL	Mail de la persona.
C_PERSONA_DIRECCION	Dirección domiciliaria de la persona.
C_PERSONA_OCUPACION	Ocupación de la persona.
C_PERSONA_LTRABAJO	Lugar de trabajo de la persona.
C_PERSONA_EMPRESA	Empresa si trabaja la persona.
C_PERSONA_TTRABAJO	Tiempo de trabajo en la empresa actual.
C_PERSONA_FONOTRABAJO	Número de telefono del trabajo.

TABLA TBCONYUGE	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_CONYUGE_CEDULA	Cédula del conyuge.
C_CONYUGE_APELLIDOP	Apellido paterno del conyuge.
C_CONYUGE_APELLIDOM	Apellido materno del conyuge.
C_CONYUGE_NOMBRES	Nombres del conyuge.
C_CONYUGE_FECHANAC	Fecha de nacimiento del conyuge.
C_CONYUGE_OCUPACION	Ocupación del conyuge.
C_CONYUGE_LTRABAJO	Lugar de trabajo del conyuge.
C_CONYUGE_TELEFONO	Número de telefono del conyuge.
C_CONYUGE_INGRESOS	Ingreso del conyuge.

TABLA TBNACIONAL	
NOMBRE DEL CAMPO	**DESCRIPCION**
NOMPOSTU	Nombre del beneficiario en base histórica
CEDPOSTU	Cédula del beneficiario en histórica
NOMCONYU	Nombre del conyuge en la tabla histórica.
CEDCONYU	Cédula del conyuge en la tabla histórica.
PROVINCIA	Nombre de la provincia.
CANTON	Nombre del canton.
PROYECTO	Nombre del proyecto de vivienda.

TABLA TBCALIFICACION	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_CALIFICACION_COD	Código para la calificación de postulantes.
C_CALIFICACION_PUNTAJE	Puntaje total de la calificación.
C_CALIFICACION_APORTE	Aporte total del grupo familiar.
C_CALIFICACION_INGRESO	Ingresos familiares del nucleo.
C_CALIFICACION_VALORBONO	Valor en dólares del bono de vivienda.
C_CALIFICACION_AREAT	Area del terreno donde se contruye.
C_CALIFICACION_CALIFICA	Condicionante para saber si califica o no.
C_CALIFICACION_C_POSX	Coordenada en X, en formato WGS84.
C_CALIFICACION_C_POSY	Coordenada en Y, en formato WGS84.
C_CALIFICACION_C_POSZ	Coordenada en Z, en formato WGS84.
C_CALIFICACION_C_ALTURA	Altura del nivel del mar del proyecto.
C_CALIFICACION_C_ZONA	Zona segun los usos horarios del proyecto.
C_CALIFICACION_AVANCEOBRA	Porcentaje de avance de obra de cada casa.
C_CALIFICACION_ACTAPROVISIONAL	Actas provisionales para los proyectos.
C_CALIFICACION_ACTADIFINITIVA	Actas definitiva para los proyectos.

TABLA TBFISCALIZADOR	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_FISCALIZADOR_CEDULA	Número de cédula del fiscalizador.
C_FISCALIZADOR_NOMBRES	Nombres del fiscalizador.
C_FISCALIZADOR_APELLIDOS	Apellidos del fiscalizador.
C_FISCALIZADOR_TELEFONO	Número de teléfono del fiscalizador.
C_FISCALIZADOR_MAIL	Dirección de mail del fiscalizador.
C_FISCALIZADOR_DIRECCION	Dirección del fiscalizador.
C_FISCALIZADOR_COMPANIA	Compañia que pertenece el fiscalizador.
C_FISCALIZADOR_REPRESENTANTE	Nombre del representante del fiscalizador.
C_FISCALIZADOR_PROVINCIA	Alcance de provincia del fiscalizador.
C_FISCALIZADOR_ESTADO	Estado del fiscalizador.

TABLA TBCONSTRUCTOR	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_CONSTRUCTOR_CEDULA	Número de cédula del constructor.
C_CONSTRUCTOR_NOMBRES	Nombres del constructor.
C_CONSTRUCTOR_APELLIDOS	Apellidos del constructor.
C_CONSTRUCTOR_TELEFONO	Número de teléfono del contructor.
C_CONSTRUCTOR_MAIL	Mail del contructor.
C_CONSTRUCTOR_DIRECCION	Dirección de la empresa del contructor.
C_CONSTRUCTOR_PROVINCIA	Provincia que ejerce oficio el constructor.
C_CONSTRUCTOR_ESTADO	Estado del constructor.
C_CONSTRUCTOR_NUMOBRAS	Número de obras sin terminar.
C_CONSTRUCTOR_COMPANIA	Compañia al que pertencece el constructor.
C_CONSTRUCTOR_REPRESENTAN	Representante al que pertence el constructor

TABLA TBCONTRATO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_CONTRATO_COD	Código de contrado.
C_CONTRATO_FECHAFIRMA	Fecha de la firma del contrato.
C_CONTRATO_MONTO	Monto del contrato.
C_CONTRATO_PLAZO	Plazo de vigencia del contrato.
C_CONTRATO_NUM	Número de contrato.
C_CONTRATO_FECHAANTICIPO	Fecha de anticipo del contrato.
C_CONTRATO_FECHATERMINO	Fecha de termino del contrato.
C_CONTRATO_FECHADEFINITIVA	Fecha definitva del contrato.
C_CONTRATO_INCOP	Número del incop en el contrato.
C_CONTRATO_APORTEBENEFICIA	Aporte de beneficiaio del contrato.

TABLA TBPOLIZA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_POLIZA_COD	Código de póliza.
C_POLIZA_FECHAINICIO	Fecha de inicio que consta en la póliza.
C_POLIZA_DIAS	Número de días de vigencia de la póliza.
C_POLIZA_NUMRENOVACION	Número de renovaciónes de la póliza.
C_POLIZA_PORCENTAJE	Porcentaje de la póliza.
C_POLIZA_PLANILLA	Valor de la planilla de póliza.
C_POLIZA_SALDO	Saldo restante de la póliza.
C_POLIZA_NUM	Número de póliza.
C_POLIZA_MONTO	Monto en dólares que se emite la póliza.
C_POLIZA_FECHAFIN	Fecha de fin que consta en la póliza.

TABLA TBPAGO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_PAGO_COD	Código para el pago del proyecto.
C_PAGO_FECHA	Fecha de registro de pago.
C_PAGO_MONTO	Valor en dólares del monto de pago.
C_PAGO_HORA	Hora de registro de pago.
C_PAGO_CUR	Número de CUR o comprobante de pago.

TABLA TBAVANCEOBRA	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_AVANCEOBRA_COD	Código de avance de obra del proyecto.
C_AVANCEOBRA_FECHAVISITA	Fecha de la visita de avance de obra.
C_AVANCEOBRA_PORCENTAJE	Valor porcentual de avance de obra.

TABLA TBEMITIDO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_EMITIDO_COD	Código de proyecto emitido.
C_EMITIDO_FECHA	Fecha de emisiónd de proyecto
C_EMITIDO_HORA	Hora de emisión de proyecto.
C_EMITIDO_MONTO	Monto de emesión de proyecto.

TABLA TBADJUDICADO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_ADJUDICADO_COD	Código para proyecto adjudicado.
C_ADJUDICADO_FECHA	Fecha de adjudicación del proyecto.
C_ADJUDICADO_HORA	Hora de adjudicación del proyecto.
C_ADJUDICADO_MONTO	Monto en dólares de adjudicación.

TABLA TBANULADO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_ANULADO_COD	Código de anulaciones.
C_ANULADO_RAZON	Causa de anulación del registro.
C_ANULADO_OBSERVACION	Observación de la anulación.

TABLA TBDUPLICADO	
NOMBRE DEL CAMPO	**DESCRIPCION**
C_DUPLICADO_COD	Código para las postulaciones duplicadas.
C_DUPLICADO_PROYECTO	Registro de poryectos duplicados.
C_DUPLICADO_FECHAINGRESO	Fecha de inserción del registro duplicado.
C_DUPLICADO_HORAINGRESO	Hora de inserción del registro duplicado.

Figura 6.80: Diccionario de Datos (b).
Fuente: Autor de Tesis.

DISEÑO DE LA BASE DE DATOS

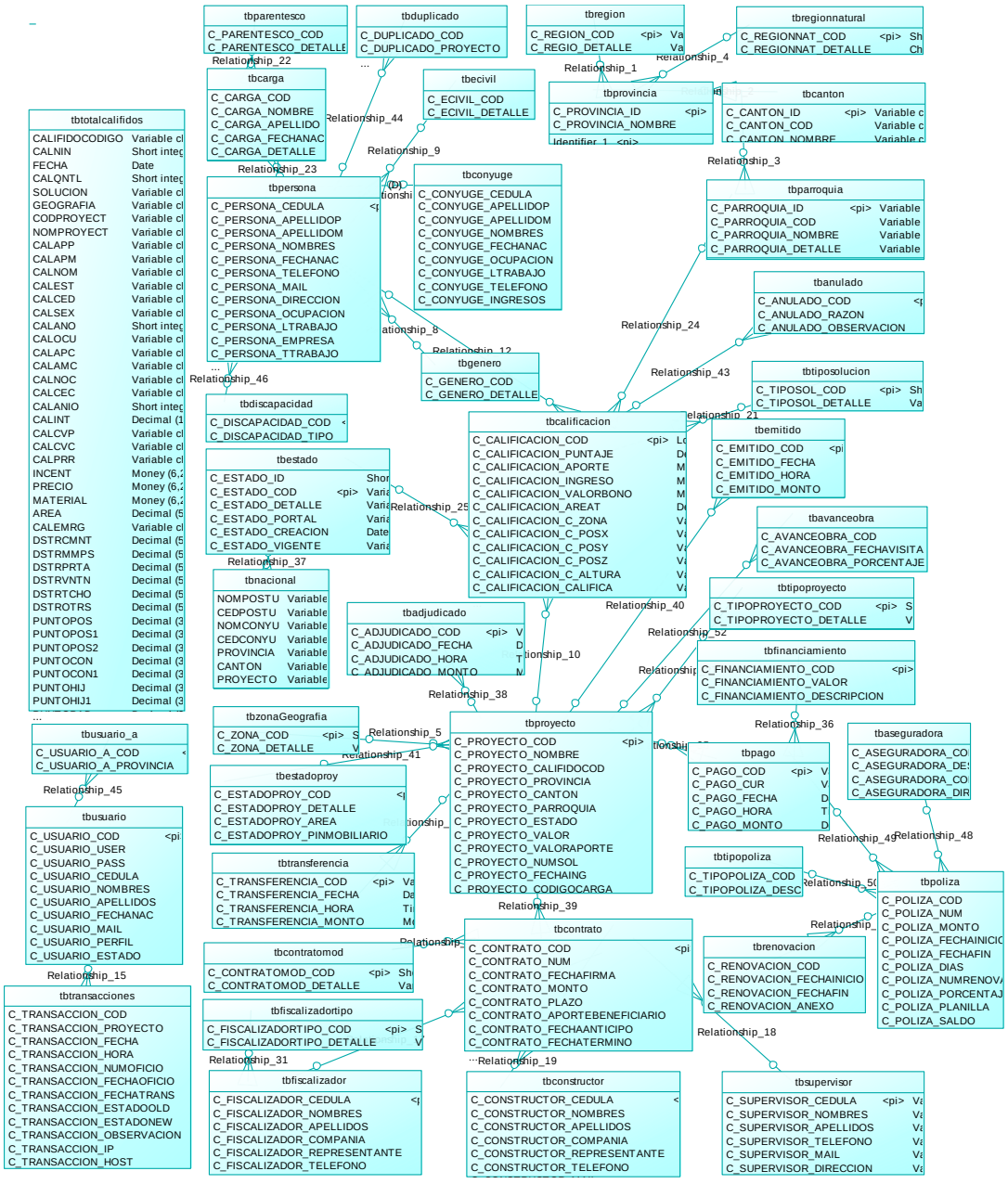


Figura 6.81: Diagrama entidad relación de la base de datos general del modulo de control.
Fuente: Autor de tesis.

Toda esta investigación se realizó pensando siempre en mejorar los procesos que maneja la institución para brindar un mejor servicio a la gente más necesitada. El MIDUVI estará siempre listo y con la mejor predisposición para brindar un servicio de calidad, con la ayuda de nuevas aplicaciones y los avances tecnológicos se pensará en un país más transparente y servicial.

CONCLUSIONES

La fuente o recurso más importante que maneja y gestiona cualquier organización, empresa o institución es la INFORMACIÓN, la cual debe ser protegida, custodiada, monitorizada, respaldada y asegurada en todos los ámbitos, frente a cualquier desastre o daño que pueda poner en riesgo la integridad de este recurso.

El desarrollo e implementación de las aplicaciones web propuestas en este proyecto, permitirá al personal técnico de la institución, un mejor control y administración de la información de los proyectos e incentivos de vivienda que otorga el MIDUVI a los ecuatorianos más necesitados.

El Ministerio de Desarrollo Urbano y Vivienda ofrece a las personas ecuatorianas la posibilidad de ingresar al portal web desde cualquier parte del mundo, para consultar si puede postular y participar del incentivo de vivienda, mediante una interfaz amigable, rápida y confiable.

La información sobre la gestión y control de bonos de vivienda que se encuentra alojada en los servidores del MIDUVI, presenta problemas de seguridad a nivel físico y lógico. El presente proyecto presenta las mejores soluciones que solventarán los principales problemas, y de esta forma evitar los riesgos y amenazas que ponen en peligro la información existente en la institución.

El desarrollo de las interfaces utilizando software libre, permitió un mayor acoplamiento a las diferentes tecnologías de información que existen en la actualidad. El gestor de base de datos MySQL y la utilización del lenguaje PHP, permitió implementar los diferentes módulos de consulta y control de los proyectos de vivienda.

El resultado final del presente proyecto se refleja positivamente en las tareas y procedimientos que permitieron incrementar la seguridad y mejoraron la gestión de la información en el Ministerio de Desarrollo Urbano y Vivienda.

RECOMENDACIONES

La implementación de la Virtualización de sistemas, sería una alternativa efectiva para mejorar el rendimiento, productividad y seguridad de equipos que trabajan con información importante y confidencial para la institución.

Planificar talleres de capacitación para socializar primero a las autoridades y luego al resto de personal de la institución sobre las diferentes alternativas en el desarrollo del plan de seguridad y procesamiento de información que se plantea, y de esta manera poder continuar con la ejecución del proceso.

Gestionar la aplicación y aceptación de convenios interinstitucionales para acceder mediante Web Service a las bases de datos del Registro Social y Registro Civil que ayudarán enormemente para la validación de datos y corrección de errores en línea.

Desarrollar planes estratégicos para la utilización de herramientas con software libre, ya que reduce costos, no necesitan licencias, es de libre distribución y lo más importante posee un grado alto de seguridad en todos los aspectos al manejar formatos estándar socializados a nivel mundial, se logra formar una comunidad que colabora para desarrollar sistemas mucho más estables.

Contar con la infraestructura adecuada en cuanto al hardware, equipos, servidores, etc., que brinden y garanticen un entorno de seguridad general, primero al recurso humano y luego a la información así como al espacio físico.

Preparar y planificar capacitaciones en diferentes áreas como, redes informáticas, seguridad de datos, gestión de bases de datos, configuración de servidores, etc., para que el personal técnico esté en la capacidad de solucionar la mayor cantidad de problemas tecnológicos sin tener que recurrir a empresas externas que brinden el servicio.

BIBLIOGRAFÍA

LIBROS

- **Autor**: BOTT, Ed.; Siechert, Carl

  Título: Guía completa de seguridad en Microsoft Windows.

  Madrid: MC Graw – Hill, 2003, 608p

- **Autor**: TOM ADELSTEIN, BILL LUBANOVIC; Ed Anaya

  Título: Administración de sistemas Linux.

  O'RELLY – 2007. 336p.

DOCUMENTOS PDF

- La información confidencial, Concepto y sugerencias para su adecuado manejo y administración.
- ANOMINO, Linux Máxima Seguridad, Editorial PRENTICE HALL.
- BILL VON HAGEN – BRIAN K JONES, Linux server los mejores trucos - 2006

REFERENCIAS WEB

- http://lifestyle.iloveindia.com/lounge/importance-of-information-technology-8087.html
- http://www.matem.unam.mx/~rajsbaum/cursos/web/resumen_seguridad_1.pdf
- http://www.virusportal.com/es/formacion/train_dat3.shtml
- http://www.cafeonline.com.mx/virus/tipos-virus.html
- http://www.segu-info.com.ar/articulos/4-backup-bastion-caido-seguridad.htm
- http://www.rediris.es/cert/doc/unixsec/node7.html

- http://www.une.com.co/Uploads/RelacionesExt/seguridad/ELEMENTOS%20DE%20SEGURIDAD-CRT-Enero%204%202007.htm
- http://www.maestrosdelweb.com/editorial/historia-y-evolucion-del-sistema-operativo-mac-os/
- http://foro.elhacker.net/windows/historia_completa_de_windows_y_sus_versionesby_burnhack-t202558.0.html
- http://securitysad.blogspot.com/
- http://www.juanfelipe.net/node/26
- http://www.kriptopolis.org/backtrack
- http://www.informatizando.es/?p=135
- http://forums.remote-exploit.org/guias-y-tutoriales/31398-arrancar-la-red-en-backtrack-4-a.html
- http://sectools.org/tools2.html
- http://www.mitecnologico.com/Main/EstandaresParaElManejoDeDatosEInformacion
- http://slony.blogspot.com/2007/03/instalacin-de-slony-i-en-windows-xp.html
- http://hadi-en.search4buy.com/2009/12/slony-i-configuration-in-windows-xp.html
- http://www.maestrosdelweb.com/editorial/snort/
- http://bulma.net/body.phtml?nIdNoticia=2083
- http://www.proyectofedora.org/wiki/Detector_de_intrusos_en_la_red_psad
- http://www.alcancelibre.org/staticpages/index.php/como-saned/print
- http://www.linuxtotal.com.mx/index.php?cont=info_admon_006
- www.slideshare.net
- http://www.how-to-linux.com/2008/12/install-snort-and-base-on-centos-52/

Anexos

ANEXO A

GLOSARIO

APACHE: Servidor de distribución libre y de código abierto, su potencialidad y flexibilidad es muy alta, ya que puede funcionar en una amplia variedad de plataformas y entornos.

BASES DE DATOS: Conjunto de información, ya sea datos o registros pertenecientes a un mismo contexto, almacenados en algún medio para su acceso y manipulación de los mismos.

BONOS DE VIVIENDA: Incentivo en dólares entregado por el MIDUVI, para la realización de viviendas ya sea de tipo nueva, mejoramiento o terminación.

DBA: Administrador de la base de datos, responsable de la integridad, seguridad, recuperabilidad y disponibilidad de la información.

DDP: Protocolo de entrega de datagramas mediante sockets sobre redes AppleTalk.

DPA: División Política Administrativa regulada por el Instituto Nacional de Estadísticas y Censos, sirve para identificar y codificar la ubicación de un sitio según la provincia, cantón y parroquia.

ETHERNET: Estándar de redes de computadoras de área local, define las características del cableado, señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

GNU/LINUX: Combinación del núcleo o kernel libre similar a Unix denominado Linux, con las herramientas y utilidades del proyecto GNU para formar y desarrollar un sistema operativo completo, robusto y disponible libremente, con la idea de software libre.

IDS: Sistema de detección de intrusos utilizado principalmente para detectar accesos no autorizados

IP: Protocolo de internet, es el principal protocolo de comunicaciones utilizado para transmitir datagramas a través de una interconexión de redes.

IPX: Intercambio de paquetes entre redes, es un protocolo de datagramas rápido orientado a conexiones sin conexión.

ISP: Proveedor de Servicios de Internet.

MIDUVI: Ministerio de Desarrollo Urbano y Vivienda.

MYSQL: Sistema de gestión de bases de datos relacional, multihilo y multiusuario desarrollado como software libre compatible con múltiples sistemas.

NESSUS: Herramienta de escaneo de vulnerabilidades en varios sistemas operativos. Una de las funcionalidades es que posee programación de tareas.

NetBEUI: Interfaz extendida del usuario de Net Bios, es un protocolo a nivel de red bastante sencillo utilizado como una de las capas en las primeras redes de Microsoft. Desarrollado por IBM.

NetBios: Sistema básico de entrada /salida de red, es una interfaz para el acceso a servicios de red. Sirve para enlazar un sistema de red con hardware específico.

NETCAT: Herramienta de red que permite a través del intérprete de comandos abrir o cerrar puertos TCP / UDP.

NIS: Sistema de información de red, nombre de un protocolo de servicios de directorios para el envío de datos de configuración en sistemas distribuidos.

NMAP: Programa de código abierto que sirve para efectuar rastreo de puertos.

PHP: Lenguaje de programación interpretado del lado del servidor, diseñado para el desarrollo de páginas web dinámicas.

PROYECTOS DE VIVIENDA: Conjunto de postulaciones conformadas por un grupo de personas que desean participar y obtener el incentivo que otorga el MIDUVI, cumpliendo los requisitos estipulados en los reglamentos.

RS: Registro Social, conforma el Ministerio de Coordinación y Desarrollo Social

SCANNERS: Herramientas de seguridad que poseen la capacidad de detectar los puntos vulnerable de una red de información.

SISTEMA INFORMÁTICO: Conjunto de partes interrelacionadas con hardware, software y recurso. Generalmente el sistema informático engloba computadoras que gestionan y procesan información.

SNIFFERS: Programa de captura de tramas de red. Monitorea y analiza el tráfico de una red.

SPOOFING: Es la creación de tramas TCP / IP, utilizando una IP falseada. En otras palabras son técnicas de suplantación de identidad para fines maliciosos.

TCP/IP: Conjunto de protocolos de red más importantes en redes de información, es la base del internet. Se compone del Protocolo de Control de Transmisión y Protocolo de Internet.

TI: Tecnologías de Información.

UID: Identificador de usuario, generalmente un numero positivo que lo genera el sistema operativo.

UNIX: Sistema operativo portable, multitarea y multiusuario desarrollado en 1969 por AT&T.

WINDOWS: Nombre de una serie de sistemas operativos desarrollados por Microsoft, iniciado y comercializado, en respuesta al creciente interés del mercado de una interfaz gráfica de usuario. En el año 2009 fue el más popular y utilizado por todo el mundo.

ANEXO B

ANÁLISIS DE REQUERIMIENTOS PARA EL DESARROLLO DE LAS APLICACIONES

ANALISIS DE REQUERIMIENTOS.

El Ministerio de Desarrollo Urbano y Vivienda, es el Organismo del Estado Ecuatoriano que controla, coordina y aprueba las solicitudes del bono o incentivo de vivienda, para las personas que cumplan con requisitos preestablecidos en los reglamentos elaborados para tal efecto.

El MIDUVI, requiere de una solución web de consulta rápida y confiable sobre los incentivos de vivienda que esta cartera de Estado otorga, dirigida a las personas ecuatorianas que desean saber si son potenciales postulantes al bono de vivienda.

El MIDUVI, requiere de una solución web para el control y seguimiento de los proyectos de vivienda que se entregan por parte de la institución, dirigido a los empleados técnicos encargados de la gestión de proyectos habitacionales.

Requerimiento General

Automatizar el proceso de consulta de bonos de vivienda para las personas que solicitan el incentivo.

Automatizar el proceso de control y seguimiento de proyectos de vivienda para los técnicos del MIDUVI, que están a carga de este proceso.

Requerimientos Específicos

- **Requerimientos para la Interfaz de consulta de bono de vivienda**

La interfaz web a realizarse debe permitir realizar lo siguiente:

Consultar de la base de datos que posee el MIDUVI, a las personas que ya han recibido un incentivo de vivienda, mostrando la ubicación en donde la recibieron.

Presentar una interfaz amigable al usuario

Presentar una interfaz confiable que presente los resultados en el menor tiempo posible.

Controlar y verificar la validez de la cédula de ciudadanía que ingresa el usuario.

Presentar resultados confiables y de fuentes veraces para que los usuarios puedan asegurar que la información mostrada es real.

- **Requerimientos para la Interfaz de accesibilidad al bono de vivienda.**

Consultar de la base de datos del Registro Social, para obtener el puntaje socioeconómico de cada persona que ingrese a la aplicación y de esta manera pueda conocer si es potencial postulante al bono de vivienda.

La interfaz web a realizarse debe permitir realizar lo siguiente:

Presentar una interfaz amigable al usuario

Desarrollar una interfaz confiable que presente los resultados en el menor tiempo posible.

Controlar y verificar la validez de la cédula de ciudadanía que ingresa el usuario.

Implementar dos opciones de consulta, tanto para el sector Urbano como para el sector Rural.

Para el sector Urbano la aplicación debe permitir escoger el tipo de vivienda entre: Construcción de vivienda, Adquisición y Mejoramiento.

- **Requerimientos para el Módulo de Control y Seguimiento**

Desarrollar una aplicación web que permita a los empleados técnicos encargados de los proyectos de vivienda del sector Rural y Urbano Marginal, registrar, controlar y gestionar el seguimiento de los mismos.

El modulo debe estar estructurado a partir de la base relacional única que utiliza el MIDUVI para las postulaciones y calificaciones de personas que acceden al bono de vivienda.

Se debe incorporar el concepto de proyecto de vivienda, como la agrupación de personas relacionados por un código de proyecto el cual se lo tomará como referencia para los reportes que requieren las autoridades.

Implementar una interface web para el registro de anulaciones y devoluciones de bonos de vivienda.

Implementar interfaces web que permita a los funcionarios de la Matriz del MIDUVI revisar y aprobar el bono de vivienda.

Implementar interfaces web que permita a los funcionarios de las 24 Unidades Técnicas Provinciales del MIDUVI gestionar el proceso del bono en las siguientes etapas:

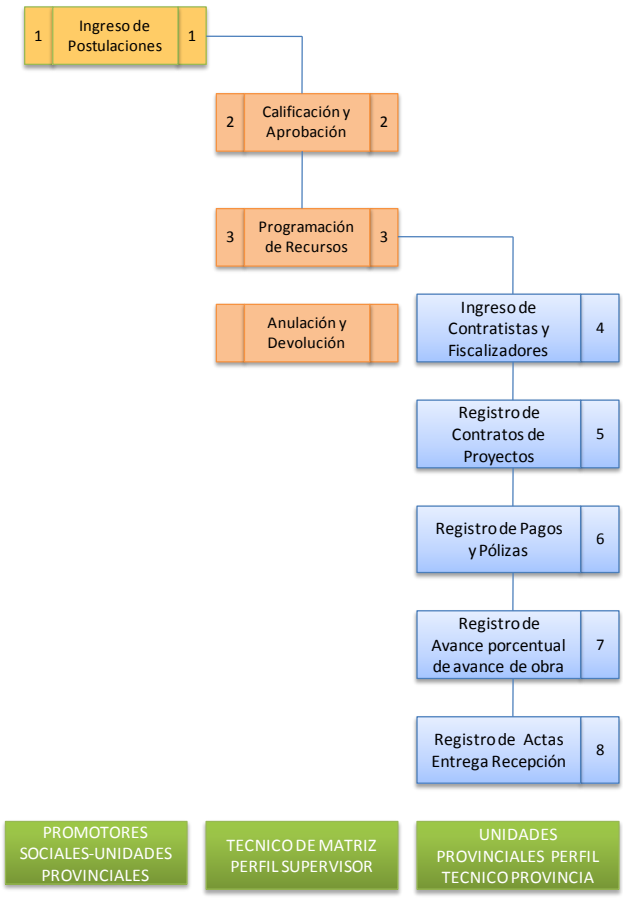
1. Ingreso de Contratistas y Fiscalizadores
2. Registro de Contratos de Proyectos
3. Registro de Pólizas y Pagos.
4. Registro de Avance porcentual de la Obra
5. Registro de Actas Entrega Recepción

ANEXO C

MANUAL DE USUARIO PARA EL MÓDULO DE CONTROL Y SEGUIMIENTO DE PROYECTOS DE VIVIENDA RURAL – URBANO MARGINAL.

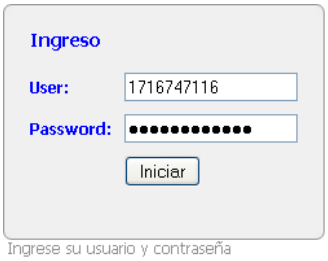
MÓDULO DE CONTROL Y SEGUIMIENTO DE PROYECTOS DE VIVIENDA

El módulo de control y seguimiento de proyectos de vivienda que se desarrolló, cuenta con 2 perfiles de usuarios: uno para el técnico de Matriz y otro para el técnico de la Unidad Provincial del MIDUVI.



Como se pudo apreciar en la anterior figura, el módulo de control y seguimiento inicia con la información ingresada por parte de los promotores sociales de las unidades provinciales del MIDUVI. La columna de color naranja muestra las opciones que están habilitadas para el perfil del supervisor y la columna de color celeste son las opciones que posee el perfil del técnico de provincia para el modulo de control de proyectos de vivienda.

PERFIL SUPERVISOR - INICIO DE SESIÓN



El inicio de sesión para el perfil supervisor se la realiza ingresando un nombre de usuario asignado y una contraseña que se define por el administrador.

Posteriormente, el usuario registrado podrá cambiar la contraseña a una más personalizada, si así lo desea.

El perfil del técnico de matriz o PERFIL DEL SUPERVISOR, permite visualizar los proyectos de vivienda que han sido ingresados previamente en las unidades técnicas provinciales y se encuentran en estado PRECALIFICADO.

MENÚ DE OPCIONES PARA EL PERFIL SUPERVISOR

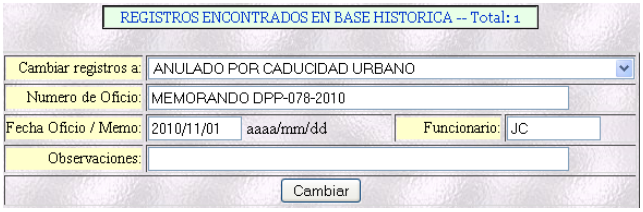
Anulación-Devolución

Esta acción la puede ejecutar el técnico supervisor que trabaja en la matriz del MIDUVI, para anular y devolver bonos.

Buscar registros para anularlos en la opción Anulación – Devolución.

Buscar: Este botón permite realizar la búsqueda mediante 2 parámetros.
Por número de cédula o por nombre.

Anular registros seleccionado en la opción Anulación – Devolución.



Cambiar: Luego de encontrar al menos un registro, este botón permite registrar la anulación o devolución.

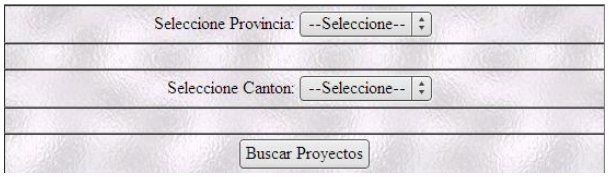
La interfaz que se presenta en la siguiente figura, muestra la búsqueda por cédula o por nombre, si el resultado devuelve un registro se puede realizar la acción requerida. Se completan los campos necesarios y se presiona el botón “cambiar”, completando el proceso.

Calificación – Aprobación.

Visualización de postulaciones ingresadas.

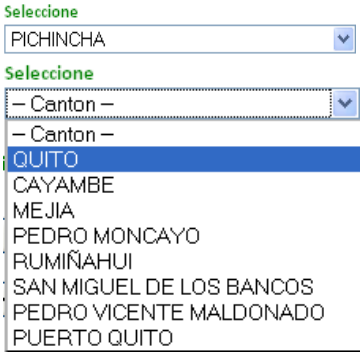
La siguiente opción permite visualizar la interfaz del supervisor y se refiere a la Calificación – Aprobación de los proyectos de vivienda.

Búsqueda de proyectos que van a ser calificados y aprobados.



Buscar Proyectos: Este botón permite realizar la búsqueda de proyectos por provincia y cantón.

Consultar proyectos de un cantón en específico.



Existen 2 combo box dinámicos que permiten la selección de los cantones según la provincia escogida.

En la figura se muestra la selección de los cantones de la provincia de Pichincha, que fue escogida en el primer combo box.

Consultar proyectos de una provincia en general.

Para realizar la búsqueda de proyectos en una determinada provincia en la cual agrupe a todos los cantones respectivos, se debe escoger únicamente en el primer combo box y el segundo combo box debe permanecer sin selección, como se muestra en la figura.

Aprobación de proyectos identificados y seleccionados.

De aquí en adelante se maneja el criterio de "**PROYECTO**", que será la reunión de personas que van a construir sus viviendas. El proyecto puede comprender entre 25 y 50 soluciones o beneficiarios.

En esta interfaz se debe registrar los siguientes datos:

Fecha Aprobación: Es la fecha en la cual las autoridades dan el visto bueno para la calificación - aprobación del proyecto.

Fecha Oficio: La fecha del documento habilitante de aprobación del proyecto.

N° Oficio: Es el número de oficio con el cual se procede al pedido.

Como se muestra en la siguiente figura, el procedimiento para aprobar un proyecto es buscarlo, seleccionarlo y luego completar los campos adicionales, para finalmente dar clic en el botón "Emitir Proyecto(s)".

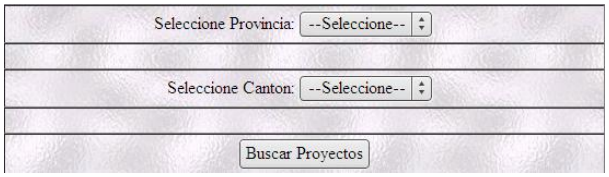
Esta aplicación valida que el usuario seleccione por lo menos un registro o proyecto de vivienda para ejecutar la acción. Luego de la aprobación del proyecto ya no se podrá revertir el proceso.

Emisión – Programación de Recursos.

Visualización de proyectos aprobados.

En esta opción se podrá visualizar los registros de proyectos que fueron previamente calificados – aprobados en el paso anteriormente revisado.

Búsqueda de proyectos van a ser emitidos – asignado presupuesto.



Buscar Proyectos: Este botón permite realizar la búsqueda de proyectos por provincia y cantón.

Esta opción funciona exactamente igual a la interfaz de aprobación de proyectos. Se puede seleccionar proyectos por provincia y por cantón.

Emisión y asignación presupuestaria de los proyectos seleccionados.

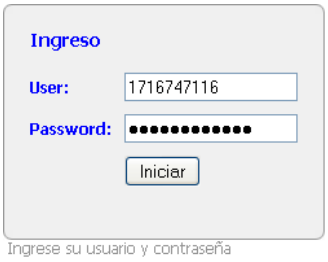
Como se muestra en la siguiente figura, esta opción permite al supervisor registrar la emisión de uno o varios proyectos. Se debe registrar los siguientes datos.

Fecha Asignación: Es la fecha en la cual las autoridades dan el visto bueno para la emisión – asignación presupuestaria de proyecto.

Fecha Memo: La fecha del documento habilitante de emisión del proyecto.

N° Memo: Es el número de memorando con el cual se procede al pedido.

PERFIL TÉCNICO PROVINCIA - INICIO DE SESIÓN



El inicio de sesión para el perfil técnico de provincia se la realiza ingresando un nombre de usuario asignado y una contraseña que se define por el administrador.

Posteriormente, el usuario registrado podrá cambiar la contraseña a una más personalizada, si así lo desea.

El perfil del técnico provincial o PERFIL TÉCNICO, permite a los promotores sociales, personal técnico de obra, personal financiero, contratistas y fiscalizadores llevar un control en el seguimiento de los proyectos de vivienda que hayan sido emitidos y con asignación presupuestaria.

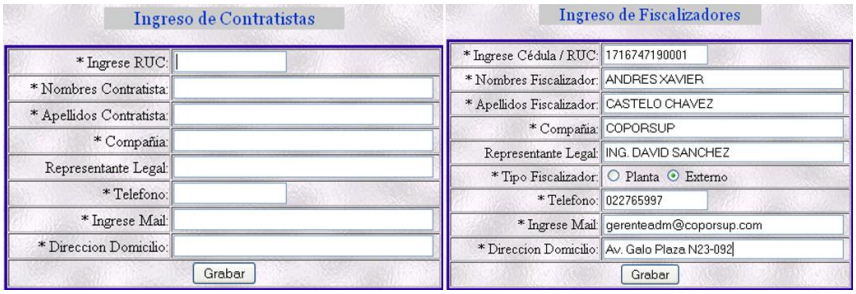
MENÚ DE OPCIONES PARA EL PERFIL TÉCNICO PROVINCIAL

En el perfil de técnico provincia se puede realizar acciones como: Ingreso de Contratista y Fiscalizadores, Contrato de Proyectos, Registro de Pagos y Pólizas, Registro de avance de obra y registro de actas.

Contratistas y Fiscalizadores

Esta opción permite a los técnicos de las diferentes unidades provinciales del MIDUIVI ingresar los datos de Contratista y Fiscalizadores que estarán presentes en la ejecución de los proyectos de vivienda.

El procedimiento para completar el ingreso de contratistas y fiscalizadores se detalla a continuación:



Cédula / RUC: Es el número de ruc o la cedula de identidad.

Nombres Contratista: Los nombres del contratista y fiscalizador.

Apellidos Contratista: Los apellidos del contratista y fiscalizador.

Compañía: El nombre de la empresa o compañía a la que pertenece.

Representante legal: El nombre del representante legal de la empresa o compañía.

Teléfono: El número de teléfono de contacto.

Dirección de Mail: La dirección de correo electrónica de contacto.

Dirección Domicilio: La dirección donde se encuentra ubicada la compañía.

Cabe aclarar que los campos que se encuentran señalados con un asterisco (*), son obligatorios y si no se completan correctamente, el ingreso de datos no será satisfactorio.

Seguimiento de Proyectos de Vivienda

Registro de contratos de Proyectos.

Esta opción permite a los técnicos registrar un contrato que realiza el constructor y el MIDUVI, en el cual se ingresa la siguiente información:

Tipo de contrato: Puede ser cotización, licitación, menor cuantía, directa.

Número de contrato: El número de contrato correspondiente al proyecto.

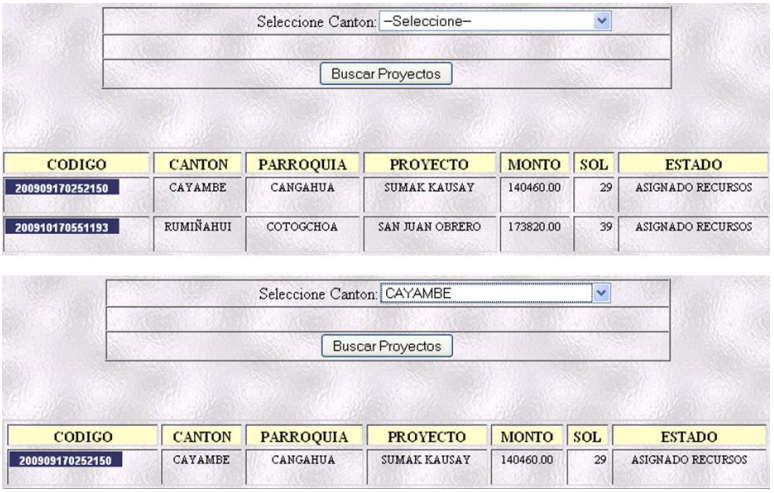
Plazo de contrato: El número de días del plazo contractual

Valor de contrato: El valor total del contrato.

Fecha y N° de Documento de pago: Fecha y número del documento habilitante.

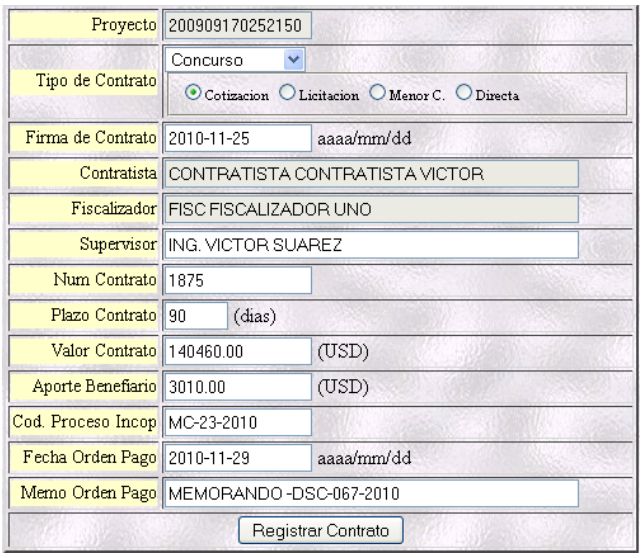
Búsqueda de proyectos a registrar contratos.

Como se muestra en la siguiente figura, la búsqueda puede ser general y específica, si el usuario no escoge ningún cantón, la aplicación devuelve un reporte con todos los proyectos que se encuentra en la provincia. Caso contrario se realiza una búsqueda solamente con en el cantón seleccionado.



Ingreso de información para completar el proceso.

Para registrar un contrato se debe llenar todos los campos, tal como se muestra en la siguiente figura.



En este caso, todos los campos son obligatorios, si uno de estos llegase a faltar, la aplicación presentará un mensaje de error indicando que campo falta de completar.

Registro Pago de Proyectos y Registro de Pólizas

De la misma forma se deben buscar los proyectos que se encuentran en estado CONTRATADO y van a ser pagados.

Luego de seleccionar el proyecto dando clic en el código, se presentará una pantalla para registrar las fechas y número de CUR correspondiente al proyecto, tal como se visualiza en la figura.

Ingreso de Pólizas.

Inmediatamente luego del registro del pago del bono, se debe registrar las 2 pólizas que habilitan al proyecto a seguir el proceso. Los campos a llenar son los siguientes:

Num Póliza 1: Buen uso del anticipo

Num Póliza 2: Fiel cumplimiento del contrato

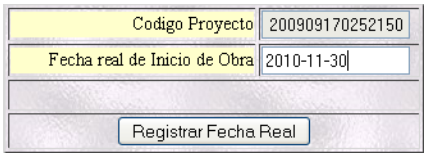
Luego de llenar y verificar la información de las pólizas, se procederá a registrar la información presionando el botón “Registrar Pago”.

Registro de avance de obra

Esta opción permite a los técnicos registrar el avance de obra de los proyectos de vivienda.

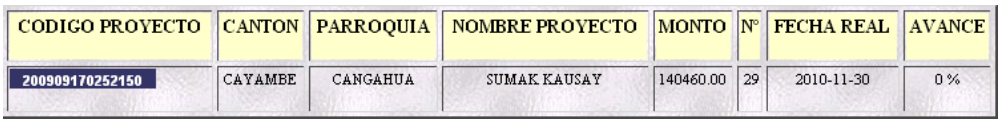
El primer paso es la búsqueda y selección el proyecto de vivienda, como se muestra en la figura.

Registro de Fecha real de inicio de obra.



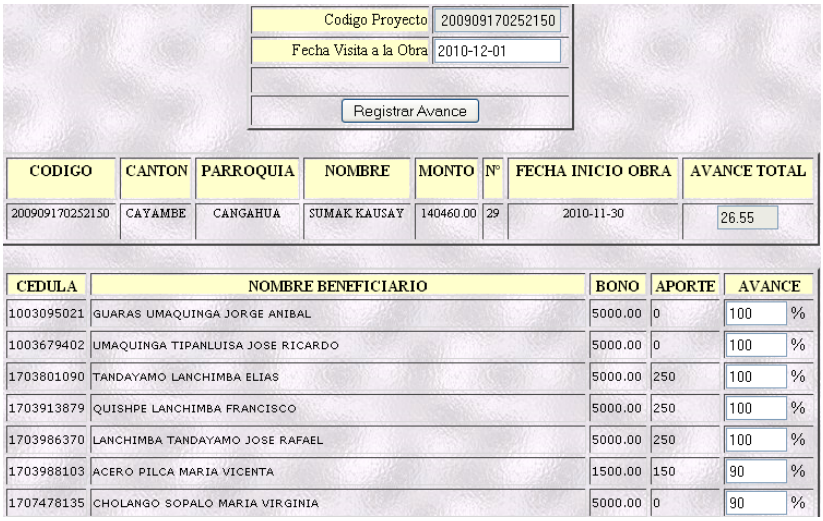
Para registra la fecha real de inicio de obra basta ingresar en el campo correspondiente y presionar el botón “Registrar Fecha Real”.

Luego de haber registrado la fecha real de inicio de obra, se procede a registrar el avance de obra de cada uno de los postulantes que componen el proyecto de vivienda, en la siguiente figura se puede visualizar que el avance esta con valor 0%, lo cual significa que todavía no se ha ingresado ningún registro.



CODIGO PROYECTO	CANTON	PARROQUIA	NOMBRE PROYECTO	MONTO	N°	FECHA REAL	AVANCE
200909170252150	CAYAMBE	CANGAHUA	SUMAK KAUSAY	140460.00	29	2010-11-30	0 %

Para finalizar y completar el proceso de avance de obra se debe ingresar en cada caja de texto frente a cada nombre de los postulantes, el avance de obra según las fechas de las visitas. Cada vez que se vayan registrando los datos de todos los postulantes automáticamente irá calculando el avance total del proyecto. Para poder completar este proceso el sistema comparará si el avance total es del 100%, el proyecto se asume como terminado y finalizado. La siguiente figura muestra el momento en que se registran los avance de obra para los primeros postulantes.



CODIGO	CANTON	PARROQUIA	NOMBRE	MONTO	N°	FECHA INICIO OBRA	AVANCE TOTAL
200909170252150	CAYAMBE	CANGAHUA	SUMAK KAUSAY	140460.00	29	2010-11-30	26.55

CEDULA	NOMBRE BENEFICIARIO	BONO	APORTE	AVANCE
1003095021	GUARAS UMAQUINGA JORGE ANIBAL	5000.00	0	100 %
1003679402	UMAQUINGA TIPANLUISA JOSE RICARDO	5000.00	0	100 %
1703801090	TANDAYAMO LANCHIMBA ELIAS	5000.00	250	100 %
1703913879	QUISHPE LANCHIMBA FRANCISCO	5000.00	250	100 %
1703986370	LANCHIMBA TANDAYAMO JOSE RAFAEL	5000.00	250	100 %
1703988103	ACERO PILCA MARIA VICENTA	1500.00	150	90 %
1707478135	CHOLANGO SOPALO MARIA VIRGINIA	5000.00	0	90 %

Registro de acta provisional y acta definitiva

Para el registro de actas se debe ingresar únicamente las fechas en las cuales se firmarán los documentos, teniendo en cuenta que existen 2 actas, una provisional y una definitiva, como se muestra en la siguiente figura.

Resumiendo lo anterior, el módulo de control y seguimiento de proyectos de vivienda para el área rural – urbano marginal, brinda a los técnicos del MIDUVI, la posibilidad de registrar todo el proceso del bono de vivienda, desde la aprobación hasta la culminación del proyecto con actas entrega recepción.

La información ingresada, estará almacenada en una base de datos centralizada que estará a disposición de los funcionarios del MIDUVI para que la utilicen en la generación de reportes tanto para técnicos como autoridades.

ANEXO D

MANUAL TÉCNICO DE SEGURIDAD.

Instalación segura del servidor Web.

Para las configuraciones del servidor web se debe ingresar al archivo de configuración “httpd.conf”, y modificar las opciones siguientes:

- Ocultar la versión de Apache y otra información sensible.

```
ServerSignature Off
ServerTokens Prod
```

- Ejecutar el usuario y grupo propio y de Apache.

```
User apache
Group apache
```

- Los ficheros fuera del web root no deben ser accesibles.

```
<Directory />
  Order Deny,Allow
  Deny from all
  Options None
  AllowOverride None
</Directory>
<Directory /web>
  Order Allow,Deny
  Allow from all
</Directory>
```

- Desactivar el listado de directorios y los *server side includes*.

```
Options -Indexes
Options -Includes
```

- Desactivar la ejecución de CGIs.

```
Options -ExecCGI
```

- Limitar permisos de acceso solo al usuario *root*.

```
chown -R root:root /usr/local/apache
chmod -R o-rwx /usr/local/apache
```

- Disminuir el valor del *timeout*.

```
Timeout 45
```

- Limitar el tamaño de las *requests*.

```
LimitRequestBody 1048576
```

- Restringir el acceso mediante IP.

```
Order Deny,Allow
Deny from all
Allow from 176.16.0.0/16
```

Configuración óptima de DNS para el acceso de las aplicaciones.

- Configurar el direccionamiento de dns de nic.ec hacia everydns.

```
DESTINATION NAT-FIREWALL
OBJETO                  DESTINO         PUERTO          NAT CNT
ConsultaBonos           192.168.4.22    80              10.80.8.8
ConsultaRS              192.168.4.23    80              10.80.8.16
```

- Configurar el direccionamiento de DNS de nic.ec hacia EveryDns.

```
CONFIGURACIÓN DNS DE NIC.EC A EVERYDNS
PRIMER DNS      ns1.everydns.net
SEGUNDO DNS     ns2.everydns.net
TERCER DNS      ns1.everydns.net        OPTIONAL
```

- Configurar de everydns a MIDUVI.GOB.EC

```
CONFIGURACIÓN DNS DE NIC.EC A EVERYDNS
HOST                            TYPE            VALUE
*.miduvi.gob.ec                 A               204.92.106.13
consultabonos.miduvi.gob.ec     A               201.219.3.16
savmiduvi.miduvi.gob.ec         A               201.219.3.17
```

- Acceso a las aplicaciones desarrolladas.

Si no se siguen estas recomendaciones el acceso a las aplicaciones será de la siguiente forma:

http://201.219.3.16/index.php

Luego de seguir las recomendaciones el acceso será de la siguiente forma:

http://consultabonos.miduvi.gob.ec/

Respaldo de bases de datos.

Para respaldar las bases de datos de las aplicaciones realizadas se puede implementar el siguiente procedimiento.

- Verificar que la herramienta Crontab este activa.

```
[root#server]          ls /usr/bin
```

- Generar el script para el respaldo diario automático.

```
Min     Hora    dia     mes     diase          usuario        comando
01 * * * * root tar -czvf /home/respaldo/bk.tar.gz  /var/www/consultab
```

- Reiniciar el servicio.

```
[root#server]          service crond restart
```

Programación segura en PHP.

- Limpiar entradas de variables.

```
function htmlclean($input) {
$sb_convert = $input;
$sb_input = array("<",">","(",")");
$sb_output = array("&lt;","&gt;","&#40;","&#41;");
$output = str_replace($sb_input, $sb_output, $sb_convert);
return $output;
}
```

- Utilizar funciones que deshabilitan intrusiones.

```
mysql_real_escape_string();  addslashes();
```

- Utilizar funciones que deshabilitan SQL inyection.

```
function no_injection($string) {
    if(get_magic_quotes_gpc())
        $string = stripslashes($
string);
    return $string;
}
```

```
function des($string){
$string = striptags($string);
$string = htmlspecialchars($string)
;
$string = trim($string);
$string = stripslashes($string);
$string = mysql_real_escape_string(
$string);
return $string;}
```

ANEXO E

NORMAS Y ESTÁNDARES EN LA ADMINISTRACIÓN DE LA INFORMACIÓN.

INTRODUCCIÓN A LA ADMINISTRACIÓN DE LA INFORMACIÓN.

En este apartado se pretende abarcar los principales problemas y las mejores prácticas para obtener un eficaz procesamiento y administración de la información, logrando agilitar los procesos de automatización de una institución para mejorar su productividad.

Generar nuevas ideas y aplicar nuevos procedimientos en el manejo de la información es la clave para triunfar en la actualidad, pues se tendrá la capacidad de generar reportes generales, específicos, gerenciales, tabulados, estadísticos, etc. a partir de datos que son procesados adecuadamente.

"Como menciona Shoshana Zuboff, la administración de Información con Tecnología agiliza el proceso de automatización, pero una compañía que persiga la información no sólo por razones de automatización o reporte de actividades, sino que la explore por su valor intrínseco, utilizará esta información para mejorar su rendimiento"[10]

ESTÁNDARES PARA EL MANEJO DE INFORMACIÓN.

Un estándar establece un sistema común de terminología y de definiciones que estén presentes al documentar o guardar datos. Todos los conjuntos de metadatos[11] deberían tener su referencia en un estándar.

Existen varios estándares disponibles para el manejo de datos, y la razón es que existan tantos es que los metadatos se emplean en casi todos los procesos de automatización.

Ejemplos: IEEE/LTSC LOM- IMS Global Learning Meta-Data, Dublin Core

[10] Fuente: http://www.osmosislatina.com/administracion/

[11] Metadato: son datos que escriben otros datos. Fuente: http://es.wikipedia.org/wiki/Metadato/

PRINCIPALES VENTAJAS AL UTILIZAR ESTÁNDARES.

Al utilizar un estándar, encontrar información específica en un banco de datos resulta mucho más fácil y ágil que si no se utiliza ningún estándar.

Permiten búsquedas automatizadas, ya que se puede programar una búsqueda determinada que cumpla con ciertos parámetros y bajo ciertas condiciones.

Se trabaja con un lenguaje común entre las personas que se interesan por el manejo y tratamiento de la información, logrando minimizar la duplicación de esfuerzos en la elaboración, procesamiento o distribución de la información.

NORMAS PARA EL MANEJO DE INFORMACIÓN.

- *Información pública.*

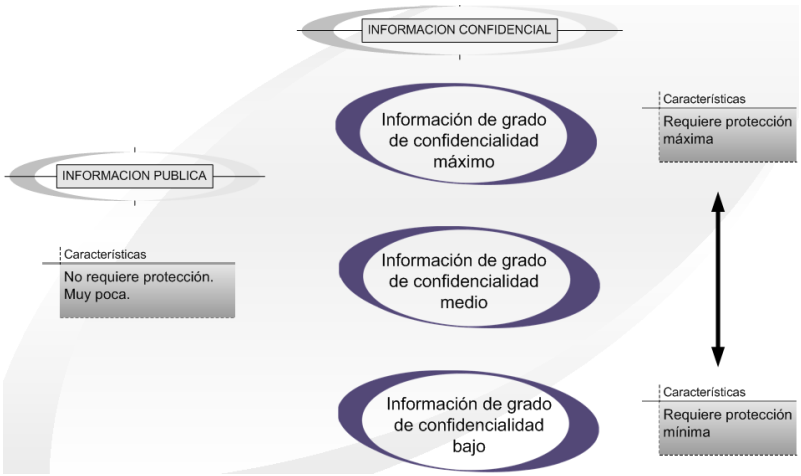
Es aquella información que ha sido declarada de conocimiento público y que puede ser publicada sin ninguna prohibición, ya que este tipo de información debe ser de conocimiento público.

Se puede deducir que en este caso la información publicada no genera daño o amenaza alguna a la empresa o institución, ni tampoco a los procesos o a los sistemas que procesen este recurso.

- *Información confidencial.*

La información confidencial es aquella que por su naturaleza no puede ser revelada a terceros y por lo tanto no es pública, se entiende que ésta posee un determinado nivel crítico y que por ello debe ser tratada y protegida con mayor atención.

Para este caso se debe tener una persona que acoja la responsabilidad de salvaguardar este tipo de información, y a la vez, que pueda asegurar una protección adecuada de este recurso.

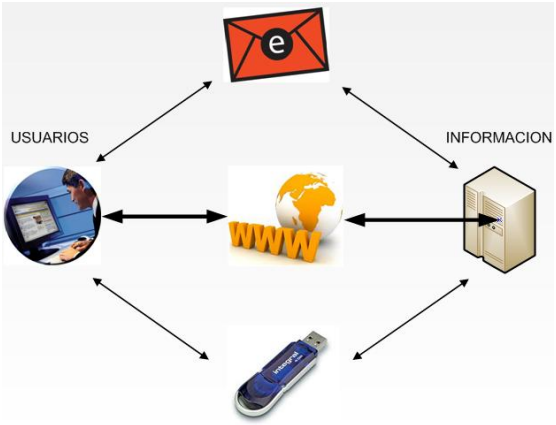


Tipos de información confidencial

Información con grado de confidencialidad mínimo

Es la información que puede ser conocida por terceros con una restricción mínima, que no requiera un proceso complejo.

El acceso debe ser permitido a funcionarios, empleados, usuarios externos cuyas actividades requieran de esta información.



Ejemplo:

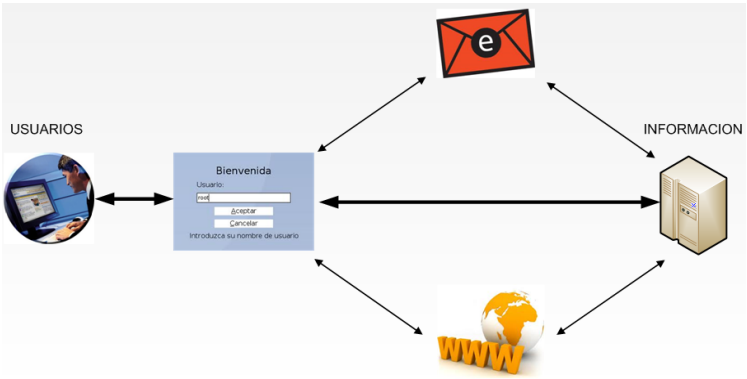
Detalle de los nombres de beneficiarios del bono de vivienda.

Información con grado de confidencialidad medio

Es la información que puede ser conocida por terceros con restricción considerable, por ejemplo un acceso de login con usuario y contraseña.

Se debe tener un responsable para salvaguardarla.

El acceso debe ser permitido a funcionarios, empleados, usuarios externos cuyas actividades requieran de esta información.



Ejemplo:

Detalle de los nombres de beneficiarios, ubicación geográfica, monto del beneficio entregado.

Información con grado de confidencialidad máximo

Es la información que NO puede ser conocida por terceros que no pertenezcan a la organización o institución, se debe tener un administrador único.

El acceso debe ser permitido a funcionarios y empleados registrados, y en caso extremo si hubiere usuarios externos se debería crear una licencia de uso y confidencialidad para protección de la misma.

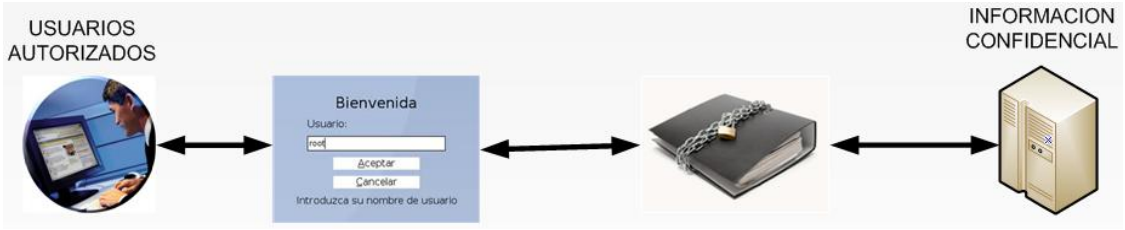


Grafico 4: Esquema de información con grado de confidencialidad máximo. Fuente: Investigación del autor.

Ejemplo:

Detalle específico de los beneficiarios (cédula, teléfono, dirección domiciliaria, número de cuenta bancaria) a los cuales se les otorga el beneficio.