UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO-CAMPUS SUR

CARRERA DE INGENIERÍA EN SISTEMAS

MENCIÓN TELEMÁTICA

"DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA COMWARE S.A. EN LA CIUDAD DE QUITO, APLICANDO LA NORMA ISO/IEC 27001"

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO DE SISTEMAS

DIEGO CALDERÓN

DAVID SANCHEZ

DIRECTOR: ING. RAFAEL JAYA

QUITO, Octubre 2012

DECLARATORIA DE RESPONSABILIDAD

Nosotros, Diego Omar Calderón Merchán y David Alejandro Sánchez Meza, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

_____ _____

Diego Omar Calderón Merchán David Alejandro Sanchez Meza

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diego Omar Calderón Merchán y David Alejandro Sánchez Meza, bajo mi dirección.

_____

Ing. Rafael Jaya

Director de Tesis

DEDICATORIA

A Dios, por haberme dado la fortaleza de continuar frente a todas las adversidades de la vida, por su infinito amor y por todas las bendiciones que derrama sobre mi vida, por ser un DIOS DE PACTOS.

A mi viejito el Sr. Edgar Sánchez, que sin el nada de esto habría sido posible, por haberme enseñado a pelear en medio de las adversidades, por levantarme cuando estaba caído, por todos sus consejos y desvelos, por ser un padre tan ejemplar, por cuidarme y protegerme, no tengo palabras para agradecerle todo lo que hace por mí y su familia, espero poder llegar un día a ser por lo menos la mitad del maravilloso ser humano que es mi padre, lo único que me resta decir es Dios le pague papá le amo con toda mi vida.

A mi madrecita Laurita, por todo su amor entregado a su familia, por todos sus cuidados por que sin lugar a duda tiene el corazón más noble y bueno que puede existir sobre la faz de la tierra, gracias madre por haber estado junto a mí siempre en todos los momentos de mi vida por no dejarme de amar pese a mis faltas y mis errores, porque tu amor es el más puro que se puede tener, Dios le pague madre sin usted nada de esto habría sido posible.

A mi hermano Edgar, por todos sus sabios consejos por haberme enseñado el camino perfecto el camino de Dios.

A mi hermana Patricia, por el ejemplo de mujer que es, por que cada día demuestra lo importante que es el perseverar para alcanzar los sueños.

A mi hermano Daniel, por su sinceridad y esforzarse cada momento de su vida para lograr sus objetivos.

David Sánchez.

DEDICATORIA

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres Flora y Segundo, por darme la vida, por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis hermanos Esthela, Xavier, Vinicio y José, por su apoyo y cariño incondicional.

A mi hermana Viviana, que a pesar de ya no estar entre nosotros siempre será la fuerza que nos ayudara a superar las adversidades y un gran ejemplo a seguir.

A mis sobrinos(as), por su ternura y su cariño fraterno, y a pesar de la corta edad de algunos de ellos, son una parte fundamental para el logro de este objetivo.

A mis amigos(as) Jessy, Verito, Fernanda, Geovanna, Oscar, Marce, Willy, Edison, Danny, y Andrés; por su apoyo en todo momento y circunstancia, ya que a pesar de cualquier problema siempre estamos juntos como hermanos ayudándonos mutuamente.

Diego Calderón.

AGRADECIMIENTO

Agradezco a todas y cada una de las personas que contribuyeron con la realización de la presente tesis de grado.

A la Universidad Politécnica Salesiana y sus docentes, por haberme permitido estudiar en sus aulas y por todo el conocimiento impartido.

A los ingenieros Rafael Jaya y Alberto Duchi por su valiosa guía y ayuda, por haberme permitido concluir con éxito la carrera universitaria.

A mis dos grandes amigos de la universidad Galo Montenegro y Jorge Rúales por todo el esfuerzo realizado en todos nuestros años de estudio y sobre todo por todo el apoyo incondicional recibido, gracias amigos.

A la empresa ComWare S.A y sus directivos por permitirnos desarrollar el presente proyecto de tesis en tan prestigiosa empresa.

David Sánchez.

Agradezco a todas las personas que de una u otra forma contribuyeron con el desarrollo y culminación del presente proyecto.

A mis maestros, y en especial a los Ingenieros Rafael Jaya y Alberto Duchi, por su gran apoyo y motivación para la culminación del presente proyecto.

A la Universidad Politécnica Salesiana, por abrirme sus puertas y ayudarme en mi formación personal y profesional.

A David, mi compañero de tesis, ya que juntos logramos alcanzar este objetivo.

A Comware por permitirnos realizar nuestro proyecto de tesis en sus instalaciones.
Gracias a Todos.

Diego Calderón.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

PRESENTACIÓN

En el presente proyecto de titulación se pretende dar un enfoque de diseño adecuado para la solución de seguridad informática a la empresa Comware S.A, tomando como base estándares internacionales.

El primer capítulo, muestra el análisis de la situación actual por medio de una descripción detallada de cómo se encuentra conformada la empresa tanto a nivel gerencial y jefaturas así como el adentrarse a la red informática con la descripción de los diferentes equipos que se encuentran activos en la red.

El segundo capítulo, exterioriza una descripción de la Norma ISO 27001:2005, en donde señala que la seguridad de información no se trata sólo de aspectos tecnológicos sino que su objetivo es organizar la seguridad de información, por tanto propone toda una secuencia de acciones tendientes al "Establecimiento, Implementación, Operación, Monitorización, Revisión, Mantenimiento y Mejora del Sistema de Gestión de Seguridad de la Información".

El tercer capítulo, se realizara el análisis del riesgo y vulnerabilidades dentro de la red por medio de herramientas (software), de esta manera se podrá tener una visión general de puntos que pueden ser afectados dentro de la seguridad de la red en los diferentes servidores de alta criticidad en la empresa.
Se mostrará mediante cada uno de los ítems cuales serían los pasos a seguir para diseñar o implementar un SGSI aplicando la Norma ISO/IEC 27001, la forma de medir los riesgos, así como la metodología de implementación, selección de controles y demás haciendo referencia a puntos clave de la norma, estableciendo una guía el momento que se requiera implementar y certificarse en la norma ISO/IEC 27001.

El cuarto capítulo, se realiza una propuesta formal para la empresa ComWare S.A del cómo se realizaría la implementación del Sistema de Gestión de la

seguridad de la información propuesto, tomando en cuenta temas puntuales y dando a conocer de una forma resumida cuales serian los pasos a seguir de tal forma que no se presente de una forma confusa, y los directivos de la empresa puedan tener una comprensión del tema totalmente efectiva.

En el capítulo final se presentan las conclusiones y recomendaciones en base al desarrollo de este proyecto de titulación.

RESUMEN

El presente proyecto de titulación tiene como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Comware S.A en la ciudad de Quito basado en la Norma ISO 2700:20051, con el fin de lograr un esquema que sirva como guía para la posterior implementación y certificación en la Norma ISO 27001:2005 en la empresa. Además se podrán evidenciar claramente amenazas y riesgos que se encuentran presentes y pueden llegar a afectar el correcto funcionamiento de los sistemas informáticos. De esta forma, los riesgos de seguridad en la red son identificados y minimizados en base a los procedimientos para el tratamiento de los mismos.

También se realizó un análisis por medio de varios software que permitieron ver algunas falencias dentro de los sistemas que se manejan en la empresa y de esta forma realizar un análisis de las amenazas que se encuentran latentes en los sistemas informáticos.

Por último se da una breve explicación de cuáles son los pasos a seguir para que la empresa pueda certificarse en la Norma ISO 27001:2005.

CAPITULO I

ANÁLISIS DE SITUACION ACTUAL DE COMWARE

1.1 PRESENTACIÓN

La compañía Comware S.A es una de las empresas líderes en integración en servicios y soluciones informáticos con una experiencia de más de 35 años. Su sede principal se encuentra en la ciudad de Quito y cuenta con una sucursal en Guayaquil y Cuenca. Es representante de las reconocidas marcas mundiales en el ámbito de sistemas, tales como: Avaya, Cisco, Dell, EMC2, Enterasys, IFS, Sungard, Oracle Sun, Symantec, entre otros. El objetivo de este capítulo es dar a conocer la manera cómo se encuentra constituida actualmente la empresa, tanto a nivel gerencial como de procesos así como su infraestructura de red.

1.2 ANTECEDENTES DE LA EMPRESA

A continuación se detallara la información más relevante de la Compañía Comware S.A basándose en su sitio web: http://www.comware.com.ec/

1.2.1 ESTRUCTURA

"La compañía se constituyó en la ciudad de Guayaquil, en octubre de 1973[…]. Posteriormente, cambió su nombre a COMWARE del Ecuador S.A. para finalmente, en el año 2004, convertirse en COMWARE S.A.,[…]."[1]

"A lo largo de su trayectoria, COMWARE ha logrado una evolución en los productos y servicios que ofrece, pasando de ser un proveedor de equipos de

[1]Comware, "Mi Compañía", 2012-02-09, http://www.comware.com.ec/jsp/user/go.do?sectionCode=20

computación y comunicaciones, a ser un Integrador de Servicios y Soluciones,[…].”[2]

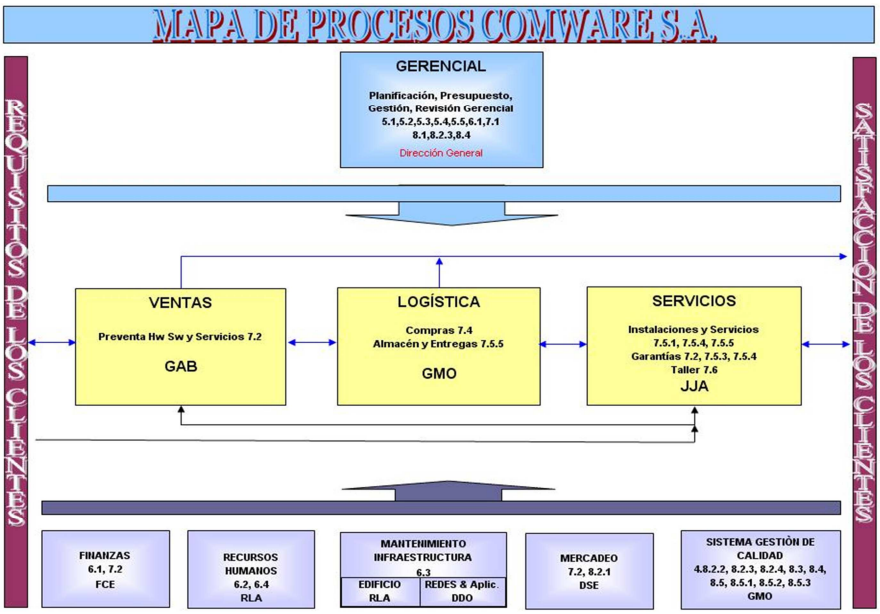


Fig. 1. 1Mapa de procesos de Comware
F**uente:** La Empresa

1.2.2 MISIÓN

“Poner al alcance de nuestros clientes soluciones tecnológicas innovadoras que mejoren la operación de su negocio, con un equipo humano especializado y comprometido con la calidad”.[3]

1.2.3 VISIÓN

“Ser para nuestros clientes el socio que apoya en la operación de su negocio”.[4]

1.2.4 OBJETIVO DE LA EMPRESA

- Brindar soluciones a nuestros clientes, integrando aplicaciones, equipos y servicios en las áreas de computación y

[2]Comware, “Mi Compañía”, 2012-02-09, http://www.comware.com.ec/jsp/user/go.do?sectionCode=20

[3]Idem 2

[4]Idem 3

telecomunicaciones, mediante alianzas con fabricantes de prestigio internacional, tales como Avaya, Cisco, Dell, EMC2, Enterasys, IFS, Sungard, Sun Microsystems Symantec, entre otros.

- Contar con un grupo de profesionales capacitados y certificados por los fabricantes, para proporcionar servicios de la más alta calidad, buscando la satisfacción de sus Clientes.[5]

1.2.5 SERVICIOS BRINDADOS.

- Servidores y Virtualización
- Almacenamiento y recuperación de datos; Virtualización de almacenamiento
- Continuidad del Negocio “BussinessContinuity”
- Servicios de identidad; Servicios de Integración
- Cableado estructurado e infraestructura de red
- Soluciones de Telefonía IP
- Comunicaciones unificadas y soluciones de mensajería
- Contact Center
- Outsourcingde Infraestructura Voz y Datos
- Soluciones Empresariales
- Servicios de Educación y Consultoría TI
- Convenios de Soporte y Mantenimiento
- Capacitación[6]

1.3 INFRAESTRUCTURA DE RED.

1.3.1 CENTRO DE DATOS

El centro de datos es un espacio especialmente asignado y equipado de tal forma que pueda mantener los equipos de infraestructura de red y aplicaciones

[5]Comware, “DocManager”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[6]Idem 5

de la empresa funcionando adecuadamente sin que exista peligro evidente para su inoperabilidad.

El centro de datos se encuentra equipado de la siguiente manera:

- Aire acondicionado.
- Racks
- Ups
- Acceso mediante llave de seguridad
- Tablero de energía eléctrica
- Los equipos que se encuentran en el centro de datos serán descritos a continuación en la infraestructura de red física.[7]

1.3.2 INFRAESTRUCTURA DE RED FÍSICA

Descripción de la red.-

La red se encuentra conformada por los siguientes equipos:

SERVIDORES:

Centos.- Este servidor elaborado con el sistema operativo Centos, el mismo que es utilizado para realizar pruebas a diferentes aplicaciones.

Proxy.- El servidor proxy permite interceptar las conexiones de red que un cliente hace a un servidor de destino.

Web.- El servidor web es en donde se almacena la página web de la empresa.

Docmanager.- El servidor de Docmanager permite el almacenamiento de los registros y documentos de la norma ISO 9001:2008

Backups.- El servidor de Backups permite el almacenamiento de todos los backups de los computadores de los usuarios.

[7]Comware, "Infraestructura Redes", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

Exactus.- El servidor Exactus es en donde se encuentra almacenada la aplicación contable de la empresa.

Sac.- El servidor Sac es en donde se encuentra almacenada la aplicación de generación de tickets para la atención de los clientes de la empresa.

Aranda.- El servidor Aranda es en donde se encuentra almacenada la aplicación para generación de tickets de atención internos en la empresa.[8]

EQUIPOS DE COMUNICACIÓN:

Central Avaya.- La central telefónica Avaya permite la comunicación interna y externa de llamadas telefónicas.

Intuity.- Este servidor es el encargado de almacenar los buzones de voz correspondientes a cada uno de los usuarios.

Sip.- La troncal Sip permite la comunicación directa con la sucursal de Guayaquil

Firewall.- El firewall permite las conexiones entrantes o salientes al sistema

Router.-Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la ruta más apta.

Switch.-Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Accespoint.- Los accesspoint permiten la comunicación inalámbrica hacia la red e internet.[9]

[8]Comware, “Infraestructura Redes”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[9]Idem 8

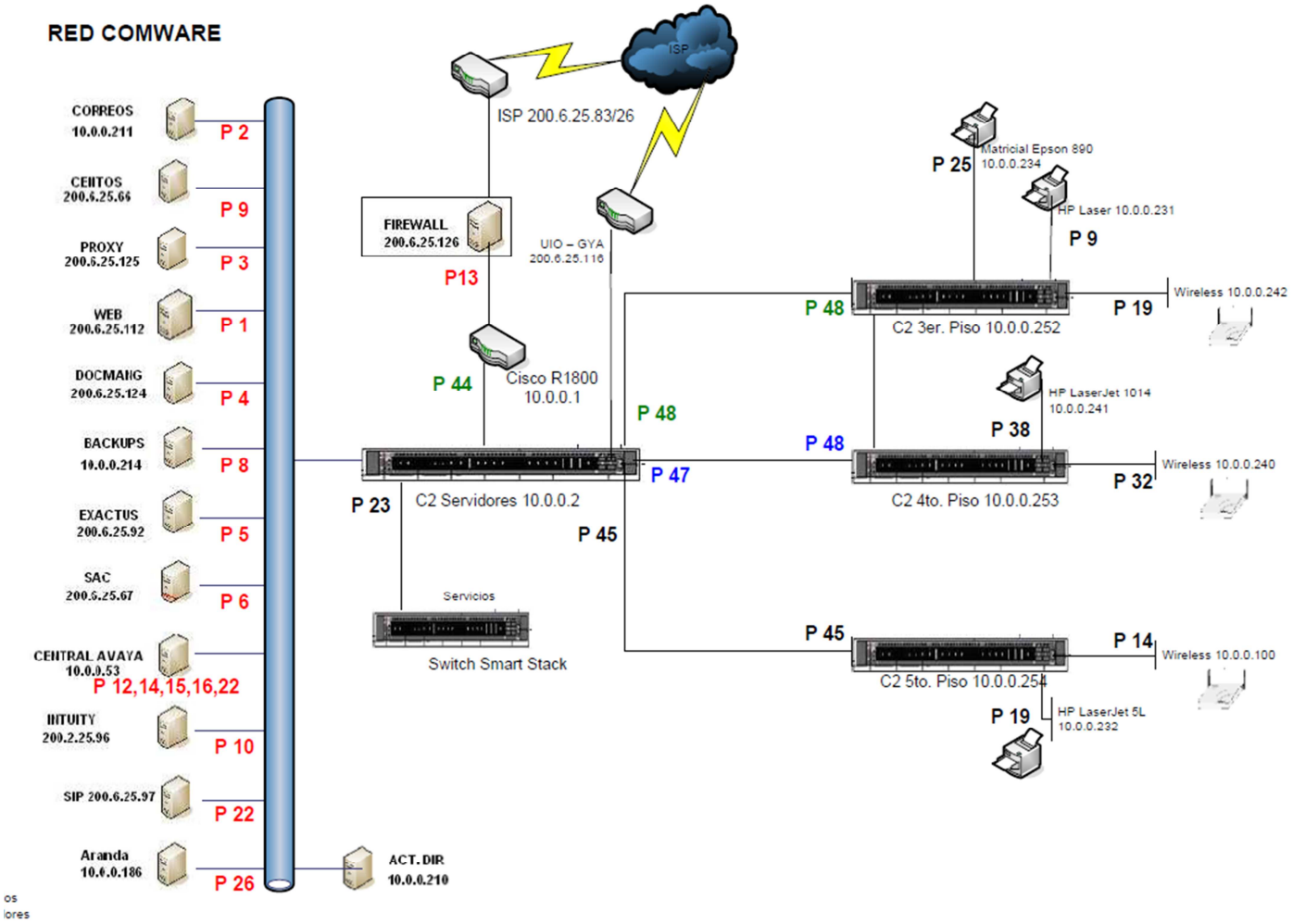


Fig. 1. 2 Red de ComwareRed de Comware
Fuente: La Empresa

1.3.3 INFRAESTRUCTURA DE RED LÓGICA.

"Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. […].
Topología bus-estrella: implementa una topología estrella a través de una topología de bus física."[10]

Todas las estaciones se conectan directamente a un único canal físico (cable) de comunicación (bus). Según los sentidos posibles de transmisión, el bus puede ser unidireccional (principalmente buses de fibra óptica), los extremos del canal (cable) no están interconectados sino simplemente finalizados con un

[10]ANGELFIRE, "TUTORIAL DE REDES", 2012-09-02 http://www.angelfire.com/cantina/oronaweb/topologia.htm

terminador de 50 ohmios. El terminador elimina automáticamente la señal de los extremos. Es posible unir varios segmentos de buses en una configuración "multibus" siendo necesario utilizar repetidores de señal en el caso de grandes distancias.

Pero su funcionamiento realmente es como un anillo, es decir, se utiliza con el fin de facilitar la administración de la red debido a que cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino.

1.4 MANUAL DE LA CALIDAD DE GESTIÓN ISO 9001:2008

1.4.1 MANUAL DE CALIDAD

La empresa Comware S.A maneja un manual de calidad de gestión ISO 9001:2008 en donde se describe la manera cómo la empresa se encuentra obligada a mantener la calidad en los procesos.

1.4.1.1 OBJETIVO

"El objetivo del presente Manual del Sistema de Gestión de Calidad en la Organización, es el de describir las disposiciones generales para asegurar una orientación hacia la calidad en los procesos de COMWARE, de acuerdo a los requisitos de la Norma ISO 9001."[11]

1.4.1.2 ALCANCE

El sistema de Gestión de Calidad de Comware abarca la "COMERCIALIZACIÓN, COMPRA, ENTREGA E INSTALACIÓN DE HW / SW DE COMPUTACIÓN Y TELECOMUNICACIONES Y LA PROVISIÓN DE

[11]Comware, "Sistema de Gestión de Calidad", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

SERVICIOS DE MANTENIMIENTO Y EDUCACIÓN, EN LAS OFICINAS DE QUITO, GUAYAQUIL Y CUENCA".[12]

1.4.1.3 EXCLUSIONES DE LA NORMA ISO 9001

Requisito7.3 DISEÑO Y DESARROLLO: se lo excluye debido a que Comware comercializa productos y servicios diseñados, desarrollados y manufacturados por los fabricantes a los cuales representa. La configuración de las soluciones ofertadas a los clientes es controlada por el proceso de Ventas y su instalación, por el proceso de Servicios.

Requisito7.5.2 VALIDACIÓN DE LOS PROCESOS DE LA PRODUCCIÓN Y DE LA PRESTACIÓN DEL SERVICIO: se lo excluye debido a que los procesos de ejecución de COMWARE incorporan mecanismos de control y monitoreo que aseguran que los productos o servicios comercializados cumplan sus propios requisitos y aquellos de nuestros clientes, de forma previa a su entrega.[13]

1.4.2 PROCESOS DE COMWARE

Los procesos definidos por Comware son: de Ejecución, de Soporte y Gerencial, los cuales se detallan a continuación.

1.4.2.1 PROCESOS DE EJECUCIÓN

- Ventas
- Logística
- Servicios[14]

[12]Comware, "Sistema de Gestión de Calidad", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[13]Comware, "Exclusiones", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[14]Comware, "Procesos", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

1.4.2.2 PROCESOS DE SOPORTE

- Finanzas
- Talento Humano
- Remuneraciones y Compensaciones
- Mantenimiento de Infraestructura del Edificio
- Mantenimiento de Infraestructura de Redes y Aplicaciones
- Mercadeo
- Sistema de Gestión de Calidad[15]

1.4.2.3 PROCESOS GERENCIALES

- Gerencial

En el proceso Gerencial se establecen las políticas y principios rectores de la organización, se aprueba la estructura organizacional, los recursos a través del Presupuesto y se monitorea el funcionamiento de la organización a través de la Gestión y Revisión Gerencial.[16]

1.4.3 ESTRUCTURA DOCUMENTAL

La Estructura de los Documentos para COMWARE S. A. se muestra a continuación:

> El Plan de Negocios de la Compañía, el Manual de Calidad, las Caracterizaciones de Procesos, los Procedimientos, Políticas, Matrices y Alcances, Instrucciones de Trabajo, los Registros, Documentos Base, Reglamentos, Formatos, Normas Externas, Catálogos, Descripciones de Puestos y los Planes de Calidad son los diferentes tipos de documentos que hacen parte del sistema documental.[17]

[15]Comware, “Procesos”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[16]Idem 15

[17]Idem 15

1.5 IDENTIFICACIÓN DE MECANISMOS DE SEGURIDAD INFORMÁTICA IMPLEMENTADOS ACTUALMENTE EN LA EMPRESA.

1.5.1 POLÍTICA DE HARDWARE Y SOFTWARE

Esta política norma la instalación y uso del software dentro de la empresa, así como la adquisición de equipos.

1.5.1.1 NORMATIVA

1.5.1.1.1 USO DE SOFTWARE

La instalación de utilitarios y demos se realizará bajo en el conocimiento y aprobación del jefe de servicios internos.

Se podrá instalar software para configuración de equipos y Proveedores que se encuentren en el registro "Lista de proveedores aprobados" R-LOG-01.

No se podrá instalar software o utilitarios que no estén relacionados con las actividades diarias de cada usuario, tales como:

- Atomix Mp3
- Kazaa
- Audio MP3
- Converter
- Limewire
- Torrent
- Cualquierotroaplicativo P2P
- Sniffer o software para capturar tramas de red y analizar el tráfico en una red de computadoras

El área de Sistemas Internos será la responsable de implementar mecanismos de control y auditoría de uso de software dentro de la empresa.

El software autorizado para uso interno de la compañía se encuentra detallado en el documento IT-MIR-08: “Instructivo para la instalación del Software”. Si existiera algún software adicional que, por excepción,requiera utilizar un usuario deberá ser autorizado por su Jefe Inmediato.[18]

1.5.1.1.2 USO DE HARDWARE

Los computadores personales y servidores para uso interno de la Compañía deberán ser de alguna marca representada a la fecha por Comware S.A., siempre y cuando los precios sean competitivos con equipos de otras marcas. Se podrán comprar equipos de otras marcas o clones, considerando lo que dice el IT-LOG-01: “Selección y Evaluación de Proveedores”, referente a las compras emergentes.[19]

1.5.2 POLÍTICA DE RESPALDOS Y RECUPERACIÓN

La recuperación de sistemas resulta necesaria, ante una interrupción del servicio. Ésta no siempre se debe a factores extraordinarios, sino que puede surgir de un mal funcionamiento del sistema, errores humanos u otras fallas, que producen un tiempo de caída del sistema comparativamente menor al que produciría un desastre. […].[20]

[18]Comware, “Mecanismos”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[19]Idem 18

[20]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

1.5.2.1 NORMATIVA

- Los respaldos del sistema operativo, programas de los sistemas y su configuración deberán realizarse con base al tipo de equipo del que se trate, apegándose al procedimiento establecido.

- Cuando se vaya a realizar un servicio de mantenimiento a los servidores, deberá generarse el respaldo correspondiente. Si el mantenimiento es de tipo preventivo o rutinario, deberá hacerse con la anticipación necesaria y bajo lo dispuesto en esta política.

- Todo sistema, antes de entrar en producción, deberá contar con la documentación de los procedimientos de respaldo y recuperación. La misma será controlada por el área de Sistemas Internos de la Compañía para verificar que es clara, completa y contempla como mínimo la recuperación de los siguientes elementos:

  El remplazo de los servidores críticos.
  El sistema operativo y su configuración (parámetros, file systems, particiones, usuarios y grupos).
  Los utilitarios y paquetes de software base, necesarios para que la ejecución de las aplicaciones de la compañía.
  Los programas que componen la aplicación.
  Los archivos y/o bases de datos del sistema.
  Horario de ejecución de respaldo.
  Documentación de aplicaciones y diccionario de Base de Datos.[21]

1.5.2.2 ADMINISTRACIÓN DE RESPALDOS

Las cintas deben tener la siguiente información en las etiquetas de control:

[21]Comware, "Políticas", 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

- Fecha del primer uso de la cinta.
- Nombre del servidor o sistema del cual se está obteniendo el backup.
- Las cintas de respaldo que se almacenen en sitios internos deben guardarse dentro de armarios, con su respectiva seguridad.
- Las cintas de respaldo de datos y programas podrán ser reutilizados de acuerdo al siguiente esquema:
- Respaldo mensual: después de 12 meses.
- Respaldo semanal: después de 4 semanas.
- Respaldo diario: después de 7 días.
- Para los respaldos en cinta se debe contar con una bitácora para registro y control de respaldos: R-MIR-10 “Control de Respaldos”, la cual deberá contener los siguientes datos: Nombre del Respaldo, mes y fecha del respaldo, contenido del respaldo, encargado del respaldo, observaciones. Dicho documento será almacenado en el archivo principal del Área de Sistemas Internos.
- Los respaldos que se realizan en GYE tanto para servidores como para equipos de los usuarios con el software Symantec Netbackup serán de forma automática y verificada que se cumplan por parte del encargado (JVI).
- Los respaldos automáticos realizados en UIO y CUE con la herramienta por los programas clientes CobianBackup y Handy Backup a un servidor de respaldo será responsabilidad del responsable del área encargado de dichos respaldos revisar diariamente que los respaldos se realicen correctamente.[22]

1.5.2.3 ADMINISTRACIÓN DE RECUPERACIÓN DE RESPALDOS

- Se efectuarán pruebas de recuperación de las copias de respaldo de acuerdo a lo estipulado en el documento IT-MIR-07 “Instrucciones para la obtención de los respaldos y su recuperación". Estas pruebas

[22]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

servirán para constatar que se puedan obtener correctamente los datos grabados en la cinta al momento de ser necesarios, de forma de garantizar su propósito.

- En caso de contingencia, se realizará la recuperación de los respaldos necesarios para la solución de los problemas originados.
- Se debe contar con una bitácora para el registro y control de la recuperación de respaldos: R-MIR-16 “Bitácora de Control de Recuperación de Respaldos”, la cual deberá contener los siguientes datos: Etiqueta respaldo, mes y fecha del respaldo, fecha de recuperación del respaldo, encargado de la recuperación del respaldo, estado respaldo, observaciones. Dicho documento será almacenado en el archivo principal del Área de Sistemas Internos.
- En caso de fallar la recuperación del respaldo de una cinta, se deberá probar con un backup anterior y de acuerdo al error deberá reutilizarse o desecharse dicha cinta.[23]

1.5.2.4 RESPALDO DE BASE DE DATOS, APLICACIONES Y SISTEMAS OPERATIVOS

- Los respaldos ejecutados deben cumplir con lo siguiente:

Aplicación	Motivo
Sistema Operativo	En caso de modificaciones, actualizaciones de la configuracióno instalaciones de nuevas versiones
Software de aplicaciones	En caso de modificaciones de la configuración, actualizaciones o instalaciones de nuevas versiones
Bases de Datos y Sistemas Transaccionales	De acuerdo a lo establecido en el documento IT-MIR-07 “Instrucciones para la obtención de los respaldos y su recuperación", y en caso demodificaciones a la estructura o nuevas versiones

Tabla 1. 1 Respaldos
Fuente: Los autores

[23]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

1.5.2.4.1 RESPALDO OUTSIDE

Se contrató una casilla de seguridad con el Banco del Pichincha para almacenar las cintas de respaldo de los sistemas que maneja la empresa así como cualquier información que sea de importancia en la empresa.

- Las cintas serán colocadas en la casilla de seguridad de forma trimestral; en este caso serán 4: Sistema Comercial, Logística, Sac y DocManager
- El total de cintas a colocar serán las que el espacio físico de la casilla lo permita.
- Los respaldos se los realizará en base al documento IT-MIR-07 “Instrucciones para la obtención de los respaldos y su recuperación".
- En caso catástrofes naturales el área de Sistemas Internos procederá a retirar los discos duros de los servidores.[24]

1.5.3 POLÍTICA DE USO DE INTERNET

Esta política normará el uso correcto del Internet.

1.5.3.1 NORMATIVA

General:

- No se considera el Internet en Comware S.A. como una fuente de diversión o entretenimiento. De igual manera, no se autoriza ni es ético el uso del servicio de Internet de la compañía, para manejar o administrar un negocio privado.
- Toda persona que sea sorprendida haciendo uso de un salón de “Chat” o páginas del Internet que vayan en contra de la moral o propósitos relacionados con el negocio de Comware S.A, será sancionada de acuerdo con el reglamento interno de compañía.

[24]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

- No se podrán bajar archivos de música, videos o cualquier otro archivo cuya finalidad no esté relacionada al giro del negocio de Comware S.A http://iso.comware.com.ec/docmanager/docmanag.nsf. Si es necesario bajarse un archivo de un proveedor que se encuentre en la "Lista de proveedores aprobados" R-LOG-01, por ser de utilidad para resolver un problema en un cliente, se lo realizará de preferencia en horas no laborables, para no interrumpir las actividades normales de la compañía.
- No se debe utilizar la infraestructura de COMWARE S.A. para perpetrar cualquier forma de fraude electrónico, hacking, propagación de virus o gusanos, apropiación de información confidencial y violación de la privacidad de las personas.
- No se deben realizar cambios en la configuración inicial de Internet: página de inicio, dirección y/o nombre del proxy y/o puerto por donde se conecta.[25]

Queda prohibido:

- Conectarse a otro servidor proxy que no sea parte de la configuración original realizada por el personal de Sistemas Internos.
- Deshabilitar del navegador el uso del servidor Proxy sin autorización del Jefe de Sistemas Internos.
- Diseminar intencionalmente y con conocimiento de causa: virus, gusanos, troyanos, malware, y otro tipo de programas dañinos para los sistemas de Comware S.A.[26]

Queda prohibido el uso de internet para:

- Visitar sitios con contenido obsceno, lascivo o pornográfico, sitios de entretenimiento, descarga de música, videos, juegos o cualquier otro

[25]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[26]Idem 25

material que no tenga relación con el trabajo que realiza el usuario dentro de la empresa.

- Personas externas que no tengan permiso para utilizar dicho servicio.
- Publicar material que viole las leyes vigentes en el Ecuador, así como derechos de autor, amenazas, material obsceno o información confidencial de propiedad de Comware S.A. que no tenga la debida autorización.
- Activar intencionalmente y con conocimiento de causa: links, por medio de los cuales se ejecute algún tipo de instalador o programa que ponga a la red de COMWARE S.A. bajo la amenaza de algún virus o peligro informático.
- Cualquier uso con fines propagandísticos, comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio.
- Envío de material ofensivo, lascivo, difamatorio o discriminatorio a otros usuarios, perjudicando de esta manera la imagen institucional de Comware S.A.
- Descargar de manera intencional, gran cantidad de información no relacionada con la actividad laboral, que provoque saturación del canal de comunicación externo, afectando las labores cotidianas en la compañía.
- Accesar a estaciones de televisión (streaming de video), estaciones de radio (streaming de audio) y video chat con fines recreacionales.
- Participar en juegos en línea.
- Ejecutar en equipos conectados a la red de la compañía, software de dudosa procedencia, con fines no éticos y que hayan sido descargados desde Internet.
- Descargar software para uso propio ó de terceros, cuyas licencias se encuentren protegidas por las leyes de propiedad intelectual.
- Descargar música, videos, fotos o cualquier otra información que no sea definida dentro del uso laboral.
- Acceso a los salones de conversación “Chat”, que no sea para comunicación con Clientes, Proveedores que se encuentran en el

registro "Lista de proveedores aprobados" R-LOG-01, o compañeros de sucursales, siempre y cuando las conversaciones estén relacionadas con actividades del negocio de Comware S.A.

- El área de Sistemas Internos será la responsable de bloquear el acceso a sitios y descarga de archivos no permitidos de acuerdo a lo estipulado en esta política y comunicará cualquier hallazgo a Recursos Humanos.[27]

1.5.3.2 SANCIONES

Toda persona que sea sorprendida o monitoreada infringiendo esta política será sancionada de acuerdo con el reglamento interno de Comware S.A.[28]

[27]Comware, “Políticas”, 2012-02-09, http://iso.comware.com.ec/docmanager/docmanag.nsf

[28]Idem 27

CAPÍTULO II

MARCO TEÓRICO

2.1 PRESENTACIÓN

En este capítulo, se detallará los fundamentos teóricos de las redes, sus ámbitos de aplicación; los conceptos de seguridad para la información de la red, sus vulnerabilidades, los ataques y amenazas a los que se encuentra expuesta; las herramientas para determinar las mismas. Además se explicará el Sistema de gestión de seguridad de la Información (SGSI) sus requisitos y documentación; y su metodología para el análisis y evaluación del riesgo.

2.1.1 DESCRIPCIÓN Y FUNCIONAMIENTO BÁSICO DE LAS REDES

"Una red de computadoras, […] es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos."[29]

2.1.1.1 CÓMO FUNCIONA UNA RED

A continuación se describe el funcionamiento de una red informática, basándonos en el sitio web: http://joan004.tripod.com/clatop.htm, ya que las pruebas de vulnerabilidad que se realizaran para la presente tesis se harán dentro de la red de Comware.

"Se puede pensar por un momento en el servicio de correo, […]del tiempo la carta devolverá al origen por los mismos cauces que llegó al supuesto destino."[30]

> Más o menos, esta es la forma en que funciona una red: la carta escrita es la información que se quiere transmitir; el sobre y sello es el paquete con el formato impuesto por el protocolo que se utiliza en la transmisión;

[29]WIKIPEDIA, "Red De Computadoras", 2012-09-02, http://es.wikipedia.org/wiki/Red_de_computadoras
[30]TRIPOD, "Cómo funciona una Red", 2012-09-03, http://joan004.tripod.com/clatop.htm

la dirección del destinatario es la dirección del nodo destino y la dirección del remitente, será la dirección del nodo origen, los medios de transporte que llevan la carta cerca del destino es el medio de transmisión (cable coaxial, fibra óptica); las normas del servicio de correos, carteros y demás personal son los protocolos de comunicaciones establecidos.[…].

Si se supone que se está utilizando el modelo OSI de la ISO. Este modelo tiene 7 niveles, es como decir que la carta escrita pasa por 7 filtros diferentes (trabajadores con diferentes cargos) desde que la ponemos en el buzón hasta que llega al destino. Cada nivel de esta torre se encarga de realizar funciones diferentes en la información a transmitir. Cada nivel por el que pasa la información a transmitir que se ha insertado en un paquete, añade información de control, que el mismo nivel en el nodo destino irá eliminando. Además se encarga de cosas muy distintas: desde el control de errores, hasta la reorganización de la información transmitida cuando esta se ha fragmentado en tramas.[…].

Si la información va dirigida a una red diferente (otra ciudad en el caso de la carta), la trama debe llegar a un dispositivo de interconexión de redes (router[31], gateway[32], bridges[33]), que decidirá, dependiendo de su capacidad, el camino que debe seguir la trama. Por eso es imprescindible que el paquete lleve la dirección destino y que esta contenga, además de la dirección que identifica al nodo, la dirección que identifica la red a la que pertenece el nodo.[34]

2.1.2 TOPOLOGÍA DE UNA RED

"La topología de una red define únicamente la distribución del cable que interconecta los diferentes computadores, es decir, es el mapa de distribución del cable que forma la Intranet."[35]

[31]Router: también conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.
[32]Gateway: Una pasarela o puerta de enlace (del inglés gateway) es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.
[33]BridgesUn puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.
[34]TRIPOD, "Cómo funciona una Red", 2012-09-03, http://joan004.tripod.com/clatop.htm
[35]Idem 34

Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El costo que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una Intranet teniendo en cuenta la escalabilidad.[36]

2.1.2.1 TOPOLOGÍA FÍSICA

"Es [...] la forma en la que el cableado se realiza en una red. Existen tres topologías físicas puras:

- Topología en anillo.
- Topología en bus.
- Topología en estrella."[37]

2.1.2.2 TOPOLOGÍA EN BUS

"Consta de un único cable que se extiende de un computador al siguiente de un modo serie. […] Fácil de instalar y mantener.[…] Si se rompe el cable en algún punto, la red queda inoperativa por completo."[38]

[36]TRIPOD, "Cómo funciona una Red", 2012-09-03, http://joan004.tripod.com/clatop.htm
[37]Idem 36
[38]Idem 36

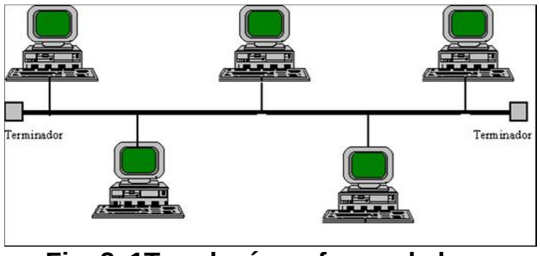


Fig. 2. 1Topología en forma de bus.
Fuente: http://joan004.tripod.com/clatop.htm

2.1.2.3 TOPOLOGÍA EN ANILLO

"[…] El cable forma un bucle cerrado formando un anillo.
Todos los computadores que forman parte de la red se conectan a ese anillo. […]Si se rompe el cable que forma el anillo se paraliza toda la red.
Es difícil de instalar."[39]

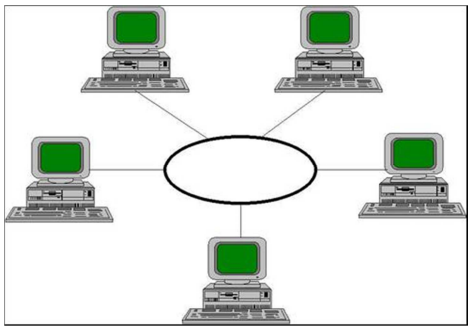


Fig. 2. 2 Topología en forma de anillo
Fuente: http://joan004.tripod.com/clatop.htm

2.1.2.4TOPOLOGÍA EN ESTRELLA

"[…] Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física. […] Existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.Es fácil de detectar y de localizar un problema en la red."[40]

[39]TRIPOD, "Cómo funciona una Red", 2012-09-03, http://joan004.tripod.com/clatop.htm
[40]Idem 39

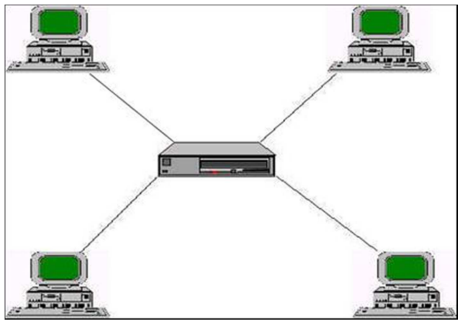


Fig. 2. 3 Topología en forma de estrella

Fuente: http://joan004.tripod.com/clatop.htm

2.1.3 ÁMBITOS DE APLICACIÓN DE LAS REDES

El remplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de redes de computadores, veremos ahora brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido. Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver cómo pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente o necesita de una máquina muy grande para correrlo. […].

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a un computador remoto mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio más bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuando se están transmitiendo los

datos. Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (INTERNET). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.[41]

2.2 CONCEPTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN EN LA RED

2.2.1 INTRODUCCIÓN

"La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta […]. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. […]."[42]

2.2.2 VULNERABILIDADES, AMENAZAS Y ATAQUES

Por vulnerabilidad se entiende la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus[43], códigos maliciosos[44], gusanos[45], caballos de troya[46] y hackers[47]; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas

[41]MONOGRAFIAS.COM, ¿Qué es una Red?, 2012-09-03,http://www.monografias.com/trabajos82/que-es-red/que-es-red.shtml
[42]WIKIPEDIA, Seguridad Informática, 2012-09-03, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
[43]Virus: Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.
[44]Códigos maliciosos:En seguridad informática, código malicioso es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.
[45]Gusanos:Otro tipo de código malicioso son los gusanos. Primos hermanos de los virus, su principal misión es reproducirse y extenderse al mayor número de ordenadores posibles.
[46]Caballos de Troya: Un troyano era en sus comienzos, un programa que camuflado dentro de otro (de ahí el nombre, asociado al caballo que los griegos utilizaron para ganar su guerra contra Troya) para conseguir que un usuario de un ordenador lo ejecutara pensando que en realidad estaba ejecutando un programa lícito.
[47]Hacker es una persona que (burla la seguridad para dañar sistemas, archivos, robas cuentas, contraseñas y demás).

deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos. […].

Específicamente, en los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el Web Site de la compañía. Con ello, es evidente que los riesgos están en la red, no en la PC. […].

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo. […].

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos. […].

Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible)
- Establecer niveles de prioridad e importancia sobre esta información
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger. […].

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional (firewalls[48], autenticación[49], antivirus[50], controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros), y no únicamente tecnología.[51]

2.3.- HERRAMIENTAS DE ESCANEO

2.3.1.- CARACTERÍSTICAS

"Muchas empresas sólo realizan el escaneo de vulnerabilidades para los periodos de las famosas auditoria seguridad informáticas […].Para organizaciones muy grandes, es importante realizar el escaneo de vulnerabilidades como parte del análisis de seguridad regular con una mayor cantidad de escaneos, mucho más frecuente […]."[52]

2.3.2 PUNTOS DÉBILES

"[…] Cada nueva actualización que se le haga al sistema trae consigo el potencial para generar nuevas vulnerabilidades por otros puntos del sistema o red. Y mientras estas vulnerabilidades son encontradas por los diversos equipos que se dedican a esto, […], los hackers […] reciben estos informes

[48]Firewalls: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
[49]Autenticación o autentificación es el acto de establecimiento o confirmación de algo (o alguien) como auténtico.
[50]Antivirus: En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos.
[51]YAGUARETE, Amenazas, 2012-09-03, http://www.yaguarete-sec.com/the-news/49-amenazas.html
[52]VULNERABILITYTEAM, Guía Esencial para el Escaneo de Vulnerabilidades, 2012-09-03, http://vulnerabilityteam.wordpress.com/contenidos/guia-escencial-para-el-escaneo-de-vulnerabilidades/

(por medio de IRC[53], foros undergrounds[54]) para generar invasiones tan rápido como puedan […], creando nuevas vulnerabilidades continuamente."[55]

2.3.3 APLICACIONES TÍPICAS

2.3.3.1 TIPOS DE ESCÁNER

A continuación, se describirá una serie de escáneres de vulnerabilidades que pueden ser utilizados por las empresas para encontrar los puntos débiles y así mitigar los riesgos:

- **Escáner de Red:** escáner de uso general usado para encontrar vulnerabilidades potenciales en la red de la empresa. (También se podría incluir a los escáneres de redes VoIP)
- **Escáner de Puerto:** software diseñado para buscar en una red los puertos abiertos que podrían ser usados por los atacantes como puntos de entrada.
- **Escáner para la Seguridad de aplicaciones web:** Permite a los negocios realizar evaluaciones de riesgo para identificar las vulnerabilidades en aplicaciones web y así evitar ataques. Este tipo de escáneres deberían ser utilizados también por el departamento de desarrollo (programación) de una aplicación web, ayudando así a encontrar todos los bugs que puedan generarse durante la creación de la aplicación, antes de poner la aplicación a un entorno de producción.
- **Escáner de Base de datos:** permite encontrar puntos débiles en bases de datos, protegiendo así el activo más importante de una empresa.[56]

[53]IRC (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas.
[54]Foros undergrounds: Foro en Internet es una aplicación web que da soporte a discusiones u opiniones en línea, permitiendo al usuario poder expresar su idea o comentario respecto al tema tratado.
[55]Idem 36
[56]VULNERABILITYTEAM, Guia Escencial para el Escaneo de Vulnerabilidades, 2012-09-03, http://vulnerabilityteam.wordpress.com/contenidos/guia-escencial-para-el-escaneo-de-vulnerabilidades/

2.3.4 ENTORNOS DE TRABAJO

2.3.4.1 ESCÁNERES

Estos son ejemplos de algunas herramientas que actualmente son muy utilizadas por los administradores de redes y encargados de seguridad:

- **Acunetix Web Vulnerability Scanner:** Este software incluye un escáner de seguridad Web, una consola para el análisis de informes y una base de datos para gestionar todas las plataformas principales del servidor web.
- **GFI LANguard Network Security scanner:** Esta solución incluye la exploración de vulnerabilidades de red y también sirve para realizar auditorías informáticas de seguridad.
- **TenebleNessus 3**: Compatible con varios tipos de Unix, este producto ejecuta más de 900 comprobaciones de seguridad y sugiere soluciones para los problemas encontrados (open source)
- **Nmap**: es un escáner de puerto utilizado para la exploración de la red o la revisión de seguridad (open source)
- **Retina Network Security Scanner:**Su distribuidor es la firma eEye Digital Security Inc. Afirman que su escáner de vulnerabilidad descubre tanto las vulnerabilidades conocidas como las vulnerabilidades denominadas “zerodays”. El producto también proporciona la opción de realizar análisis de riesgos basados en la seguridad ayudando a la empresa a ejecutar y poner las mejores prácticas, ayuda a reforzar las políticas y a manejar las auditorias.
- **SAINT Network Vulnerability Scanner:** Este escáner de vulnerabilidad de red está integrado con un sistema para realizar pruebas de penetración (pentest) permitiendo así al usuario a explotar las vulnerabilidades encontradas.
- **WATCHFIRE RATIONAL APPSCAN:**escáner de IBM utilizado para aplicaciones web.

- **ISS Internet Scanner:** escáner de vulnerabilidades de red de la compañía IBM.[57]

2.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

A continuación se describe al SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), basándonos en el sitio web: http://www.iso27000.es/sgsi.html, ya que será esta la guía para desarrollar el diseño de nuestro sistema de gestión de seguridad.

2.4.1 INTRODUCCIÓN

"El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.
La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.[…]"[58]

2.4.1.1 ¿QUÉ ES UN SGSI?

"SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. […], se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita […]."[59]

[57]VULNERABILITYTEAM, Guia Escencial para el Escaneo de Vulnerabilidades, 2012-09-03, http://vulnerabilityteam.wordpress.com/contenidos/guia-escencial-para-el-escaneo-de-vulnerabilidades/
[58]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[59]Idem 58

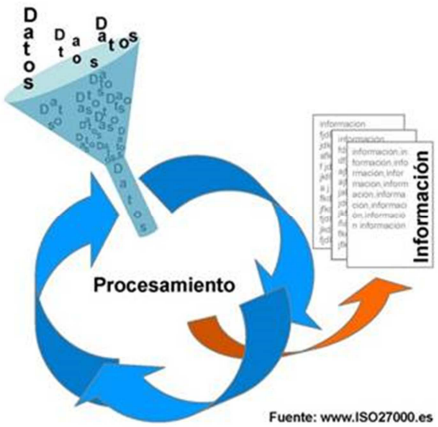


Fig. 2. 4 SGSI
Fuente: www.iso27000.es

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, […]:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.[…].[60]

2.4.1.2 ¿PARA QUÉ SIRVE UN SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. […] Sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que […] pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o

[60]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. […].[61]

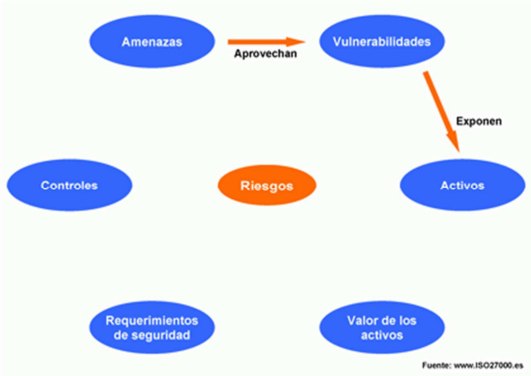


Fig. 2. 5 SGSI
Fuente: www.iso27000.es

[…] El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.[62]

2.4.1.3 ¿QUÉ INCLUYE UN SGSI?

"En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. […] de la siguiente forma:"[63]

[61]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[62]Idem 61
[63]Idem 61

Fig. 2. 6 SGSI
Fuente: www.iso27000.es

2.4.2 REQUISITOS DE LA DOCUMENTACIÓN DEL SGSI

Documentos de Nivel 1

"Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. […] el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI."[64]

Documentos de Nivel 2

"Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información."[65]

Documentos de Nivel 3

"Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información."[66]

[64] ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[65] Idem 64
[66] Idem 64

Documentos de Nivel 4

"Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos."[67]

2.4.3 CONTROL DE DOCUMENTOS

2.4.3.1 CONTROL DE LA DOCUMENTACIÓN

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.

[67]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.[68]

2.4.3.2 ¿CÓMO SE IMPLEMENTA UN SGSI?

"Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA[69], tradicional en los sistemas de gestión de la calidad."[70]

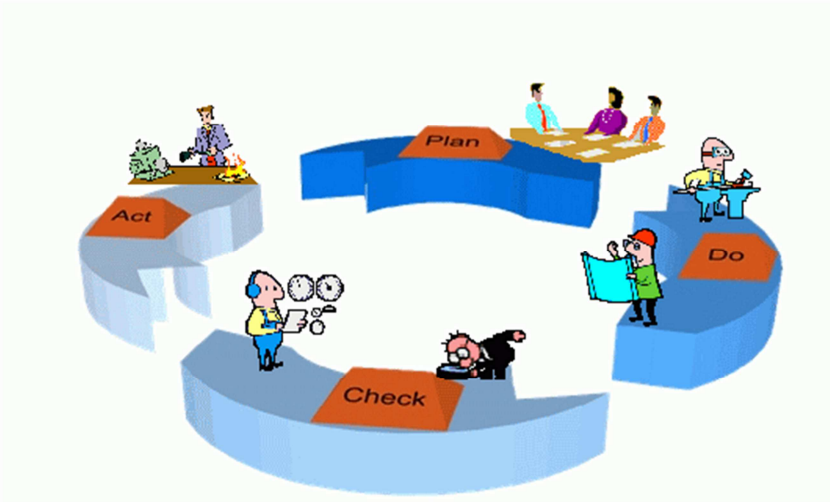


Fig. 2. 7 SGSI
Fuente: www.iso27000.es

"Plan (planificar): establecer el SGSI.
Do (hacer): implementar y utilizar el SGSI.
Check (verificar): monitorizar y revisar el SGSI.
Act (actuar): mantener y mejorar el SGSI."[71]

Plan: Establecer el SGSI

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. […].

[68]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[69]PDCA: El ciclo PDCA, también conocido como "Círculo de Deming o circulo de Gabo" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.
[70]Idem 68
[71]Ídem 68

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia). […].

Analizar y evaluar los riesgos. […].

Identificar y evaluar las distintas opciones de tratamiento de los riesgos.

Definir una declaración de aplicabilidad que incluya […] Los objetivos de control y controles seleccionados.[…].[72]

Fig. 2. 8 SGSI
Fuente: www.iso27000.es

2.4.3.2.1 DO: IMPLEMENTAR Y UTILIZAR EL SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

[72]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.[73]

2.4.3.2.2 CHECK: MONITORIZAR Y REVISAR EL SGSI

Se deberá ejecutar procedimientos de monitorización y revisión para:

Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;

Identificar brechas e incidentes de seguridad;

Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de

[73]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.

Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.[74]

2.4.3.2.3 ACT: MANTENER Y MEJORAR EL SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

[74]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.[75]

2.4.4 RESPONSABILIDADES DE ADMINISTRACIÓN

2.4.4.1 ¿QUÉ TAREAS TIENE LA GERENCIA EN UN SGSI?

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección. […].[76]

2.4.4.1.1 COMPROMISO DE LA DIRECCIÓN

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.

[75]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[76]Idem 75

- Realizar revisiones del SGSI, como se detalla más adelante.[77]

2.4.4.1.2 ASIGNACIÓN DE RECURSOS

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.[78]

2.4.4.1.3 FORMACIÓN Y CONCIENCIACIÓN

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe […]:

- Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.
- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de estudios, formación, habilidades, experiencia y cualificación.[79]

[77]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html
[78]Idem 77
[79]Idem 77

2.4.4.1.4 REVISIÓN DEL SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora. […].[80]

2.4.4.2 ¿SE INTEGRA UN SGSI CON OTROS SISTEMAS DE GESTIÓN?

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio-ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS[81] 18001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

[80]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

[81]OHSAS 18001: OHSAS (Occupational Health and Safety Assessment Series). OHSAS 18001 (OccupationalHealth and Safety Assessment Series, Sistemas de Gestión de Salud y Seguridad Laboral)

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último debería ser llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA de mejora continua común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos.[82]

2.5 HERRAMIENTAS A SER UTILIZADAS

Paracomprobar el ingreso no autorizado a la red procederemos a analizar algunas herramientas para saber que herramienta es la más factible para utilizarse.

2.5.1 AIRCRACK-NG

Es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador[83] de redes WEP[84] y WPA/WPA2-PSK[85] y otro conjunto de herramientas de auditoría inalámbrica. […].

Esta suite está diseñada para trabajar con tarjetas inalámbricas con circuitos integradosAtheros[86] y con algunas con circuitos Railink[87] sin necesidad de configurarlas. [88]

---

se refiere a una serie de especificaciones sobre la salud y seguridad en el trabajo, materializadas por BSI (British StandardsInstitution) en la OHSAS 18001 y OHSAS 18002.

[82]ISO27000.ES, Sistema de Gestión de la Seguridad de la Información, 2012-09-03, http://www.iso27000.es/sgsi.html

[83]Un crack informático es un parche cuya finalidad es la de modificar el comportamiento del software original y creado sin autorización del desarrollador del programa.

[84]WEP: Abreviatura de WiredEquivalentPrivacy, un protocolo de seguridad para redes inalámbricas de área local inalámbricas (WLAN) definido en el estándar 802.11b.

[85]WPA/WPA2-PSK: WPA, abreviatura de Wi-Fi® Protected Access, es una especificación de codificación de data para un LAN inalámbrica. Mejora con la función de seguridad de WEP utilizando Extensible AuthenticationProtocol (EAP) a un acceso de network seguro y un método de codificaión para asegurar la transmisión de datos.

[86]Atheros: Tarjeta de red, no necesariamente tiene que ser la inalámbrica.

[87]Railink: RalinkTechnology, Corp. es un fabricante de chips Wi-Fi, que es conocido principalmente por sus conjuntos de chips WLAN.

[88]WIKIPEDIA, Aircrack-ng, 2012-09-03, http://es.wikipedia.org/wiki/Aircrack-ng.

2.5.2 BACKTRACK

"Es una distribuciónGNU/Linux[89] en formato LiveCD[90] pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.[…]."[91]

2.5.3 NESSUS

"Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd[92], el daemon[93]Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos.[…]."[94]

2.5.4 NMAP

"Mapeador de redes es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios.[…]."[95]

2.5.5 OPENVAS

"Es un escaner de vulnerabilidades en redes, servidores y aplicaciones. Destaca su integración con otras herramientas de seguridad y la posibilidad de desarrollar plugins y networkvulnerabilitytests (NVTs)[96]. OpenVAS Manager se

[89]GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux, que es usado con herramientas de sistema GNU.
[90]LiveCD Una distribución live o Live CD o Live DVD, más genéricamente Live Distro, traducido en ocasiones como CD vivo o CD autónomo, es un sistema operativo almacenado en un medio extraíble.
[91]WIKIPEDIA, BackTrack, 2012-09-03, http://es.wikipedia.org/wiki/Backtrack.
[92]Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.
[93]Un demonio, daemon o dæmon (de sus siglas en inglés Disk And ExecutionMONitor), es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario.
[94]WIKIPEDIA, Nessus, 2012-09-03, http://es.wikipedia.org/wiki/Nessus.
[95]NMPA.ORG, Nmap, 2012-09-03, http://nmap.org/man/es/.
[96](NVTs) Una evaluación de la vulnerabilidad de la red evalúa todos sus sistemas, ya que se ven de forma remota a través de Internet sobre una base diaria, semanal o mensual.

situa en una capa intermedia entre el servidor de OpenVAS (denominado OpenVAS Scanner) y los clientes de OpenVAS."[…].[97]

2.5.6 LANGUARD NETWORK SECURITY SCANNER

"Es una aplicación con la que se podrá analizar el computador, y los diferentes computadores que componen la red en busca de diferentes malware que podrían llegar a causar efectos catastróficos si no son tratados a tiempo, realiza profundos escaneos del sistema, los cuales permitirán analizar y detectar si algún malware se encuentra instalado en la red. "[98]

Dentro del listado presentado anteriormente se procederá a utilizar la herramienta BackTrack[99] 3, debido a que es una herramienta completa que contiene diversas herramientas dentro del sistema operativo, las aplicaciones que se utilizarán dentro de Back Track 3 son: Nmap, para poder realizar el correcto escaneo de puertos y de esta manera saber si existen servidores que se encuentren con puertos como telnet abiertos debido a que será un punto de vulnerabilidad muy alto dentro de la red empresarial; La otra herramienta a utilizarse será GFI LanGuard[100], esta herramienta de seguridad permitirá poder realizar un escaneo completo de la red viendo de manera gráfica cada uno de los computadores que se encuentran dentro de la red con su respectiva descripción de que se encuentra en cada uno de ellos.

2.5.7 ZENMAP

"Zenmap[101] es el oficial de Nmap Security Scanner interfaz gráfica de usuario. Se trata de una plataforma multilenguaje (Linux[102], Windows[103], Mac

[97]WIKIPEDIA, OpenVAS, 2012-09-03, http://es.wikipedia.org/wiki/OpenVAS.
[98]GFI, GFI Languard, 2012-09-03, http://www.gfi.com/network-security-vulnerability-scanner.
[99]BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.
[100]GFI LANguard es una seguridad de red galardonado escáner de vulnerabilidad utilizado por las empresas pequeñas y medianas empresas (pymes) de todo el mundo.
[101]Zenmap es el oficial de Nmap Security Scanner interfaz gráfica de usuario. Se trata de una plataforma multi-(Linux, Windows, Mac OS X, BSD, etc).
[102]Linux es un núcleo libre de sistema operativo basado en Unix.

OS X[104], BSD[105], etc) la aplicación gratuita y de código abierto que tiene como objetivo hacer Nmap fácil de usar para principiantes mientras que proporciona características avanzadas para usuarios experimentados de Nmap."[…].[106]

2.6 METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DEL RIESGO

El principal objetivo de la metodología de evaluación de riesgos es mejorar la objetividad y transparencia, y ofrecer bases sólidas para la evaluación de las necesidades por lo cual, a continuación, se presentan varios métodos de análisis de riesgos para obtener el mejor método.

- MAGERIT 2.0 (España)
- AS 4360 (Australia)
- NIST SO 800-30 (USA)
- EBIOS (Francia)
- OCTAVE (Cert)
- ISO 13335-1:2004
- ISO73

2.6.1 MAGERIT 2.0

> Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos […].
>
> Magerit persigue los siguientes objetivos:
>
> 1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo
> 2. Ofrecer un método sistemático para analizar tales riesgos
> 3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control

[103]Microsoft Windows es el nombre de una familia de sistemas operativos desarrollados por Microsoft desde 1981, año en que el proyecto se denominaba «Interface Manager».
[104]Mac OS X es un sistema operativo desarrollado y comercializado por Apple Inc. que ha sido incluido en su gama de computadoras Macintosh desde 2002.
[105]Berkeley Software Distribution o BSD (en español, "distribución de software berkeley") es un sistema operativo derivado del sistema Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.
[106]NMPA.ORG, Nmap, 2012-09-03, http://nmap.org/zenmap/

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.[107]

2.6.2 AS 4360

Este Estándar provee una guía genérica para el establecimiento e implementación del proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos. […]. Este Estándar puede ser aplicado a todas las etapas de la vida de una actividad, función, proyecto, producto o activo. [...].[108]

2.6.3 NIST SO 800-30

[…] Un proceso de gestión de riesgos efectiva es un componente importante de la seguridad de TI con. El objetivo principal del proceso de una organización de gestión del riesgo debería ser la protección de la organización y su capacidad para llevar a cabo su misión, no sólo sus activos de TI. Por lo tanto, el riesgo de gestión no debe ser entendido principalmente como una función técnica llevada a cabo por los expertos de TI que operan para administran el sistema de TI, sino como una función esencial de la administración de la organización.[109]

2.6.4 EBIOS

EBIOS (en francés: Expresión des besoins et des objectifs la identificación de sécurité)[…].

Los 5 pasos del método EBIOS son: estudio circunstancial, los requisitos de seguridad, estudio de riesgo, la identificación de los

[107]EAR / PILAR, Entorno de Análisis de Riesgos, 2012-09-03,https://www.ccn-cert.cni.es/publico/herramientas/pilar43/magerit/index.html
[108]IMF CONSULTING, Estándares, 2012-09-03, www.imfperu.com/.../standard__adm_risk_as_nzs_4360_1999.pdf
[109]NIST, Risk Management Guide for Information Technology Systems, 2012-09-03, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

objetivos de seguridad, y la determinación de los requisitos de seguridad.

[…]. En su primera versión, EBIOS se centró en la "seguridad redacción objetivos". Desde el año 2000, la DCSSI se dio cuenta de las normas internacionales (ISO, en particular) y los aumentos "que participan de adaptación EBIOS a este criterio". También se puede percibir como una forma de evitar el confinamiento de Francia en seguridad de la información, e incurrió en riesgos con el uso de métodos franceses que no son reconocidos en el extranjero e inadecuado a los estándares internacionales.[110]

2.6.5 OCTAVE

Operationally Critical Threats Assets and Vulnerability Evaluation. Es un método de evaluación y de gestión de los riesgos para garantizar la seguridad del sistema informativo, desarrollado por el estándar internacional ISO270001. […].

- Desmitificar la falsa creencia: La Seguridad Informática es un asunto meramente técnico.
- Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos. […].[111]

2.6.6 CUALITATIVO

La recomendación es usar un método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con mayor facilidad. Dentro de los objetivos de dicho método se tiene:

Cada activo debemos identificar todas las amenazas existentes

La posibilidad de ocurrencia de estas amenazas

Las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad.

[110]ENISA, Ebios, 2012-09-03,http://rm-inv.enisa.europa.eu/methods_tools/t_ebios.html

[111]WordPress, Seguridades en Redes de Computadores, 2012-09-03, http://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/

El método cuantitativo exigiría que todo sea llevado a valor monetario y en la mayoría de los casos esta tarea es complicada y/o tarda demasiado, puesto que no sólo implica el valor comercial de los activos sino también de la afectación que pueden tener su entorno. El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la mayor de posibilidad de amenaza.

CAPÍTULO III

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA, APLICANDO LA NORMA ISO/IEC 27001.

3.1 PRESENTACIÓN

En este capítulo, se mostrará mediante cada uno de los ítems cuales serían los pasos a seguir para diseñar o implementar un SGSI aplicando la Norma ISO/IEC 27001, la forma de medir los riesgos, así como la metodología de implementación, selección de controles y demás haciendo referencia a puntos clave de la norma, estableciendo una guía el momento que se requiera implementar y certificarse en la norma ISO/IEC 27001.

De igual manera, se realizara el análisis del riesgo y vulnerabilidades dentro de la red por medio de herramientas (software), de esta manera se podrá tener una visión general de puntos que pueden ser afectados dentro de la seguridad de la red en los diferentes servidores de alta criticidad en la empresa.

3.2 IMPLEMENTACIÓN DEL SGSI

El ciclo metodológico para la implantación de un sistema de gestión de seguridad de la información ISO 27001:2005 comienza con el entendimiento de los requerimientos del modelo como se muestra en la siguiente figura.

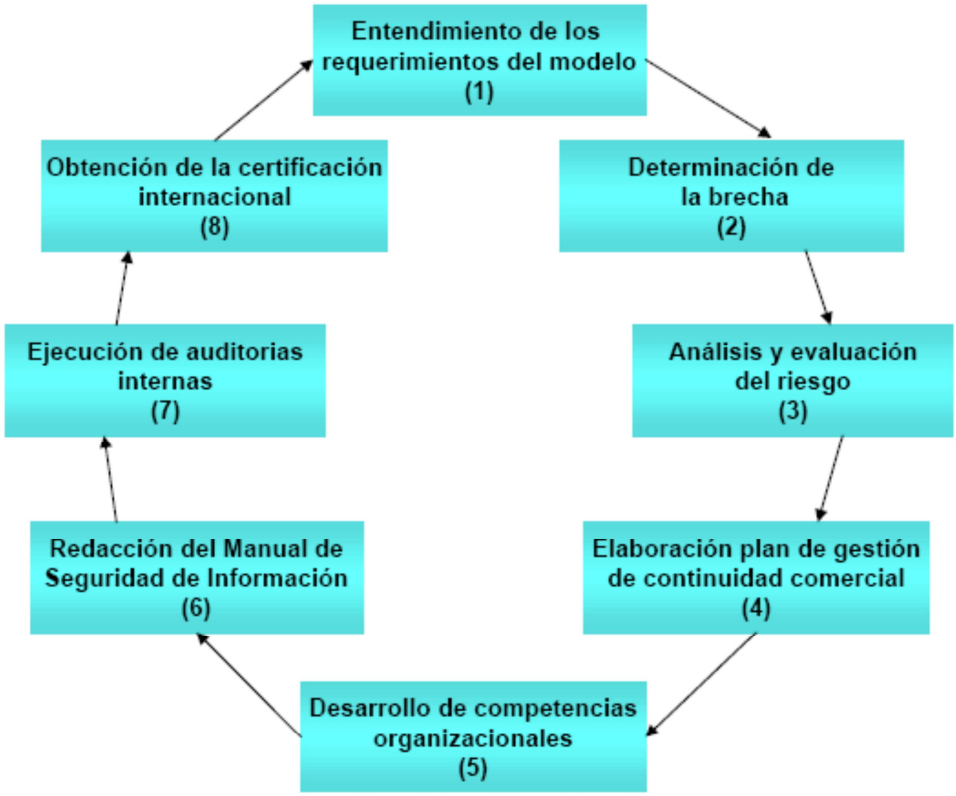


Fig. 3. 1 Ciclo Metodológico de implantación ISO 27001:2005.
Fuente: Los autores

Teniendo como primer paso el Entendimiento de los requerimientos de la Organización; en donde se procede a analizar que requerimientos son necesarios para el funcionamiento de la norma; segundo paso Determinación del alcance; en este paso se definirá cual será nuestro alcance; tercer paso Análisis y evaluación del riesgo; al determinar las diversas amenazas, vulnerabilidades e impactos se tendrá que efectuar el análisis adecuado para realizar la correcta elección de controles; cuarto paso Plan de gestión de continuidad comercial; enfoque para tratar el riesgo y utilización del Anexo A[112] de la norma; quinto paso Desarrollo de competencias organizacionales; es la elaboración del plan del tratamiento del riesgo y determinar la efectividad de dichos controles; sexto paso Redacción de la propuesta para establecer el SGSI; en donde estará establecido de una forma ordenada el manual a ser tomado en cuenta para el

[112]ISO27000, ISO 27000, 2012-09-03, http://www.iso27000.es/download/doc_iso27000_all.pdf

correcto funcionamiento del SGSI, los pasos siete Ejecución de Auditorías internas y ocho obtención de la certificación internacional; son omitidos debido a que solo se realizará el diseño y desarrollo más no la implementación de la norma. A continuación, se redacta la metodología sistemática detallada para implantar SGSI ISO27001:2005 cuya secuencia de redacción corresponde a una cronología real dentro de nuestro escenario empresarial, una empresa integradora de servicios y comunicaciones.

3.3 ESTABLECER Y MANEJAR EL SGSI

A continuación se procede a desarrollar el diseño del SGSI tomando en cuenta cada uno de los puntos establecidos por la Norma ISO 27001, en primera instancia se realiza la referencia textual de lo descrito en la norma para proceder con el desarrollo de cada punto establecido dentro de la misma.

3.3.1 ESTABLECER EL SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.

Basándose en la premisa anteriormente expuesta se procede a establecer el alcance, dicho alcance es establecido mediante la coordinación del área de Sistemas Internos de la empresa.

3.3.2 ALCANCE

Establecer un sistema de gestión de seguridad de información, para los procesos de: administración de la información, monitorización de red, aprovisionamiento y mantenimiento de la red de telecomunicaciones en la ciudad de Quito.

b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

1. Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;
2. Tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;
3. Esté alineada con el contexto de la gestión riesgo estratégico de la organización enel cual se dará el establecimiento y mantenimiento del SGSI;
4. Establezca el criterio con el que se evaluará el riesgo
5. Haya sido aprobada por la gerencia.[113]

La política de seguridad de información en esta fase inicial se la define de forma general debido a que por diversas circunstancias como: cambio de infraestructura, compra de nuevos equipos, cambio de personal, etc.; la política puede ser modificada, pero no cambiada el enfoque de hacia dónde se requiere llegar, es por eso que se pueden llegar a omitir algunos de los puntos descritos en el párrafo anterior. Una vez aclarado este punto la política para el Sistema de Gestión de Seguridad de la Información para la empresa ComWare S.A en la ciudad de Quito es la siguiente:

3.3.3 POLÍTICA

"Mantener la seguridad de la información mediante un Sistema de Gestión de Seguridad de la Información basado en la prevención, detección y eliminación de riesgos que puedan atentar contra la disponibilidad, integridad y confidencialidad en la red".

[113]ISO27000, ISO 27000, 2012-09-03, http://www.iso27000.es/download/doc_iso27000_all.pdf

3.3.4 METODOLOGÍA PARA EL CÁLCULO DEL RIESGO

El método que se utiliza es el método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con mayor facilidad, además se puede tener una calificación real en cada uno de los activos puesto que el análisis que el área realice para la tasación de los mismos permitirá lo siguiente:

- En cada activo se identificará todas las amenazas existentes
- La posibilidad de ocurrencia de estas amenazas
- Las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad.

3.3.5 CRITERIO PARA LA ACEPTACIÓN DE LOS RIESGOS

Una vez establecido el método a utilizarse, el criterio a utilizarse para la medición aceptación de los niveles de riesgo es:

- Experiencia y criterio del personal encargado de administrar el área de Sistemas Internos. Este conocimiento es el más importante debido a que son las personas que se encuentran interactuando constantemente con cada uno de los sistemas; por lo cual su opinión y tasación para cada uno de los sistemas es primordial.
- Experiencia de los usuarios que manejan los diferentes sistemas de la empresa.Este criterio permitirá conocer a los administradores de los sistemas informáticos posibles falencias o brechas de seguridad que permitan la intrusión a los sistemas.

Las medidas y/o escalas para establecer la medición de los activos son del uno al cinco, siendo uno el de menor afectación y cinco el de mayor afectación. El valor total máximo permitido para el riesgo, definido por el personal encargado del área de Sistemas Internos de la empresa es de 6.

Medida	Descripción
1	Menor afectación, en caso de ocurrencia no llega a afectar a los procesos ni a los

	sistemas en cuestión, es más bien de prevención y una alerta para saber que ningún sistema es impenetrable, pueden ser mitigados con una acción correctiva inmediatamente.
2	Menor afectación, en caso de ocurrencia no llega a afectar a los procesos ni a los sistemas pero el nivel de ocurrencia o afectación es una alerta para saber que si no se corrige inmediatamente llegará a la afectación a los procesos o sistemas
3	Mediana afectación, en caso de ocurrencia los procesos o sistemas se llegarán a afectar, y si no se toma las medidas adecuadas en el momento de la ocurrencia puede generar un evento y afectación progresiva que impida la continuidad del negocio.
4	Mayor afectación, en caso de ocurrencia los procesos o sistemas se llegarán afectar de tal forma que puede llegar a parar los la continuidad, integridad y disponibilidad de los sistemas.
5	Mayor afectación, en caso de ocurrencia los procesos o sistemas se encontrarán inevitablemente suspendidos hasta que se llegue a encontrar la solución al problema sucitado, esto deberá posteriormente ser justificado por el área de Sistemas Internos justificando el motivo por el cual no fue prevenido.

Tabla 3. 1 Escala medición activos
Fuente: Los autores

3.3.6 IDENTIFICACIÓN DE RIESGOS

Como parte fundamental dentro del desarrollo del SGSI se tiene la identificación de los procesos dentro del área de Sistemas internos para poder clasificarlos, y ´posteriormente continuar con los análisis de amenazas, vulnerabilidades e impactos para cada uno de dichos activos.

3.3.7 PROCESOS

En nuestro caso los procesos involucrados son: administración de la información, monitoreo de red, aprovisionamiento y mantenimiento de la red. Al ser ComWare una empresa que mantiene una identificación de procesos adecuada por medio de un SGS

certificado se puede realizar el levantamiento de procesos sin ningún inconveniente tomando en cuenta el mapa de procesos del SGC presentado a continuación.

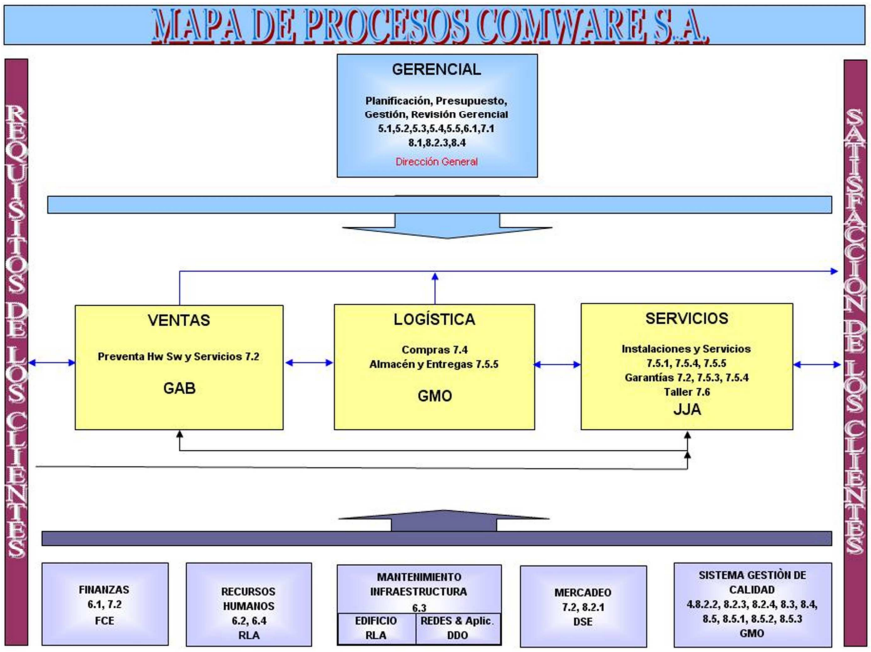


Fig. 3. 2 Mapa de Procesos Comware
Fuente: La Empresa

3.4 IDENTIFICACIÓN DE ACTIVOS INFORMÁTICOS

Los activos de informáticos tomados en cuenta son los siguientes: software, hardware, documentos, personas que utilicen información de valor para el negocio de la organización. A continuación, se presenta una tabla de los activos informáticos que serán evaluados, mostrando en su parte izquierda la descripción general de los activos clasificados en la parte derecha de la tabla.

SOFTWARE	
DESCRIPCIÓN	**ACTIVOS**
Al equipamiento lógico o soporte lógico de un sistema informático; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en	• Antivirus Symantec (Licencias) • Microsoft office (Licencias) • Sac (Licencias)

contraposición a los componentes físicos, que son llamados hardware.	• Evolution • DocManager • JdEdwars • Bases de datos Oracle • Exactus

Tabla 3. 2 SOFTWARE
Fuente: Los autores

HARDWARE	
DESCRIPCIÓN	**ACTIVOS**
Corresponde a todas las partes tangibles de un sistema informáticosus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Sus cables, gabinetes o cajas, periféricosde todo tipo y cualquier otro elemento físico involucrado	• Computadores de escritorio • Laptops • Servidores • Equipos de comunicación producción • Equipos de comunicación laboratorio

Tabla 3. 3 HARDWARE
Fuente: Los autores

SERVICIOS	
DESCRIPCIÓN	**ACTIVOS**
Son todos los servicios que la compañía posee para el correcto funcionamiento de las comunicaciones dentro de la empresa haciéndola funcionar como un todo.	• Correo Electrónico • Telefonía • Enlace de datos con Guayaquil • Página web. • Internet • Active Directory

Tabla 3. 4 SERVICIOS
Fuente: Los autores

PERSONAS	
DESCRIPCIÓN	**ACTIVOS**
Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas.	• Sistemas internos • Logística • Ventas • Talento Humano • Remuneraciones y compensaciones • Financiero

Tabla 3. 5 PERSONAS
Fuente: Los autores

DOCUMENTACIÓN	
DESCRIPCIÓN	**ACTIVOS**
Son todos los documentos que son controlados por la persona encargada de administrar los sistemas.	• Manejo de registros • Informes • Presupuesto

Tabla 3. 6 DOCUMENTACIÓN
Fuente: Los autores

Es importante realizar la clasificación de cada uno de los activos definidos por cada uno de los procesos establecidos y descritos anteriormente, a continuación se presenta una tabla estructurada en donde en su encabezado se muestran los activos y en su parte inferior se encuentra descrito cada uno de ellos identificados en la tabla anteriormente expuesta.

ACTIVOS POR PROCESO		
Proceso	**Activo**	**Descripción**
Administración de la información	Monitorización	Aprovisionamiento y Mantenimiento
Manejo de registros	Correo electrónico	Equipos de escritorio
Informes	Telefonía	Laptops
Presupuestos	Enlace de datos	Equipos de comunicación producción
Sistemas internos	Página web	Equipos de comunicación laboratorio
Logística	Internet	Servidores
Ventas	Antivirus Symantec.	Ups
Talento Humano	Active Directory	
Remuneraciones y compensaciones	Microsoft office	
Financiero	Sac	
	Evolution	
	DocManager	
	JdEdwars	
	Bases de datos Oracle	
	Exactus	

Tabla 3. 7 ACTIVOS POR PROCESO
Fuente: Los autores

3.5 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para poder realizar una correcta identificación de amenazas y vulnerabilidades se procede con las pruebas de análisis en equipos en donde se encuentra funcionando las aplicación de la empresa; esto con el fin de tener una idea general de cómo podrían llegar a penetrar la seguridad irrumpiendo en los sistemas causando daños que pueden afectar a la continuidad del negocio.

Los equipos a ser analizados son los siguientes:

- Máquinas de los usuarios, estas son en una primera instancia las de mayor afectación ya que se encuentran en interacción directa con los sistemas de la empresa en donde una mala manipulación de los mismos puede llegar a causar daños o perdida en la información.
- Segmentos de red de usuarios y de aplicaciones: Para el efecto se realizara el escaneo respectivo lo que permitirá visualizar puertos que se encuentren innecesariamente abiertos en las diversas aplicaciones y en cada uno de los servidores de la empresa. Esto podría ocasionar diversas intrusiones en los sistemas y/o servidores.

En caso que el segmento de red de aplicaciones se encuentre estable se podrá realizar acciones que mejoren el rendimiento en la ejecución de las aplicaciones, por otra parte el segmento de red en donde se encuentran los usuarios es un punto muy importante debido a que existen varias aplicaciones funcionando dependiendo del área en donde se encuentre el usuario, pues las aplicaciones necesarias para el trabajo diario no son los mismos en el área de servicios que el área administrativa, por lo cual tal vez existan aplicaciones con puertos abiertos sin ser utilizados lo que permitiría tener un punto de acceso a todo el segmento de red.

3.6 SOFTWARE Y PRUEBAS

Se inicia el análisis de puertos con el software Nmap.

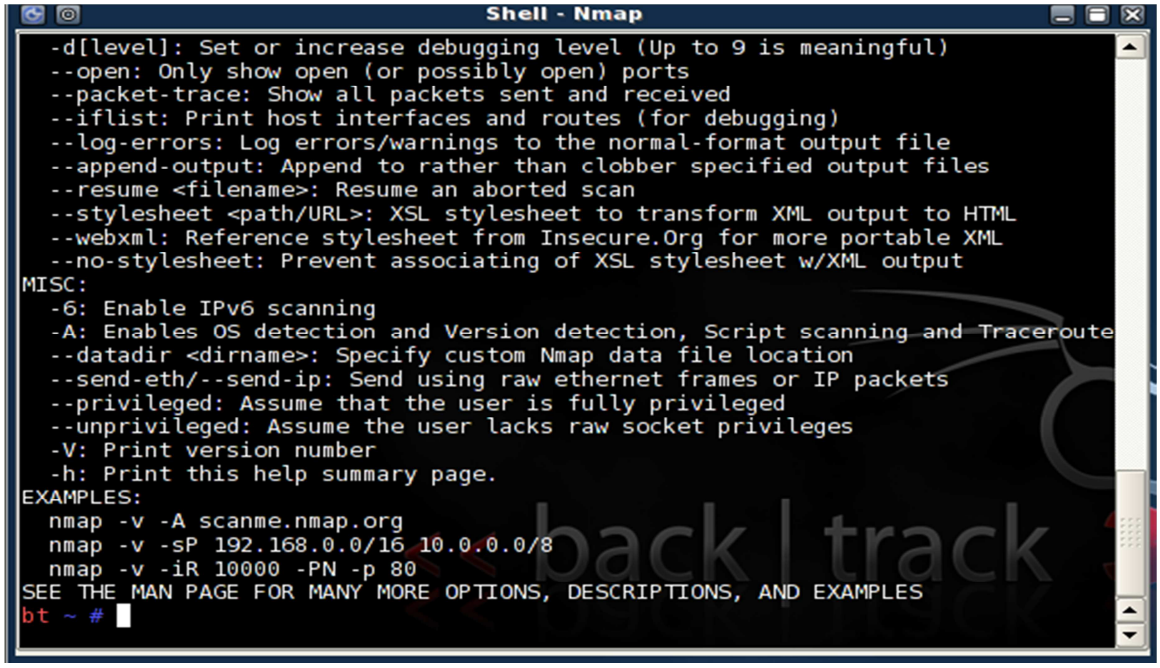


Fig. 3. 3 BackTrack
Fuente: Los autores

3.6.1 USO DE NMAP

Uso: nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}

- DESCUBRIMIENTO DE HOSTS:

-sL: Sondeo de lista - Simplemente lista los objetivos a analizar
-sP: Sondeo Ping - Sólo determina si el objetivo está vivo

- ESPECIFICACIÓN DE PUERTOS Y ORDEN DE ANÁLISIS:

-p <rango de puertos>: Sólo sondear los puertos indicados
Ej: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
-F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services
-r: Analizar los puertos secuencialmente, no al azar.

- DETECCIÓN DE SERVICIO/VERSIÓN:

-sV: Sondear puertos abiertos, para obtener información de servicio/versión

--version-intensity<nivel>: Fijar de 0 (ligero) a 9 (probar todas las sondas)

--version-light: Limitar a las sondas más probables (intensidad 2)

--version-all: Utilizar todas las sondas (intensidad 9)

--version-trace: Presentar actividad detallada del análisis (para depurar)

Para dar inicio al proceso de escaneo con esta herramienta vamos a tomar como ejemplo tres máquinas: la primera una máquina de un usuario X de la empresa.

Nmap empieza el proceso de escaneo de la red dentro del rango establecido anteriormente. Como podemos observar en la siguiente imagen podemos evidenciar que las máquinas responden y aquellas que se encuentran dentro del dominio y/ active directory aparecen con su descripción ejemplo: Host cwuioserv06.comware.prod

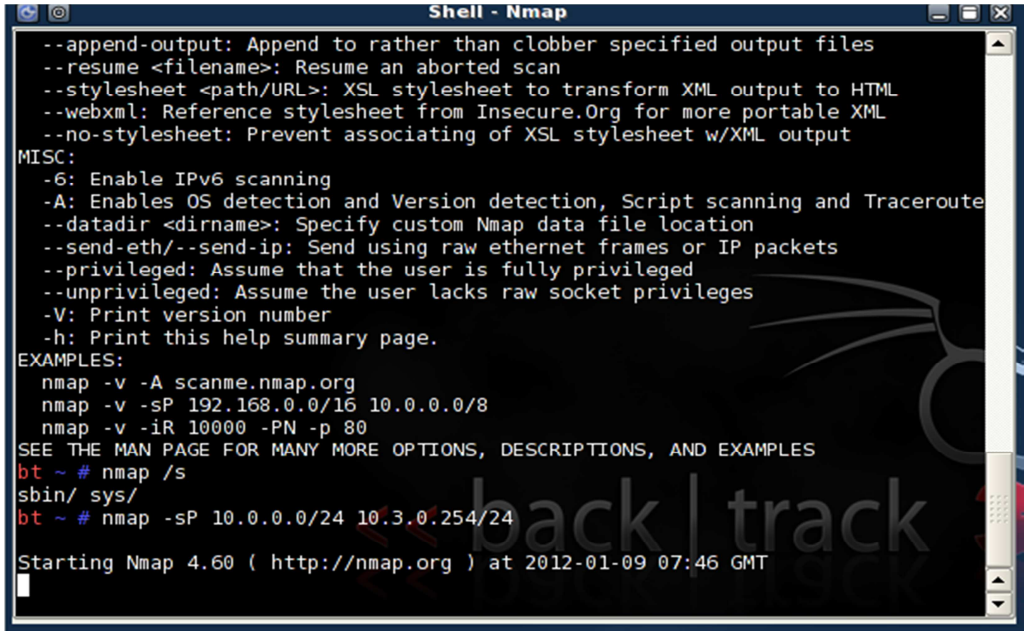


Fig. 3. 4BackTrack – Nmap descubrimiento de red
Fuente: Los autores

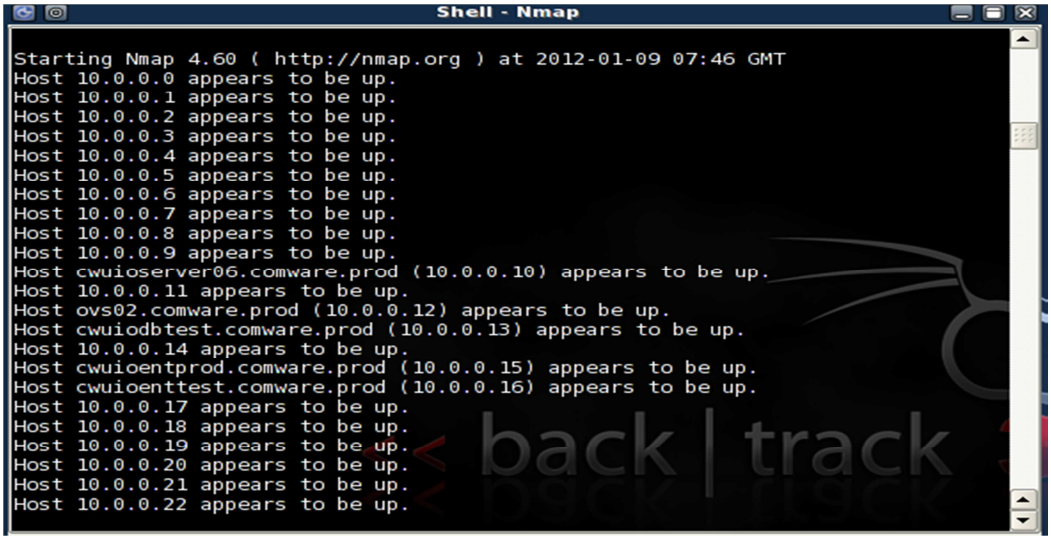


Fig. 3. 5 BackTrack - Dispositivos descubiertos nmap
Fuente: Los autores

En la siguiente imagen, se puede visualizar el rango de host desde el 10.0.0.23 hasta el 10.0.0.47 se encuentran funcionando sin ningún inconveniente.

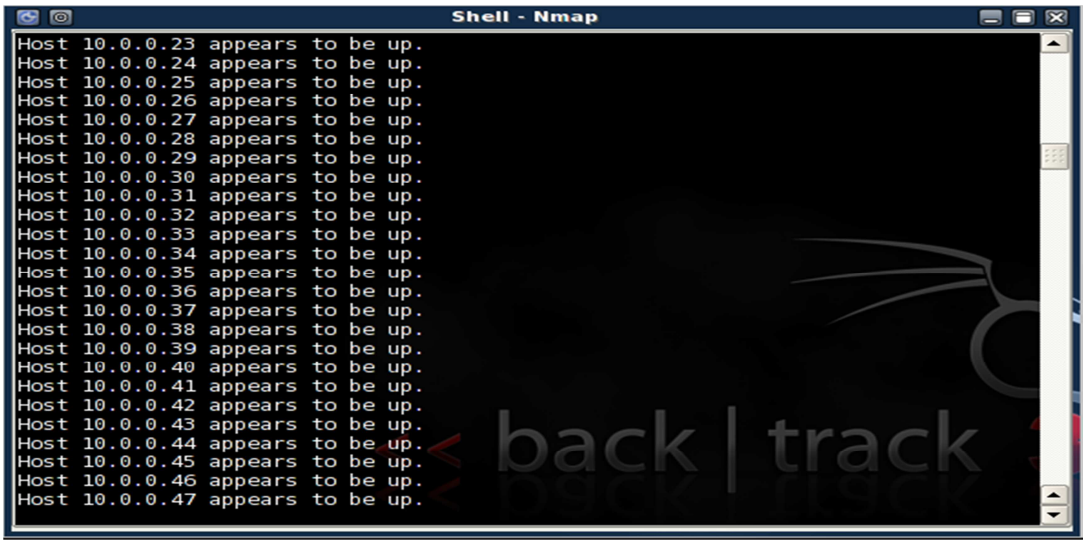


Fig. 3. 6 BackTrack - Dispositivos descubiertos nmap
Fuente: Los autores

Cuando se empieza a ver el segmento de red 10.3.0.0/16, se observa las máquinas dentro del dominio cada una con su respectiva descripción de cada host, esto se ve desde la Figura 3.7 hasta la Figura 3.12.

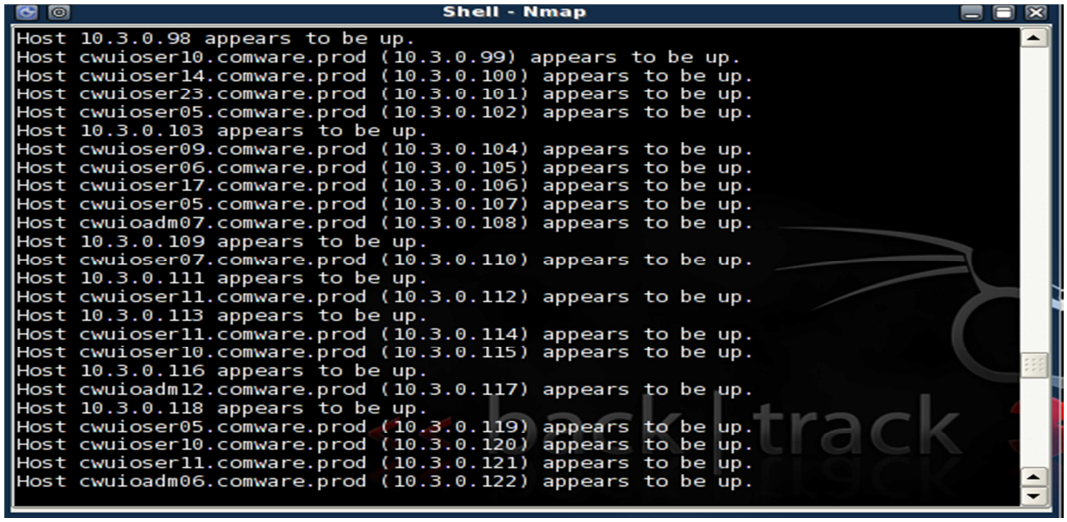


Fig. 3. 7 BackTrack – Dominio - Descripción
Fuente: Los autores

Segmento de red desde la dirección ip 10.3.0.123 hasta la 10.3.0.147, se puede observar los host que aparecen up descubiertas con su respectivo nombre, los host que únicamente aparecen con la dirección ip y up son aquellos que no se encuentran con una descripción en el nombre de host.

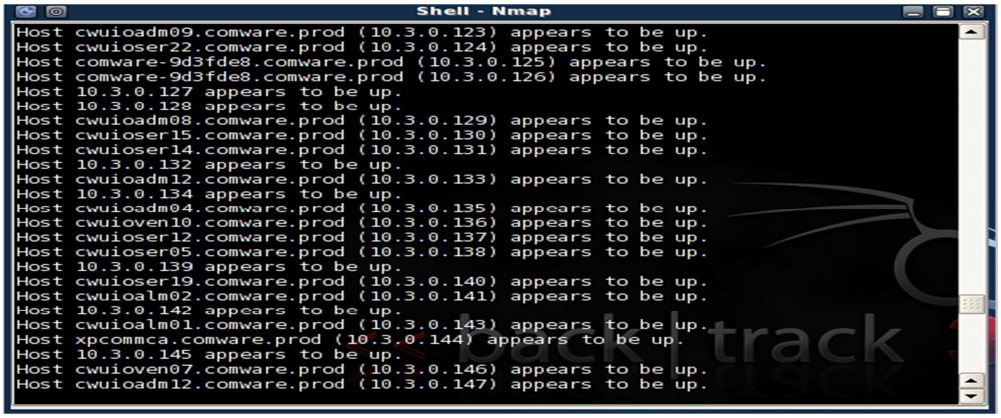


Fig. 3. 8 BackTrack – up descubiertas
Fuente: Los autores

Segmento de red desde la dirección ip 10.3.0.148 hasta la 10.3.0.172, se puede observar los host que parecen up descubiertas con su respectivo nombre, los host que únicamente aparecen con la dirección ip y up son aquellos que no se encuentran con una descripción en el nombre de host.

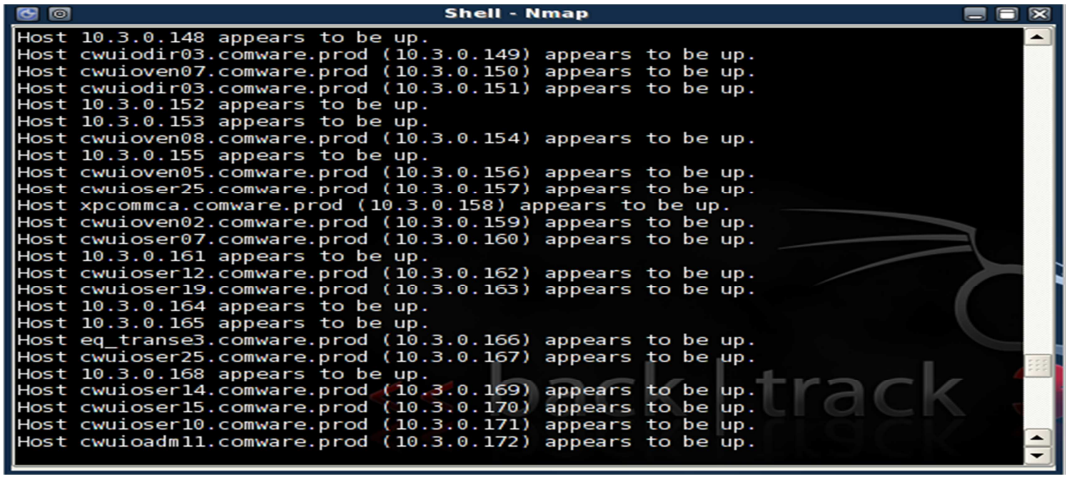


Fig. 3. 9 BackTrack - up descubiertas
Fuente: Los autores

Segmento de red desde la dirección ip 10.3.0.173 hasta la 10.3.0.197, se puede observar los host que parecen up descubiertas con su respectivo nombre, los host que únicamente aparecen con la dirección ip y up son aquellos que no se encuentran con una descripción en el nombre de host.

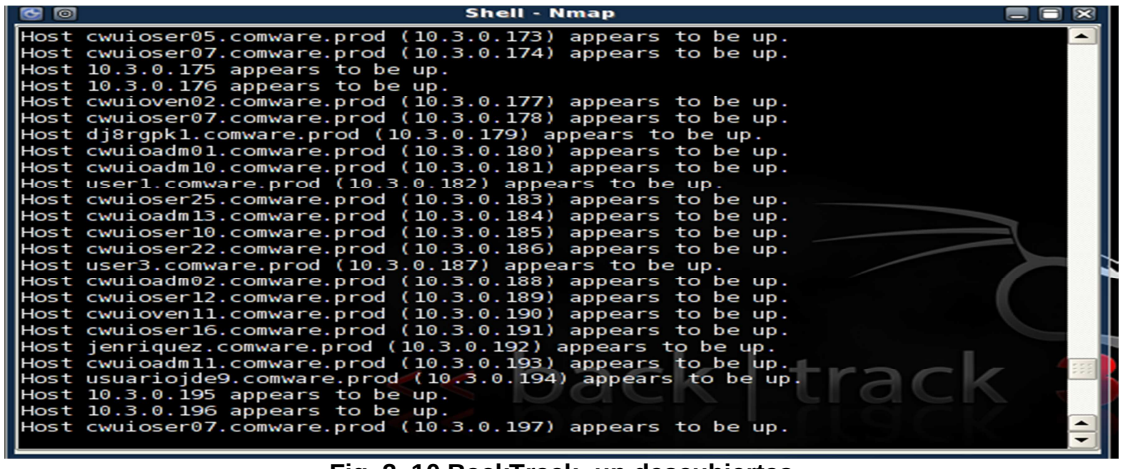


Fig. 3. 10 BackTrack- up descubiertas
Fuente: Los autores

Segmento de red desde la dirección ip 10.3.0.198 hasta la 10.3.0.222, se puede observar los host que parecen up descubiertas con su respectivo nombre, los host que únicamente aparecen con la dirección ip y up son aquellos que no se encuentran con una descripción en el nombre de host.

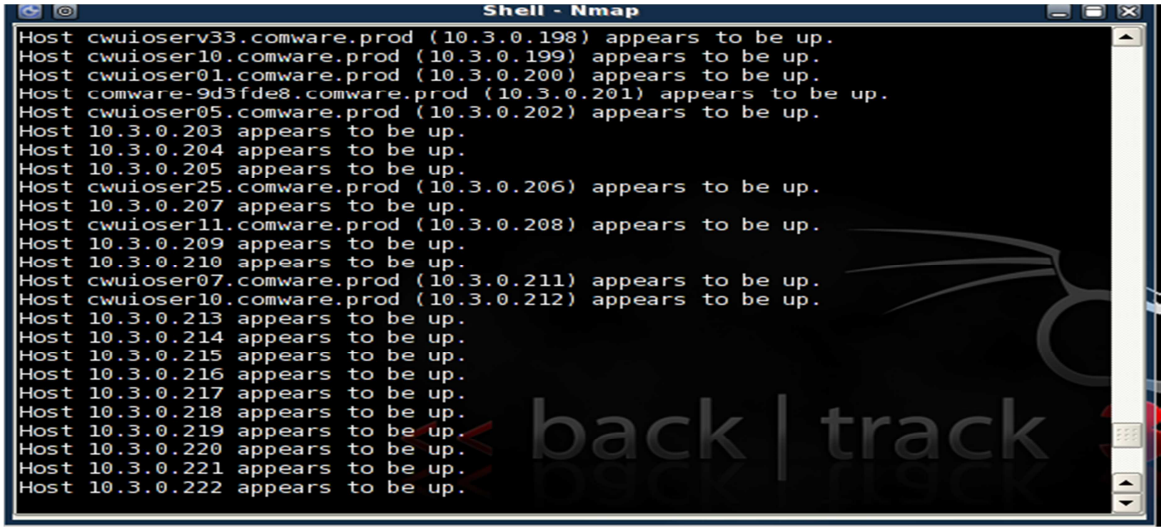


Fig. 3. 11 BackTrack- up descubiertas
Fuente: Los autores

Segmento de red desde la dirección ip 10.3.0.233 hasta la 10.3.0.255, se puede observar los host que parecen up descubiertas con su respectivo nombre, los host que únicamente aparecen con la dirección ip y up son aquellos que no se encuentran con una descripción en el nombre de host.

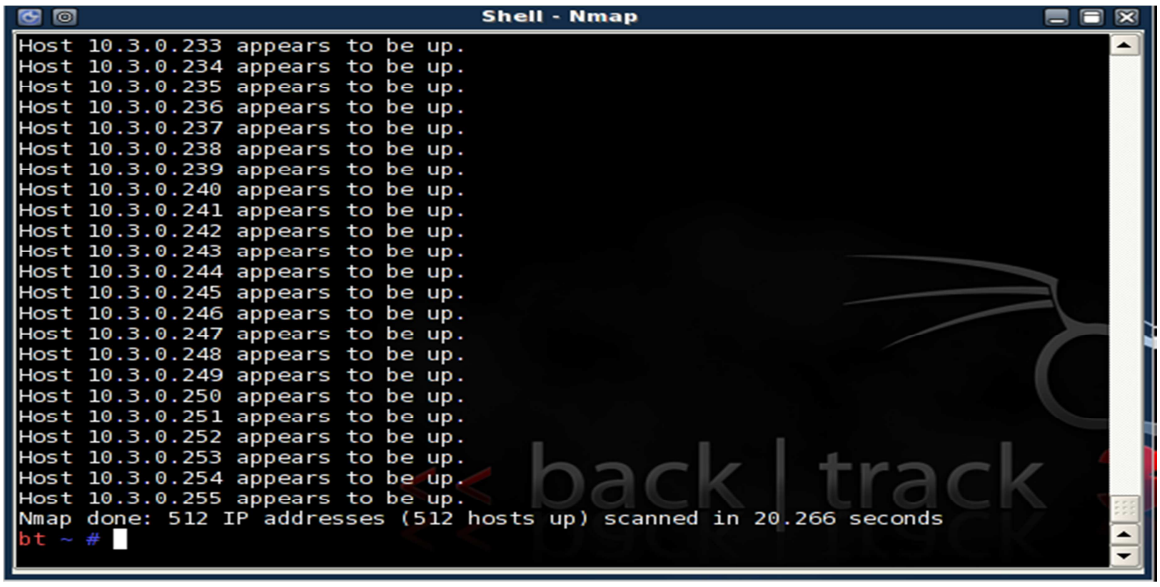


Fig. 3. 12 BackTrack- up descubiertas
Fuente: Los autores

Para visualizar los puertos que se encuentran abiertos se procede a ejecutar el siguiente comando nmap –v –A 10.3.0.138, en donde se visualiza el escaneo de puertos a la dirección especificada en el comando, como se observa en la Figura 3.16;

inicia el mapeo de puertos y en primera instancia encuentra dos puertos tcp abiertos el 1723 y 135, luego aumenta el porcentaje de escaneo en donde se ve que existen más puertos tcp abiertos como el 139 y 2002, estos dos puertos específicamente permitirían el acceso vía remota con programas específicos debido a que el puerto 139 permite el acceso a carpetas compartidas y el puerto 2002 permite el acceso por medio de conexiones remotas. Este ejemplo de escaneo de puertos se realizó en la máquina de un usuario dentro de la red.

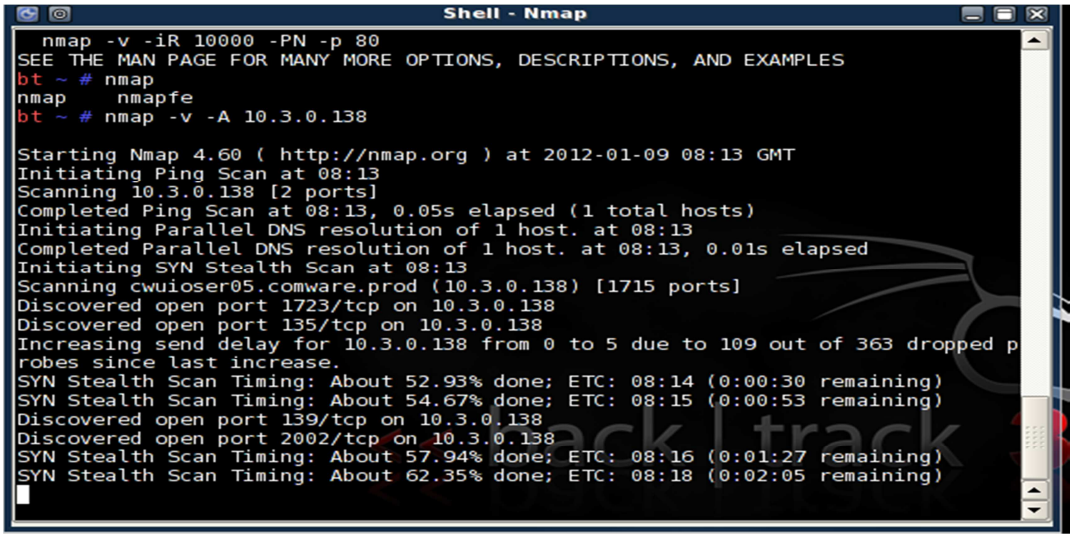


Fig. 3. 13 BackTrack - puertos abiertos
Fuente: Los autores

El siguiente mapeo de puertos, se procedió a realizar en un servidor que se encuentra en producción dicho servidor tiene la ip 200.6.25.67, y es un servidor en donde corre una aplicación para la apertura de casos de los clientes que tiene la empresa. En una primera instancia al iniciar el escaneo de puertos aparecen los puertos tcp 22, 21, 25, que permitirían las conexiones ssh, ftp, smtp, dichos puertos son controlados y no presentarían ningún peligro inminente para la conexión por dichos puertos.

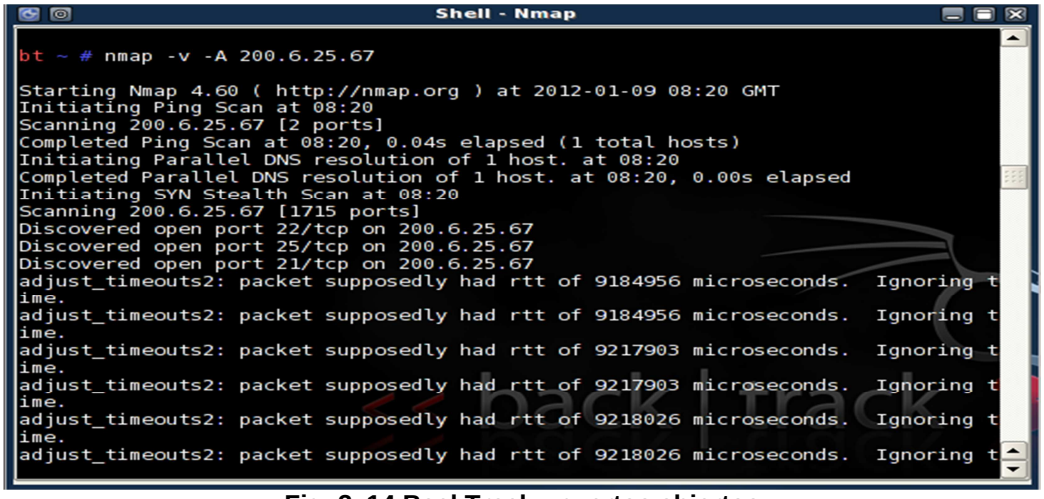


Fig. 3. 14 BackTrack - puertos abiertos
Fuente: Los autores

Continuando con el escaneo en las figuras números 3.18 y 3.19 se muestra un listado de puertos en donde se puede observar, diferentes puertos abiertos, que son utilizados por una aplicación que es la que genera los tickets para asignar a cada uno de los técnicos los casos, estos puertos son puertos controlados por medio de programación en una aplicación java al igual que iptables dentro del servidor.

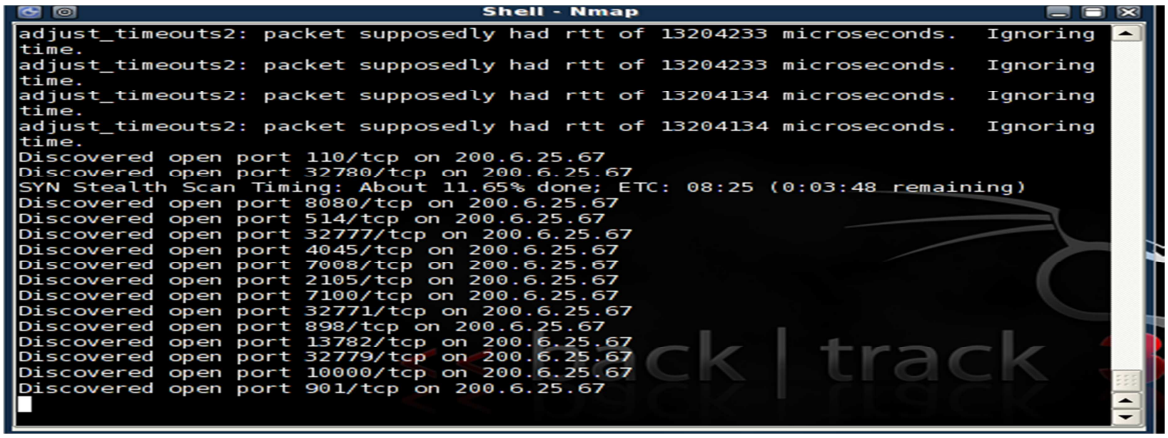


Fig. 3. 15 BackTrack - puertos abiertos
Fuente: Los autores

Se muestran los puertos abiertos dentro del servidor 200.6.25.67 y una vez completado el escaneo se muestran los detalles del escaneo como tiempo de inicio tiempo final de escaneo, cuantos servicios han sido escaneados.

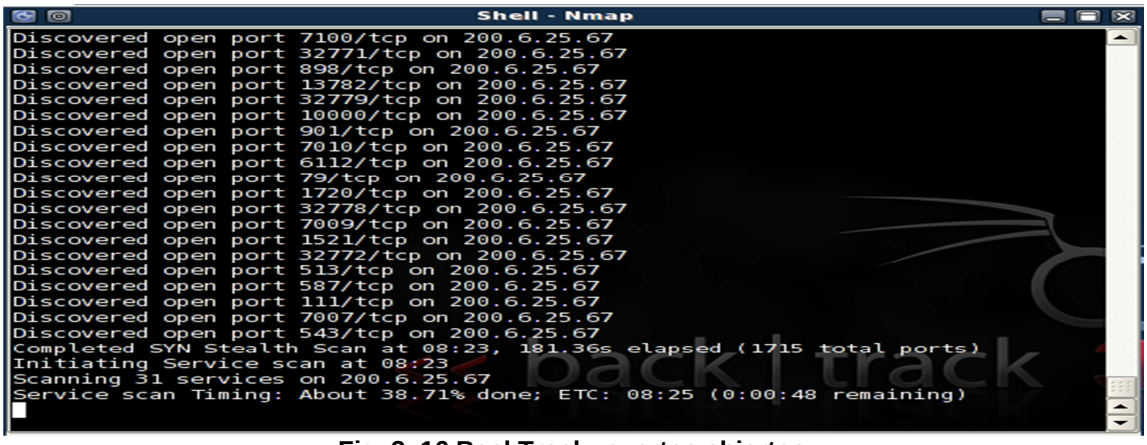


Fig. 3. 16 BackTrack- puertos abiertos
Fuente: Los autores

El siguiente mapeo de puertos, se procedió a realizar en un servidor que se encuentra en producción dicho servidor tiene la ip 200.6.25.65, es un servidor en donde se encuentra el directorio activo. En una primera instancia al iniciar el escaneo de puertos aparece una lista de puertos los cuales tendrán que ser validados con una tabla presentada posteriormente, para que de esta forma se pueda realizar la validación de puertos y saber si presentan algún peligro para la conexión en dichos puertos.

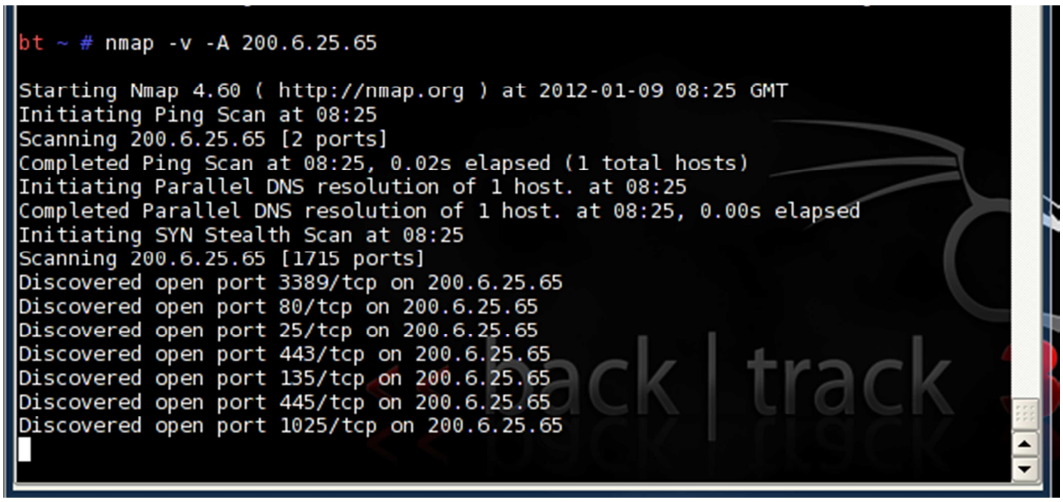


Fig. 3. 17 BackTrack - puertos abiertos
Fuente: Los autores

La siguiente figura, se muestra los puertos abiertos escaneados seguidos de la dirección ip correspondiente al servidor.

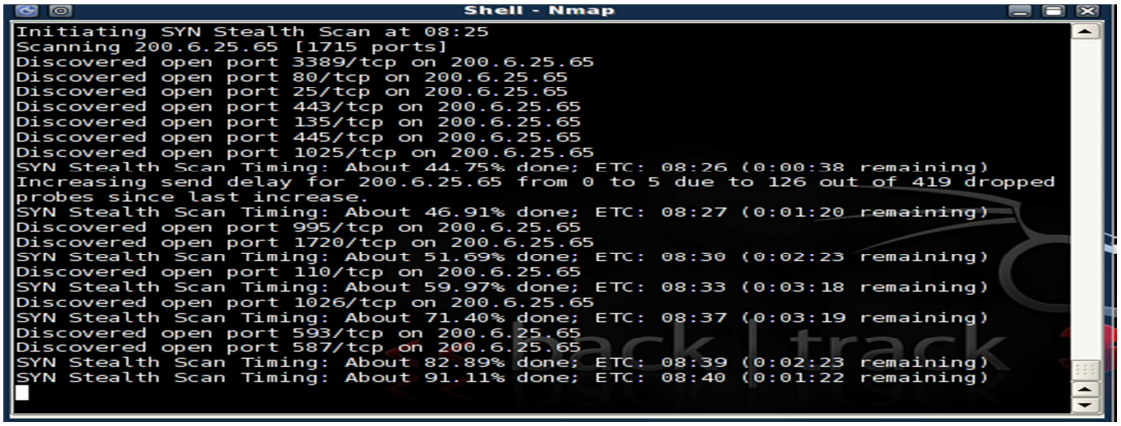


Fig. 3. 18 BackTrack- puertos abiertos
Fuente: Los autores

3.6.2 LANGUARD

En la siguiente figura, se visualiza el ingreso del software LanGuard, por medio del cual se podrá realizar un escaneo completo en los segmentos de red que se necesite visualizar.

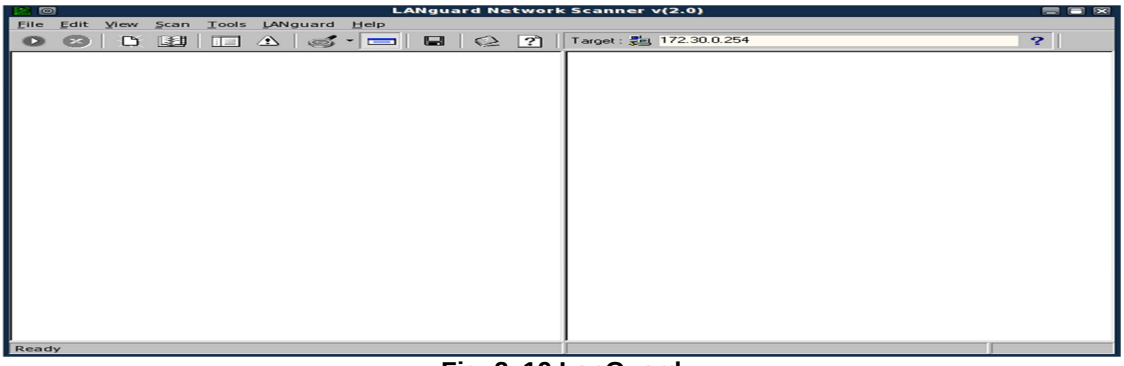


Fig. 3. 19 LanGuard
Fuente: Los autores

Se procede a realizar un nuevo escaneo dentro de la red colocando los siguientes parámetros: El rango para el escaneo de los computadores será desde 10.0.0.1 hasta 10.3.0.254, que son los segmentos de red en donde se encuentran los computadores, switchs, routers y algunos servidores. Para esto se escoge la opción Scan range of computers como muestra la imagen

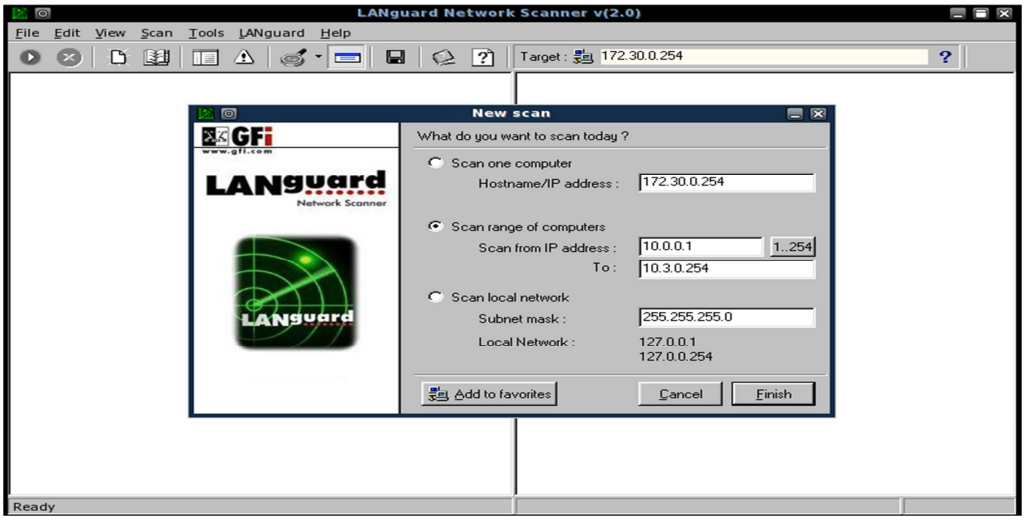


Fig. 3. 20LanGuard–Segmento de red a ser escaneado
Fuente: Los autores

En la siguiente figura, se muestra cada una de las ip's que han respondido al escaneo dentro de la red, mostrándonos diversas características como el tiempo de vida al realizar un ping TTL, puertos que se encuentran abiertos, dirección ip del computador, sistema operativo instalado, nombre netbios[114], usuario, mac[115], dominio en el que se encuentra el equipo, alertas que el equipo se encuentra enviando, recursos compartidos. Esto corresponde al segmento de red 10.0.0.1

[114]NetBIOS, "Network Basic Input/Output System", es, en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.
[115]Mac: En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

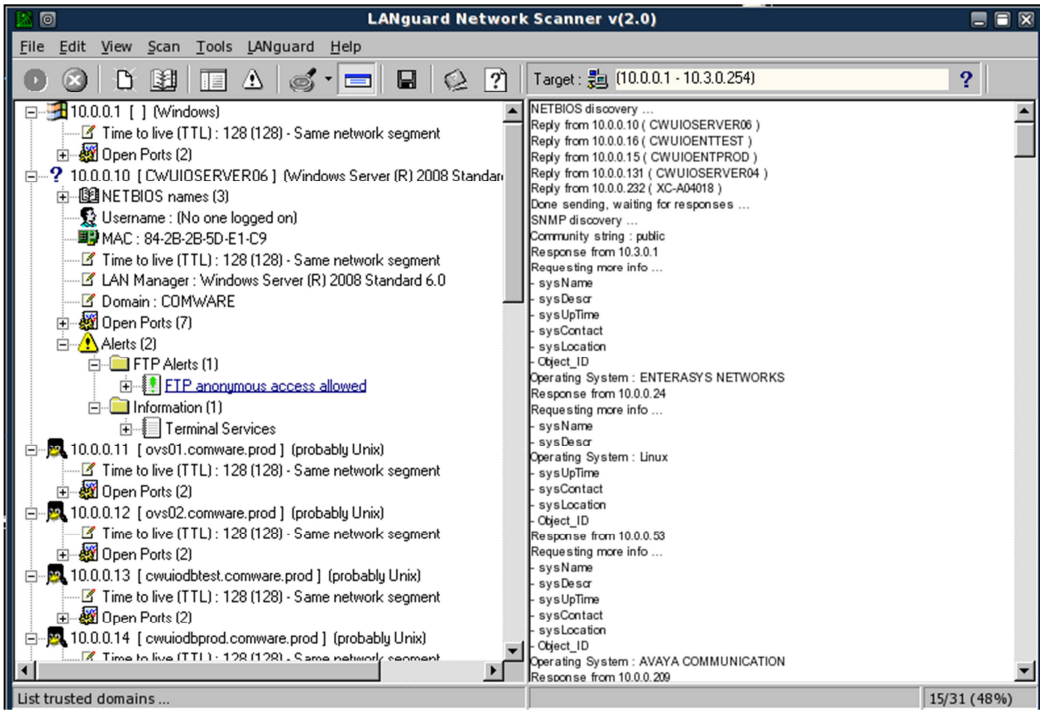


Fig. 3. 21 LanGuard – IP's Respuesta a escaneo
Fuente: Los autores

En la siguiente figura, se muestra el escaneo de los dispositivos vinculados con las direcciones ip 10.0.0.14 hasta la dirección 10.0.0.21, mostrando cada una de las características principales de los equipos como netbios, username, mac, ttl[116], lan manager[117], domain[118], archivos compartidos puertos abiertos.

[116]Tiempo de Vida o Time To Live (TTL) es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.
[117]LAN Manager es un sistema operativo de red (NOS), disponible en varios proveedores y desarrollado por Microsoft en colaboración con 3Com Corporation.
[118]Domain: Un dominio de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

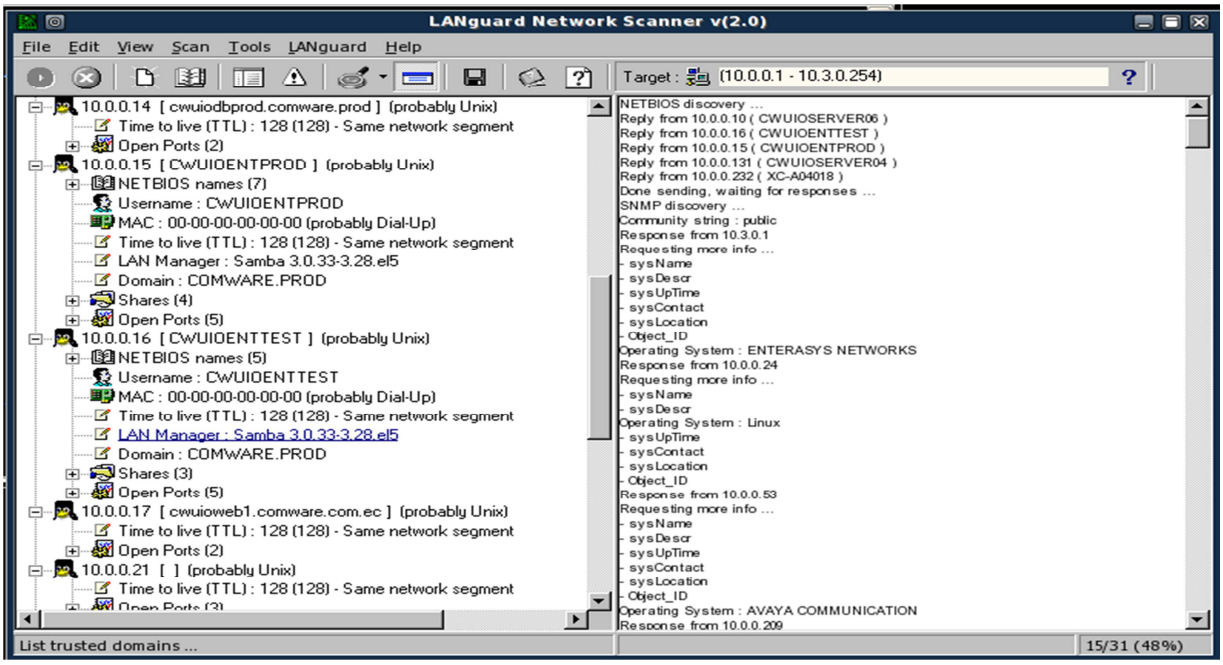


Fig. 3. 22 LanGuard -IP's Respuesta a escaneo
Fuente: Los autores

En la siguiente figura, se muestra todos los dispositivos descubiertos en el segmento de red 10.0.0.1 hasta 10.3.0.254, en este caso muestra de forma muy general cuales fueron los dispositivos encontrados, sin ampliar las características correspondientes a cada equipo.

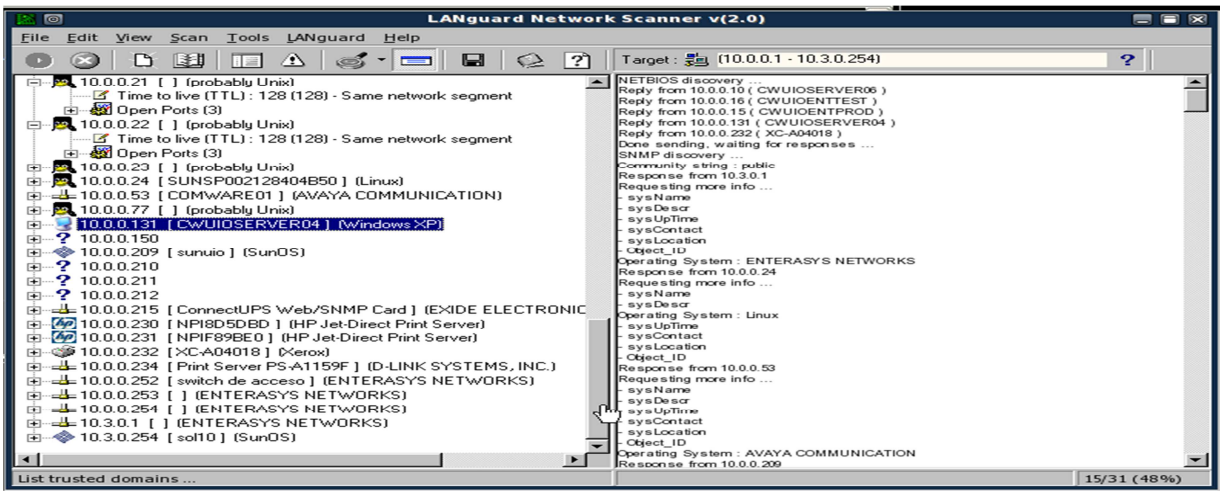


Fig. 3. 23 LanGuard -IP's Respuesta a escaneo
Fuente: Los autores

En la siguiente figura, se visualiza el escaneo al segmento de servidores que empieza en la ip 200.6.25.0 hasta la 200.6.25.254, en la parte izquierda se observa los

diferentes servidores dentro de la red con su respectivo nombre e ip, en la parte derecha se observa el tipo de conexión realizada al servidor el tiempo de vida que ha durado el ping y el tiempo de respuesta del mismo.

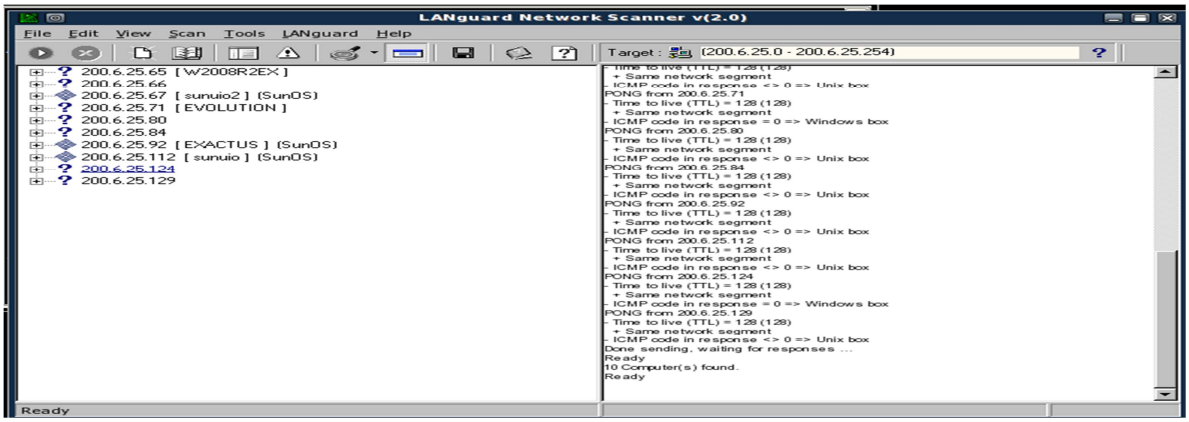


Fig. 3. 24 LanGuard-IP's Respuesta a escaneo
Fuente: Los autores

En lasiguiente figura,se observa el mapeo del servidor 200.6.25.65 correspondiente al servidor de Directorio Activo en donde se ve los diferentes nombres de Netbios, usuario logeado, la mac correspondiente y el tiempo de vida del ping, cabe destacar que con estos datos el servidor se convierte en un punto vulnerable dentro de la red debido a que se sabe qué dirección apunta el servidor, su dominio y la dirección mac, datos más que suficientes para tratar de ingresar a dicho servidor.

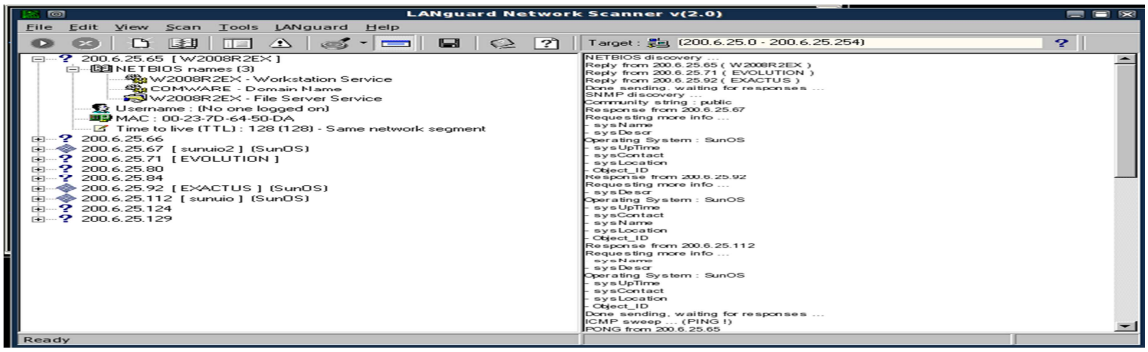


Fig. 3. 25 LanGuard-IP's Respuesta a escaneo
Fuente: Los autores

En la siguiente figura, se observa que se trata de un servidor Sun que se encuentra en producción en donde corre una aplicación de apertura de tickets para los clientes de la

empresa, visualizando el sistema operativo, días de actividad, nombre del sistema, tiempo de vida del ping[119].

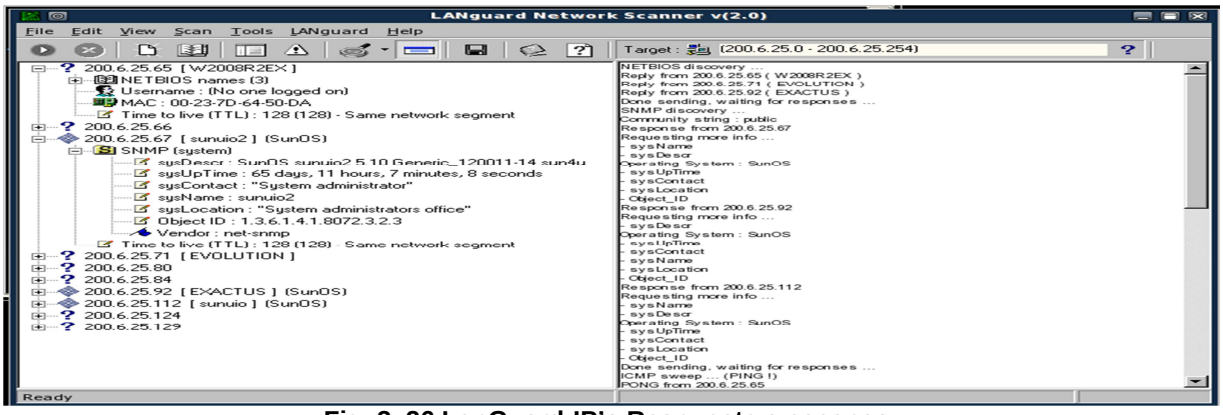


Fig. 3. 26 LanGuard-IP's Respuesta a escaneo
Fuente: Los autores

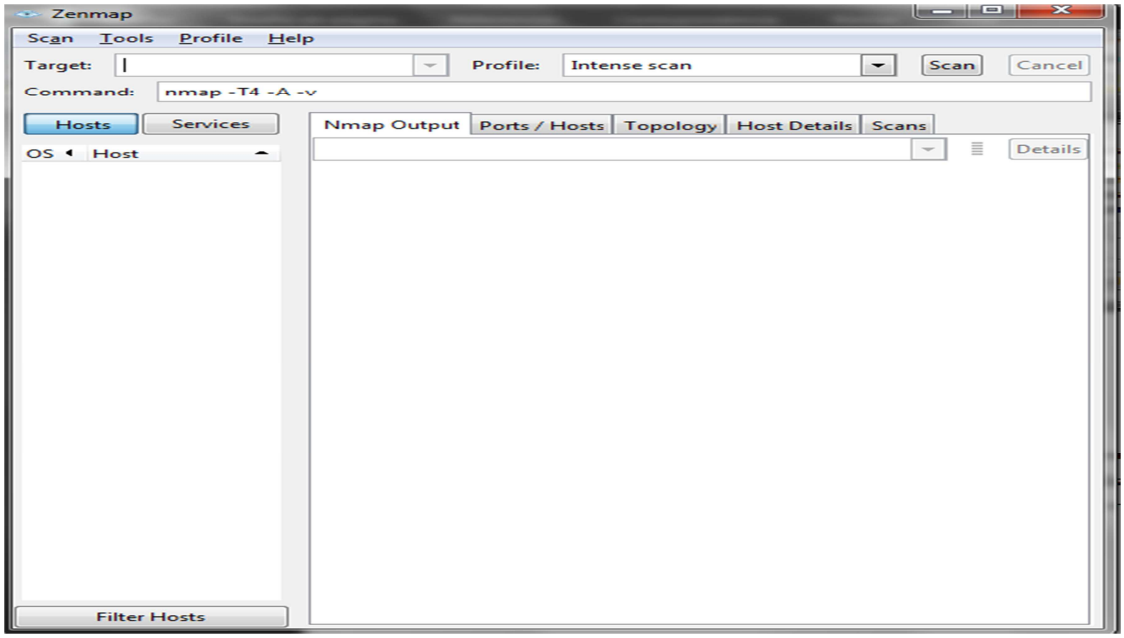


Fig. 3. 27 Zenmap
Fuente: Los autores

Para empezar el proceso de escaneo de un equipo se coloca en la primera opción Target, el nombre del equipo o su ip en este caso tenemos: **evolution.comware.com.ec,** este server se encuentra en producción, se ingresa que

[119]Ping: Formalmente, PING el acrónimo de Packet Internet Groper, el que puede significar "Buscador o rastreador de paquetes en redes".

tipo de escaneo se realizara: **Intense scan, allTcpPorts,** presionando **Scan** para iniciar el escaneo de puertos.

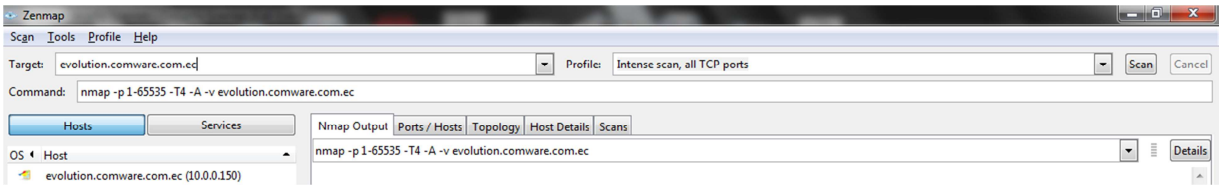


Fig. 3. 28 Zenmap
Fuente: Los autores

Una vez iniciado el escaneo dependiendo de la velocidad que se tenga con el equipo así como, dispositivos intermedios y el tipo de escaneo tardará alrededor de unos 30 minutos a 1 hora, el escaneo empieza con el descubrimiento de puertos en el servidor indicado.

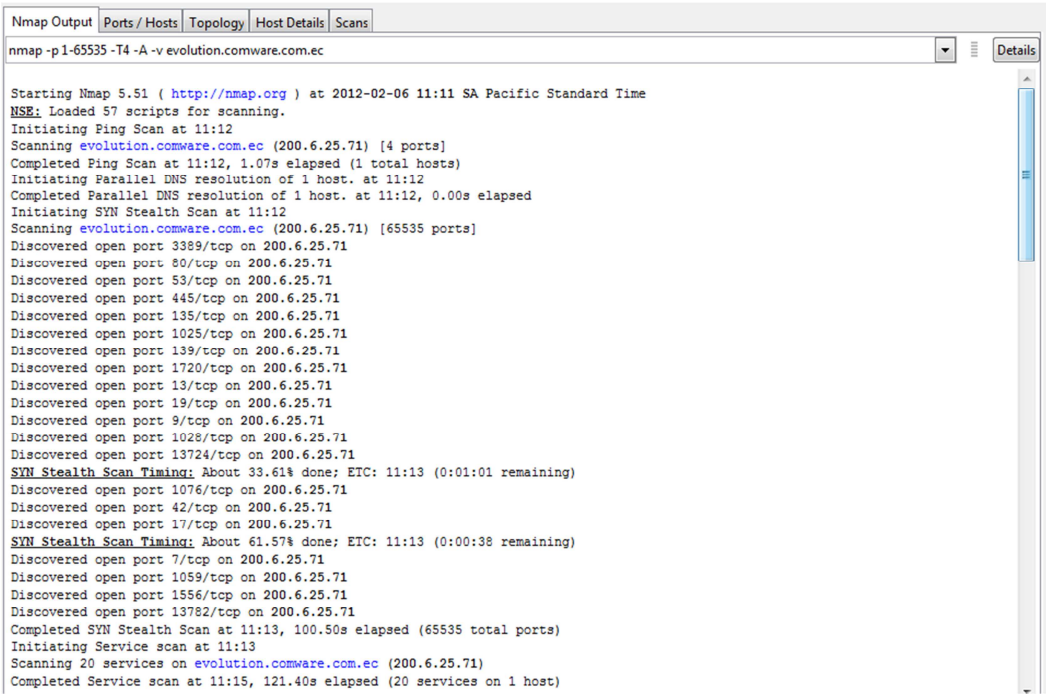


Fig. 3. 29 Zenmap - Descubrimiento de puertos
Fuente: Los autores

Se continúa con la descripción de uno por uno de los puertos abiertos, con el tipo de servicio y versión en la cual se encuentra corriendo.

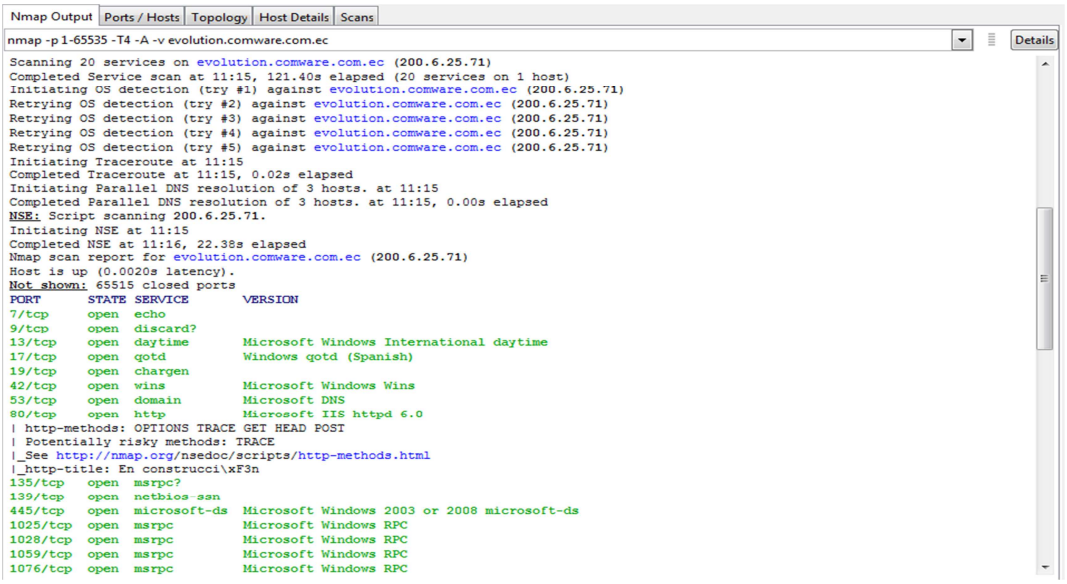


Fig. 3. 30 Zenmap - descubrimiento de puertos
Fuente: Los autores

El resultado de Host Script corresponde a la descripción de flags, algoritmos del sistema operativo, que han servido para obtener la información correspondiente al escaneo.

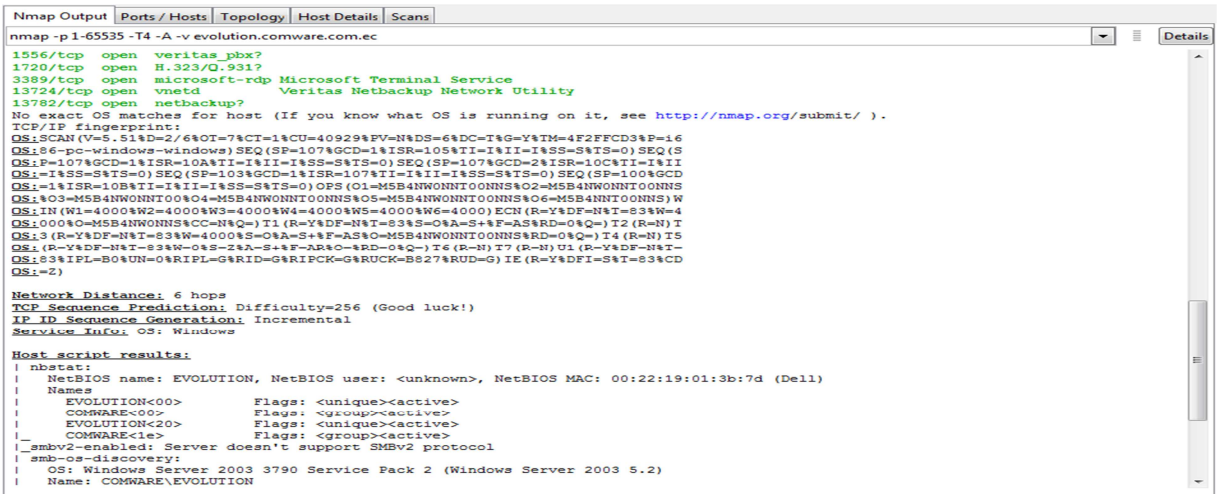
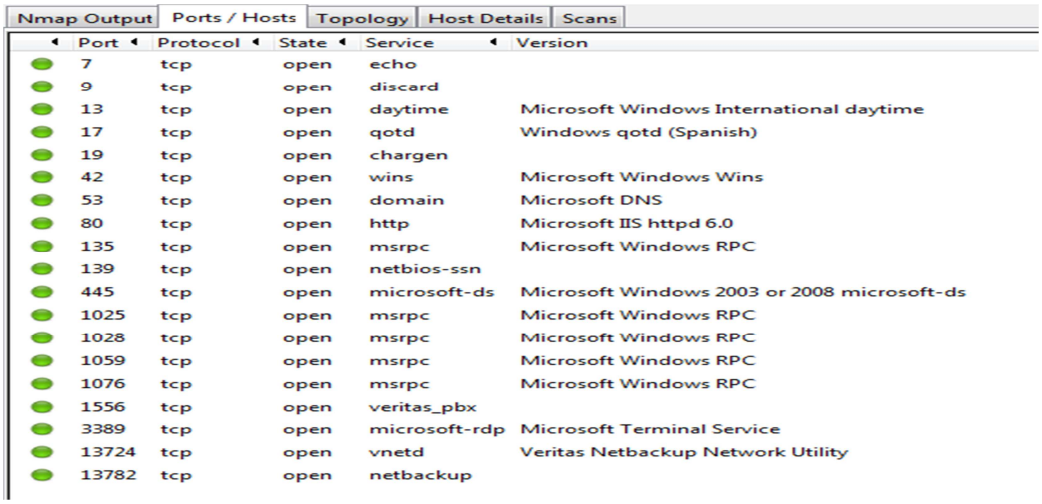


Fig. 3. 31 Zenmap - Host Script
Fuente: Los autores

El trazado correspondiente al equipo se visualiza con todos los saltos que se dieron para llegar a él, en este se tiene seis saltos, correspondientes a routers y firewall, hasta llegar al dispositivo final.

Fig. 3. 32 Zenmap – Trazado de saltos
Fuente: Los autores

Cada uno de los puertos que están abiertos se visualiza en la siguiente imagen teniendo en cuenta: el número de puerto, protocolo, estado, servicio, y versión.



Port	Protocol	State	Service	Version
7	tcp	open	echo	
9	tcp	open	discard	
13	tcp	open	daytime	Microsoft Windows International daytime
17	tcp	open	qotd	Windows qotd (Spanish)
19	tcp	open	chargen	
42	tcp	open	wins	Microsoft Windows Wins
53	tcp	open	domain	Microsoft DNS
80	tcp	open	http	Microsoft IIS httpd 6.0
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
1025	tcp	open	msrpc	Microsoft Windows RPC
1028	tcp	open	msrpc	Microsoft Windows RPC
1059	tcp	open	msrpc	Microsoft Windows RPC
1076	tcp	open	msrpc	Microsoft Windows RPC
1556	tcp	open	veritas_pbx	
3389	tcp	open	microsoft-rdp	Microsoft Terminal Service
13724	tcp	open	vnetd	Veritas Netbackup Network Utility
13782	tcp	open	netbackup	

Fig. 3. 33 Zenmap -Puertos
Fuente: Los autores

La topología que se muestra está determinada desde el localhost que este caso es la máquina origen desde donde se realiza el escaneo, llega al router 10.4.0.1, pasa al firewall 10.0.0.77, finalmente llega al destino evolution.comware.com.ec

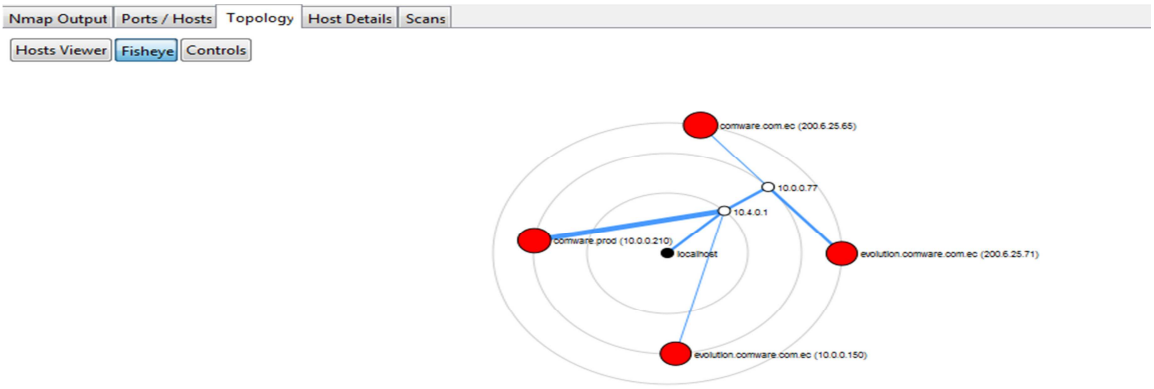


Fig. 3. 34 Zenmap -Trazado de saltos
Fuente: Los autores

El equipo escaneado se puede ver en la siguiente imagen en donde esta cada uno de los detalles correspondientes al mismo.

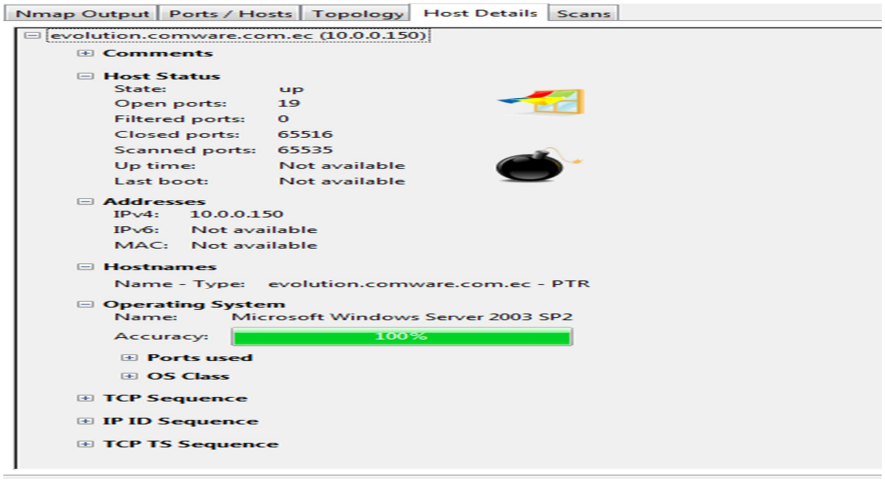


Fig. 3. 35 Zenmap –Detalles escaneo
Fuente: Los autores

3.7 TABLA COMPARATIVA DE HERRAMIENTAS UTILIZADAS

Nombre	SistemaOperativo	Tipo de escaneo	Resultados
Nmap	Linux (Live cd Backtrack)	Puertos de servidoresoperativos	Puertos tcp y udp abiertos
Languard	Linux (Live cd Backtrack)	Puertos de servidoresoperativos	Puertos tcp y udp abiertos
Zenmap	Windows 7	Puertos de servidoresoperativos	Puertos tcp y udp abiertos

Tabla 3. 8 Tabla comparativa
Fuente: Los autores

Mediante la utilización de estos tres softwares de escaneo de puertos en la red se pudo evidenciar que existen una gran cantidad de puertos que se encuentran abiertos para los diferentes equipos, el software recomendado para realizar un escaneo más profundo de la red esZendmap, debido a su fácil e intuitiva configuración para el inicio de un escaneo de red, además posee una interfaz gráfica amigable para el usuario, la topología del escaneo se puede visualizar desde: máquina origen, dispositivos intermedios (routers, switch[120], firewalls), máquina destino; la diversa información acerca de versiones de sistemas operativos, puertos, estado, servicio, hacen que este software sea uno de los principales el momento que se desea tener información acerca de puertos operativos dentro de la red.

Una vez realizado el escaneo por medio de del software Back Track 3, con sus softwares embebidos Nmap y Languard además de utilizar Zenmap, se procederá a realizar el diseño del Sistema de Seguridad de Gestión de la Información, tomando

[120]Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI.

como referencia que no es una red segura por la cantidad de puertos abiertos que fueron evidenciados durante el escaneo.

3.8 AMENAZAS Y VULNERABILIDADES

Una vez realizadas las pruebas para observar las vulnerabilidades de alguno de los sistemas se procede a realizar la identificación de las amenazas y vulnerabilidades que se presentan en cada uno de los activos, para su posterior análisis.

Tanto las amenazas como las vulnerabilidades fueron definidas por el personal encargado del área de Sistemas Internos de la empresa en base a su criterio personal.

AMENAZAS	**VULNERABILIDADES**
Instalación no autorizada de software	Falta en el control de acceso
Desastres naturales	Falta de infraestructura adecuada
Corte de suministro de energía eléctrica	Falta de ups
Acceso no autorizado	Falta de atención en el cuidado de los equipos
Copia no autorizada de software	Falta de políticas de seguridad
Degradación del hardware	Falta de mantenimientos programados
Manipulación en la configuración	Falta de control de acceso
Brechas de seguridad no detectadas	Falta de monitoreo en los servidores
Perdida de la información	Falta de un correcto almacenamiento, errores en los empleados
Divulgación de información de clientes	Falta de acuerdos de confidencialidad
Incompleta documentación de un sistema	Falta de manuales de uso acerca de las aplicaciones.
Modificación no autorizada de la información	Falta de controles de seguridad a la información
Personal no capacitado para realizar una tarea	Falta de capacitación para la atención al cliente.
Errores de usuario final	Falta de conocimiento en el uso de la aplicación
Suplantación de identidad del usuario	Falta de control de acceso
Virus en los equipos	Falta de un correcto uso y actualización de un antivirus.
Sppofing escape de información	Falta de control de acceso
Controles de seguridad no cumplidos	Falta en las políticas de seguridad

Incapacidad de restauración de la información	Falta de backups
Robo	Falta de protección física
Daño por fuego	Falta de protección contra el fuego
Daños por agua	Falta de protección física.

Tabla 3. 9 AMENAZAS Y VULNERABILIDADES
Fuente: Los autores

3.8.1 TASACIÓN DE IMPACTOS EN LOS ACTIVOS INFORMÁTICOS

A continuación se presenta la tabla descrita con los ítems: Confidencialidad, Integridad, Disponibilidad; se debe tomar en cuenta que el método para la calificación es el método cualitativo descrito anteriormente, en donde se puede visualizar cual sería el grado de afectación.

ACTIVOS	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
Antivirus Symantec	1	1	1	**3**
Microsoft Office	2	3	1	**6**
Sac	1	1	1	**3**
Evolution	1	1	1	**3**
DocManager	1	1	1	**3**
JDEdwars	1	1	1	**3**
BDD Oracle	2	2	1	**5**
Exactus	2	2	1	**5**
Computadores de escritorio	2	3	1	**6**
Laptops	2	3	1	**6**
Servidores	1	1	1	**3**
Equipos de Comunicación producción(Modems,Routers, Switchs)	1	1	1	**3**
Equipos de comunicación laboratorio(Modems,Routers, Switchs)	3	5	3	**11**
Correo electrónico	2	2	1	**5**

Telefonía	1	1	1	**3**
Enlace de datos con Gye	1	2	1	**4**
Página Web	1	2	1	**4**
Internet	2	1	1	**4**
Active Directory	1	1	1	**3**
Sistemas internos	1	1	1	**3**
Ups	1	1	1	**3**
Logística	1	1	1	**3**
Talento Humano	1	1	1	**3**
Remuneraciones y Compensaciones	1	1	1	**3**
Financiero	1	1	1	**3**
Registros	1	1	1	**3**
Informes	1	1	1	**3**
Presupuesto	1	1	1	**3**

Tabla 3. 10 TASACIÓN DE LOS ACTIVOS INFORMÁTICOS
Fuente: Los autores

3.8.2 ANÁLISIS Y EVALUACIÓN DEL RIESGO

La escala para calcular las posibilidades es de 1 al 5, siendo 5 mayor:

El valor total máximo permitido para el riesgo, definido por el personal encargado del área de Sistemas Internos de la empresa es de 6.

Activos	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	valor de activos en riesgo	total
Antivirus Symantec	*Acceso no autorizado	2	* Falta de atención en el cuidado de los equipos	2	3	7
	*Copia no autorizada de software	2	* Falta de políticas de seguridad	2	3	7
	*Degradación del hardware	1		1	2	4
	*Manipulación en la configuración	1	* Falta de mantenimientos programados	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de control de acceso	1	2	4
	*Perdida de la información	2	* Falta de monitoreo en los servidores	1	2	5
	*Divulgación de información		* Falta de un correcto almacenamiento, errores en			

	de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 1 2 1 2 1 2	los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 1 2 2 2	2 2 2 2 1 2 1	4 4 5 4 5 5 5
Microsoft Office	*Copia no autorizada de software * Personal no capacitado para realizar una tarea *Degradación del hardware *Manipulación en la configuración	3 2 1	* Falta de políticas de seguridad * Falta de capacitación para la atención al cliente. * Falta de mantenimientos programados	3 2 1	3 3 2	9 7 4

	*Brechas de seguridad no detectadas	1		1	2	4
	*Perdida de la información	1	* Falta de control de acceso	1	2	4
	*Divulgación de información de clientes	2	* Falta de monitoreo en los servidores	1	2	5
	*Incompleta documentación de un sistema	1	* Falta de un correcto almacenamiento, errores en los empleados	1	2	4
	*Modificación no autorizada de la información	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Personal no capacitado para realizar una tarea	2	* Falta de manuales de uso acerca de las aplicaciones	1	2	5
	*Sppofing escape de información		*Falta de controles de			
	*Controles de seguridad no cumplidos	1	seguridad a la información	1	2	4
	*Incapacidad de restauración de la información	2	*Falta de capacitación para la atención al cliente	2	1	5
		1	* Falta de control de acceso	2	2	5
		2	* Falta en las políticas de seguridad	2	1	5
			* Falta de backups			

Sac	* Errores de usuario final	3	* Falta de conocimiento en el uso de la aplicación	3	3	9
	* Acceso no autorizado	4	* Falta de atención en el cuidado de los equipos	4	4	12
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos					
	*Incapacidad de restauración					

	de la información	1	* Falta en las políticas de seguridad	2	2	5
		2	* Falta de backups	2	1	5
Evolution	* Perdida de la información	3	* Falta de un correcto almacenamiento.	3	3	9
	* Errores de usuario final	4	* Falta de conocimiento en el uso de la aplicación	4	4	12
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información					
	*Personal no capacitado para realizar una tarea			1	2	5

	*Sppofing escape de información	2	*Falta de controles de seguridad a la información	1	2	4
	*Controles de seguridad no cumplidos	1	*Falta de capacitación para la atención al cliente	2	1	5
	*Incapacidad de restauración de la información	2	* Falta de control de acceso	2	2	5
		1	* Falta en las políticas de seguridad	2	1	5
		2	* Falta de backups			
DocManager	* Errores de usuario final	3	* Falta de conocimiento en el uso de la aplicación	3	3	9
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación					

	de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 2 1 2 1 2	* Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 2 2 2	2 2 2 1 2 1	4 5 4 5 5 5
JDEdwars	* Errores de usuario final *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información	3 1 1 1 2	* Falta de conocimiento en el uso de la aplicación * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en	3 1 1 1 1	3 2 2 2 2	9 4 4 4 5

	*Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 1 2 1 2 1 2	los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 1 2 2 2	2 2 2 2 1 2 1	4 4 5 4 5 5 5
BDD Oracle	* Modificación no autorizada de la información * Virus en los equipos * Acceso no autorizado	2 1 2	* Falta de controles de seguridad a la información * Falta de un correcto uso y actualización de un antivirus * Falta de atención en el cuidado de los equipos	2 1 2	2 1 2	6 3 6

	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos	1	* Falta en las políticas de seguridad	2	2	5
	*Incapacidad de restauración de la información					

		2	* Falta de backups	**2**	**1**	**5**
Exactus	***** Errores de usuario final	**3**	* Falta de conocimiento en el uso de la aplicación	**3**	**3**	**9**
	*Degradación del hardware	**1**	* Falta de mantenimientos programados	**1**	**2**	**4**
	*Manipulación en la configuración	**1**	* Falta de control de acceso	**1**	**2**	**4**
	*Brechas de seguridad no detectadas	**1**	* Falta de monitoreo en los servidores	**1**	**2**	**4**
	*Perdida de la información	**2**	* Falta de un correcto almacenamiento, errores en los empleados	**1**	**2**	**5**
	*Divulgación de información de clientes	**1**	* Falta de acuerdos de confidencialidad	**1**	**2**	**4**
	*Incompleta documentación de un sistema	**1**	* Falta de manuales de uso acerca de las aplicaciones	**1**	**2**	**4**
	*Modificación no autorizada de la información	**2**	*Falta de controles de seguridad a la información	**1**	**2**	**5**
	*Personal no capacitado para realizar una tarea	**1**	*Falta de capacitación para la	**1**	**2**	**4**
	*Sppofing escape de información					
	*Controles de seguridad no					

	cumplidos *Incapacidad de restauración de la información	2 1 2	atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	2 2 2	1 2 1	5 5 5
Computadores de escritorio	* Daño por fuego * Daños por agua • * Perdida de la Información * Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes	2 2 2 3 1 1 2 1	• *Falta de protección contra el fuego * Falta de protección física. * Falta de un correcto almacenamiento, errores en los empleados * Degradación del hardware * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto	2 2 2 3 1 1 1 1	2 2 2 3 2 2 2 2	6 6 6 9 4 4 5 4

	*Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 2 1 2 1 2	almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 2 2 2	2 2 2 1 2 1	4 5 4 5 5 5
Laptops	* Daño por fuego * Daños por agua • * Perdida de la	2 2 2	• *Falta de protección contra el fuego * Falta de protección física.	2 2 2	2 2 2	6 6 6

	Información *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la	1 1 1 2 1 1 2 1 2 1	* Falta de un correcto almacenamiento, errores en los empleados * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso	1 1 1 1 1 1 1 2 2	2 2 2 2 2 2 2 1 2	4 4 4 5 4 4 5 4 5 5

	información	2	* Falta en las políticas de seguridad * Falta de backups	2	1	5
Servidores	* Daño por fuego * Daños por agua • * Perdida de la Información * Virus en los equipos *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información	2 2 2 2 1 1 1 2	• *Falta de protección contra el fuego * Falta de protección física. * Falta de un correcto almacenamiento, errores en los empleados * Falta de un correcto uso y actualización de un antivirus. * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto	2 2 2 2 1 1 1 1	2 2 2 2 2 2 2 2	6 6 6 6 4 4 4 5

	*Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 1 2 1 2 1 2	almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 1 2 2 2	2 2 2 2 1 2 1	4 4 5 4 5 5 5
Equipos de Comunicación producción	* Daño por fuego * Daños por agua * Acceso no autorizado	2 2 2	• *Falta de protección contra el fuego * Falta de protección física.	2 2 2	2 2 2	6 6 6

	*Degradación del hardware	1	* Falta de atención en el cuidado de los equipos	1	2	4
	*Manipulación en la configuración	1	* Falta de mantenimientos programados	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de control de acceso	1	2	4
	*Perdida de la información	2	* Falta de monitoreo en los servidores	1	2	5
	*Divulgación de información de clientes	1	* Falta de un correcto almacenamiento, errores en los empleados	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Modificación no autorizada de la información	2	* Falta de manuales de uso acerca de las aplicaciones	1	2	5
	*Personal no capacitado para realizar una tarea					
	*Sppofing escape de información	1	*Falta de controles de seguridad a la información	1	2	4
	*Controles de seguridad no cumplidos	2	*Falta de capacitación para la atención al cliente	2	1	5
	*Incapacidad de restauración de la información	1	* Falta de control de acceso	2	2	5
			* Falta en las políticas de			

		2	seguridad * Falta de backups	2	1	5
Equipos de comunicación laboratorio	* Daño por fuego * Daños por agua * Acceso no autorizado *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información	2 2 2 1 1 1 2 1 1	• *Falta de protección contra el fuego * Falta de protección física. * Falta de atención en el cuidado de los equipos * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso	2 2 2 1 1 1 1 1 1	2 2 2 2 2 2 2 2 2	6 6 6 4 4 4 5 4 4

	*Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	2 1 2 1 2	acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 2 2 2	2 2 1 2 1	5 4 5 5 5
Correo electrónico	* Errores de usuario final * Acceso no autorizado *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información	2 2 1 1 1 2	* Falta de conocimiento en el uso de la aplicación * Falta de cuidado equipo * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados	2 2 1 1 1 1	2 2 2 2 2 2	6 6 4 4 4 5

	*Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 1 2 1 2 1 2	* Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 1 2 2 2	2 2 2 2 2 1 2 1	4 4 5 4 5 5 5
Telefonía	* Personal no capacitado para realizar una tarea * Errores de usuario final *Degradación del hardware	2 2 1	* Falta de capacitación para la atención al cliente. * Falta de conocimiento en el uso * Falta de mantenimientos programados	2 2 1	2 2 2	6 6 4

	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos	1	* Falta en las políticas de seguridad	2	2	5
	*Incapacidad de restauración de la información	2	* Falta de backups	2	1	5

Enlace de datos con Guayaquil	* Corte de suministro de energía eléctrica	4	*Falta de ups	4	4	4
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos	1	* Falta en las políticas de seguridad	2	2	5
	*Incapacidad de restauración de la información					

		2	* Falta de backups	**2**	**1**	**5**
Página Web	***** Errores de usuario final *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no	**3** **1** **1** **1** **2** **1** **1** **2** **1**	* Falta de conocimiento en el uso de la aplicación * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la	**3** **1** **1** **1** **1** **1** **1** **1** **1**	**3** **2** **2** **2** **2** **2** **2** **2** **2**	**9** **4** **4** **4** **5** **4** **4** **5** **4**

	cumplidos *Incapacidad de restauración de la información	2 1 2	atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	2 2 2	1 2 1	5 5 5
Internet	*Sppofing escape de información * Errores de usuario final *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de	2 2 1 1 1 2 1 1	* Falta de control de acceso * Falta de conocimiento en el uso de la aplicación * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso	2 2 1 1 1 1 1 1	2 2 2 2 2 2 2 2	6 6 4 4 4 5 4 4

	la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	2 1 2 1 2	acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 2 2 2	2 2 1 2 1	5 4 5 5 5
Active Directory	* Manipulación en la configuración * Brechas de seguridad no detectadas *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información	2 3 1 1 1	* Falta de control de acceso * Falta de monitoreo en los servidores * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores	2 3 1 1 1	2 3 2 2 2	6 9 4 4 4

	*Divulgación de información de clientes *Incompleta documentación de un sistema *Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	**2** **1** **1** **2** **1** **2** **1** **2**	* Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	**1** **1** **1** **1** **1** **2** **2** **2**	**2** **2** **2** **2** **2** **1** **2** **1**	**5** **4** **4** **5** **4** **5** **5** **5**
Sistemas internos	* Incompleta documentación de un sistema *Degradación del hardware	**3** **1**	* Falta de manuales de uso acerca de las aplicaciones. * Falta de mantenimientos	**3** **1**	**3** **2**	**9** **4**

	*Manipulación en la configuración		programados			
	*Brechas de seguridad no detectadas	1	* Falta de control de acceso	1	2	4
	*Perdida de la información	1	* Falta de monitoreo en los servidores	1	2	4
	*Divulgación de información de clientes	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Incompleta documentación de un sistema	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Modificación no autorizada de la información	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Personal no capacitado para realizar una tarea	2	*Falta de controles de seguridad a la información	1	2	5
	*Sppofing escape de información	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Controles de seguridad no cumplidos	2	* Falta de control de acceso	2	1	5
	*Incapacidad de restauración de la información	1	* Falta en las políticas de seguridad	2	2	5
		2	* Falta de backups	2	1	5

Ventas	* Divulgación de información de clientes	2	* Falta de acuerdos de confidencialidad	2	2	6
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos					
	*Incapacidad de restauración					

	de la información	1	* Falta en las políticas de seguridad	2	2	5
		2	* Falta de backups	2	1	5
Logística	* Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	2	2	6
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de	1	2	5
	*Personal no capacitado para realizar una tarea					
	*Sppofing escape de					

	información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 2 1 2	seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 2 2 2	2 1 2 1	4 5 5 5
Talento Humano	* Perdida de la información * Divulgación de información de clientes *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes	2 1 1 1 1 2	* Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados	2 1 1 1 1 1	2 1 2 2 2 2	6 3 4 4 4 5

	*Incompleta documentación de un sistema	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Modificación no autorizada de la información	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Personal no capacitado para realizar una tarea	2	*Falta de controles de seguridad a la información	1	2	5
	*Sppofing escape de información	1	*Falta de capacitación para la atención al cliente	2	2	4
	*Controles de seguridad no cumplidos	2	* Falta de control de acceso	2	1	5
	*Incapacidad de restauración de la información	1	* Falta en las políticas de seguridad	2	2	5
		2	* Falta de backups	2	1	5
Remuneraciones y Compensaciones	* Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	2	2	6
	* Manipulación en la configuración	1	* Falta de control de acceso	1	1	3
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración					

	*Brechas de seguridad no detectadas	1	* Falta de control de acceso	1	2	4
	*Perdida de la información	1	* Falta de monitoreo en los servidores	1	2	4
	*Divulgación de información de clientes	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Incompleta documentación de un sistema	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Modificación no autorizada de la información	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Personal no capacitado para realizar una tarea	2	*Falta de controles de seguridad a la información	1	2	5
	*Sppofing escape de información	1	*Falta de capacitación para la atención al cliente	2	1	4
	*Controles de seguridad no cumplidos	2	* Falta de control de acceso	2	2	5
	*Incapacidad de restauración de la información	1	* Falta en las políticas de seguridad	2	1	5
		2	* Falta de backups			

Financiero	* Perdida de la información	1	* Falta de un correcto almacenamiento, errores en los empleados	1	1	3
	* Modificación no autorizada de la información	1	* Falta de controles de seguridad a la información	1	1	3
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	1	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	2		1	2	4
	*Sppofing escape de información					
	*Controles de seguridad no					

	cumplidos *Incapacidad de restauración de la información	1 2 1 2	*Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	2 2 2	1 2 1	5 5 5
Registros	* Perdida de la información *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información *Divulgación de información de clientes *Incompleta documentación de un sistema	2 1 1 1 2 1	* Falta de un correcto almacenamiento, errores en los empleados * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto almacenamiento, errores en los empleados * Falta de acuerdos de confidencialidad	2 1 1 1 1 1	2 2 2 2 2 2	6 4 4 4 5 4

	*Modificación no autorizada de la información *Personal no capacitado para realizar una tarea *Sppofing escape de información *Controles de seguridad no cumplidos *Incapacidad de restauración de la información	1 2 1 2 1 2	* Falta de manuales de uso acerca de las aplicaciones *Falta de controles de seguridad a la información *Falta de capacitación para la atención al cliente * Falta de control de acceso * Falta en las políticas de seguridad * Falta de backups	1 1 1 2 2 2	2 2 2 1 2 1	4 5 4 5 5 5
Informes	* Perdida de la información *Degradación del hardware *Manipulación en la configuración *Brechas de seguridad no detectadas *Perdida de la información	2 1 1 1 2	* Falta de un correcto almacenamiento, errores en los empleados * Falta de mantenimientos programados * Falta de control de acceso * Falta de monitoreo en los servidores * Falta de un correcto	2 1 1 1 1	2 2 2 2 2	6 4 4 4 5

	*Divulgación de información de clientes		almacenamiento, errores en los empleados			
	*Incompleta documentación de un sistema	**1**	* Falta de acuerdos de confidencialidad	**1**	**2**	**4**
	*Modificación no autorizada de la información	**1**	* Falta de manuales de uso acerca de las aplicaciones	**1**	**2**	**4**
	*Personal no capacitado para realizar una tarea			**1**	**2**	**5**
	*Sppofing escape de información	**2**	*Falta de controles de seguridad a la información			
	*Controles de seguridad no cumplidos	**1**	*Falta de capacitación para la atención al cliente	**1**	**2**	**4**
	*Incapacidad de restauración de la información	**2**	* Falta de control de acceso	**2**	**1**	**5**
		1	* Falta en las políticas de seguridad	**2**	**2**	**5**
		2	* Falta de backups	**2**	**1**	**5**

Presupuesto	* Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	2	2	6
	*Degradación del hardware	1	* Falta de mantenimientos programados	1	2	4
	*Manipulación en la configuración	1	* Falta de control de acceso	1	2	4
	*Brechas de seguridad no detectadas	1	* Falta de monitoreo en los servidores	1	2	4
	*Perdida de la información	2	* Falta de un correcto almacenamiento, errores en los empleados	1	2	5
	*Divulgación de información de clientes	1	* Falta de acuerdos de confidencialidad	1	2	4
	*Incompleta documentación de un sistema	1	* Falta de manuales de uso acerca de las aplicaciones	1	2	4
	*Modificación no autorizada de la información	2	*Falta de controles de seguridad a la información	1	2	5
	*Personal no capacitado para realizar una tarea	1	*Falta de capacitación para la atención al cliente	1	2	4
	*Sppofing escape de información	2	* Falta de control de acceso	2	1	5
	*Controles de seguridad no cumplidos					
	*Incapacidad de restauración de la información					

		1	* Falta en las políticas de seguridad	2	2	5
		2	* Falta de backups	2	1	5

Tabla 3. 11 AMENAZAS Y VULNERABILIDADES
Fuente: Los autores

3.8.3 TRATAMIENTO DEL RIESGO

A través de la tabla de evaluación de riesgo se pudo evaluar cuáles son los riesgos con más probabilidad que ocurran en los activos informáticos, por lo cual, se procederá a realizar el tratamiento del mismo pues la gestión del riesgo incluye maximizar la probabilidad y consecuencias de eventos positivos y minimizar la probabilidad y consecuencias de eventos adversos a los objetivos de proyectos, procesos o programas, es por ello que se propone las siguientes posibilidades para el tratamiento del riesgo:

- Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo.
- Reducir o controlar la probabilidad de la ocurrencia.
- Reducir o controlar las consecuencias.
- Transferir los riesgos.
- Retener los riesgos.
- Aceptar los riesgos.[121]

Para el presente caso la opción más viable es Reducir o controlar la probabilidad de ocurrencia, esto se basa en lo siguiente:

- Programas de auditoría y cumplimiento.
- Revisiones formales de requerimientos, especificaciones, diseño, ingeniería y operaciones.
- Inspecciones y controles de procesos.
- Mantenimiento preventivo.
- Aseguramiento de calidad, administración y estándares.[122]

[121]ICD, Gestión del Riesgo, 2012-09-03, http://www.icd.go.cr/sitio/downloads/uploads/web_icd_pdf/gestionriesgo/gr_004.pdf.pdf
[122]Idem 103

3.8.4 SELECCIÓN DE CONTROLES

Para realizar una correcta selección de controles las mismas que son las contramedidas o salvaguardas especificadas en el Anexo A de la Norma ISO 27001:2005, se enfocara en los 11 dominios de cobertura de la norma, a continuación especificados:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Gestión de activos.
- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y ambiental.
- A.10 Gestión de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.13 Gestión de incidentes en seguridad de la información.
- A.14 Gestión de la continuidad del negocio.
- A.15 Cumplimiento.[123]

Para realizar una correcta selección de controles para que la organización pueda implementar se debe basar en tres fuentes:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales (implementación no es discutible).
- Producto de las operaciones en el negocio de la compañía.[124]

Se tomaron los valores superiores a 6 puntos para el análisis y evaluación del riesgo.

[123]ICD, Gestión del Riesgo, 2012-09-03, http://www.icd.go.cr/sitio/downloads/uploads/web_icd_pdf/gestionriesgo/gr_004.pdf.pdf
[124]Idem 105

Activos	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	valor de activos en riesgo	total	Opción del tratamiento del riesgo	Objetivos de control	Controles de la norma ISO 27001
Antivirus Symantec	*Acceso no autorizado *Copia no autorizada de software	**2** **2**	* Falta de atención en el cuidado de los equipos * Falta de políticas de seguridad	**2** **2**	**3** **3**	**7** **7**	Reducir o controlar la probabilidad de ocurrencia	**A.11** Control de Acceso **A.11** Control de Acceso	**A.11.5.2** Identificación y Autenticación del Usuario **A11.6.1** Restricción al acceso a la información
Microsoft Office	*Copia no autorizada de software * Personal no capacitado para realizar una tarea	**3** **2**	* Falta de políticas de seguridad * Falta de capacitación para la atención al cliente.	**3** **2**	**3** **3**	**9** **7**	Reducir o controlar la probabilidad de ocurrencia	**A.11** Control de Acceso **A.8** Seguridad de los recursos humanos	**A11.6.1** Restricción al acceso a la información **A.8.2.2** Capacitación y educación en seguridad de la información
Sac	* Errores de usuario final	**3**	* Falta de conocimient	**3**	**3**	**9**	Reducir o controlar la probabilidad	**A.8** Seguridad de los recursos	**A.8.2.2** Capacitación y educación

	* Acceso no autorizado	**4**	o en el uso de la aplicación * Falta de atención en el cuidado de los equipos	**4**	**4**	**12**	de ocurrencia Reducir o controlar la probabilidad de ocurrencia	humanos **A.11** Control de Acceso	en seguridad de la información **A.11.5.2** Identificación y Autenticación del Usuario
Evolution	***** Perdida de la información ***** Errores de usuario final	**3** **4**	***** Falta de un correcto almacenamiento. * Falta de conocimiento en el uso de la aplicación	**3** **4**	**3** **4**	**9** **12**	Reducir o controlar la probabilidad de ocurrencia	**A.10** Gestión de Comunicaciones y operaciones **A.8** Seguridad de los recursos humanos	**A10.5.1** Respaldo de la información back-up **A.8.2.2** Capacitación y educación en seguridad de la información
DocManager	***** Errores de usuario final	**3**	***** Falta de conocimiento en el uso de la aplicación	**3**	**3**	**9**	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos	**A.8.2.2** Capacitación y educación en seguridad de la información

JDEdwars	* Errores de usuario final	**3**	* Falta de conocimiento en el uso de la aplicación	**3**	**3**	**9**	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos	**A.8.2.2** Capacitación y educación en seguridad de la información
Exactus	* Errores de usuario final	**3**	* Falta de conocimiento en el uso de la aplicación	**3**	**3**	**9**	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos	**A.8.2.2** Capacitación y educación en seguridad de la información
Correo electrónico	• * Errores de usuario final • * Acc	**2** **2**	* Falta de conocimiento en el uso de la aplicación * Falta de cuidado equipo	**2** **2**	**2** **2**	**6** **6**	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos **A.11** Control de Acceso	**A.8.2.2** Capacitación y educación en seguridad de la información **A.11.5.2** Identificación y Autenticación del Usuario

	eso no autorizado								
Telefonía	• * Personal no capacitado para realizar una tarea • * Err	**2** **2**	* Falta de capacitación para la atención al cliente. * Falta de conocimiento en el uso	**2** **2**	**2** **2**	**6** **6**	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos	**A.8.2.2** Capacitación y educación en seguridad de la información

	ores de usuario final								
Página Web	* Errores de usuario final	3	* Falta de conocimiento en el uso de la aplicación	3	3	9	Reducir o controlar la probabilidad de ocurrencia	**A.8** Seguridad de los recursos humanos	**A.8.2.2** Capacitación y educación en seguridad info
Active Directory	* Manipulación en la configuración * Brechas de seguridad no detectadas	2 3	* Falta de control de acceso * Falta de monitoreo en los servidores	2 3	2 3	6 9	Reducir o controlar la probabilidad de ocurrencia	**A12** Adquisición, desarrollo y mantenimiento de los sistemas de información.	**A12.2.2** Control de procesamiento interno. **A12.6.1** Control de Vulnerabilidades técnicas
Sistemas internos	* Incompleta documentación de un sistema	3	* Falta de manuales de uso acerca de	3	3	9	Reducir o controlar la probabilidad de ocurrencia	**A.10** Gestión de comunicaciones y operaciones	**A.10.8.1** Procedimientos y políticas de información y software

			las aplicaciones.						

Tabla 3. 12 AMENAZAS Y VULNERABILIDADES
Fuente: Los autores

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.
La organización según la norma ISO 27001 debe contar con una DECLARACION DE LA APLICABILIDAD, la misma consiste en un documento que comprometa e identifique los controles del anexo A de la Norma que se implementarán y la justificación en caso de que no proceda. Esto significa que por defecto todos los controles de la norma son aplicables a la organización y cualquier excepción debe ser justificada.
La declaración de aplicabilidad debe ser aprobada y revisada por la alta dirección de la empresa.

3.8.5 CONTROLES DE LA NORMA (ANEXO A[125])

En base a las vulnerabilidades identificadas se detallarán los controles que ayudarán a cubrir las vulnerabilidades cada uno de los números colocados son los números en la tabla de Anexos de la Norma ISO 27001, simplemente se lo coloca para tener de una forma más detallada y completa el control descrito.

Control A.11.5.2 de la Norma ISO 27001

Identificación y Autenticación del Usuario(REFERENCIA AL ANEXO 2)

Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.

Control A11.6.1 de la Norma ISO 27001

Restricción al acceso a la información (REFERENCIA AL ANEXO 1)

Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida

Control A.8.2.2 de la Norma ISO 27001

[125]ISO27000, ISO 27000, 2012-09-03, http://www.iso27000.es/download/doc_iso27000_all.pdf

Capacitación y educación en seguridad de la información (REFERENCIA AL ANEXO 4)

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Control A12.2.2 de la Norma ISO 27001

Control de procesamiento interno (REFERENCIA AL ANEXO 3)

Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados

A12.6.1 Control A12.6.1 de la Norma ISO 27001

Control de Vulnerabilidades técnicas (REFERENCIA AL ANEXO 1)

Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado

Control A.10.8.1 de la Norma ISO 27001

Procedimientos y políticas de información y software (REFERENCIA AL ANEXO 2)

Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

3.8.6 MEDICIÓN DE EFECTIVIDAD DE LOS CONTROLES DE LA NORMA

(ANEXO A[126])

Una vez que están claros cuáles serán los controles que se van a aplicar es necesario revisarlos de una forma periódica para saber si el objetivo del control se está cumpliendo correctamente.

La medición de la efectividad de los controles se puede hacerlo mediante indicadores de efectividad, los indicadores que se utilizara se manejaran con los siguientes parámetros.

EFICACIA		EFICIENCIA		EFECTIVIDAD
RA / RE		$\frac{(RA / CA * TA)}{(RE / CE * TE)}$		$\frac{\text{Puntaje eficiencia} + \text{Puntaje eficacia}}{2}$ / Máximo puntaje
RANGOS	**PUNTOS**	**RANGOS**	**PUNTOS**	
0 – 20%	0	Muy eficiente > 1	5	La efectividad se expresa en porcentaje (%)
21 – 40%	1			
41 – 60%	2	Eficiente = 1	3	
61 – 80%	3			
81 – 90%	4	Ineficiente < 1	1	
>91%	5			

Donde R = Resultado, E = Esperado, C = Costo, A = Alcanzado, T = Tiempo

www.planning.com.co

Fig. 3. 36 Medición de Efectividad
Fuente: www.planning.com.co

Ejemplo:

Se va a tratar el Control Procedimientos y Políticas de información y software.

- Eficacia = RA/RE ; Eficacia en el control de procedimientos= 70/90 = 0.96
- Eficiencia=(RA/CA*TA)/(RE/CE*TE) = (70/70*100)/(90/90*100)= 1

[126]ISO27000, ISO 27000, 2012-09-03, http://www.iso27000.es/download/doc_iso27000_all.pdf

- Cabe aclarar que en el punto anterior los resultados de Costo Alcanzado, así como Costo Esperado son los mismos de resultados del Resultado Alcanzado y Resultado Esperado, debido a que no difiere en ningún costo para la operación debido a que son procedimientos de información y software; los valores de Tiempo Alcanzado y Tiempo Esperado se basan en una regla de tres debido a que el tiempo medido si es un mes equivale al 100%, si son menos días en los que se realiza la medida tendrá que aplicarse dicha regla para tener valores acordes.
- Efectividad= ((Puntaje eficiencia+ puntaje eficacia)/2)/ Máximo puntaje
- Efectividad= ((1+ 0.96)/2)/5= 0.29 en porcentaje 29% por lo tanto ingresa al rango como un control muy eficiente.
- Para realizar la medición de efectividad en otros controles será necesario revisar si la formula anteriormente presentada puede ajustarse a lo indicado, de no hacerlo se deberá optar viendo los campos más representativos dentro del control que puedan medirse, es decir por ejemplo para un enlace de datos se deberá optar por medición de tiempo del enlace on line sobre el tiempo de caída para saber si realmente el control de la efectividad de este activo está dentro de los parámetros establecidos para la empresa.

3.8.7 AUDITORIA DE CONTROLES

La auditoría de los controles se llevará a cabo de la siguiente manera:

- Definir los auditores internos por medio de la direcciones de la empresa, dichos auditores deben estar capacitados y conocer de la norma ISO27001:2005 para realizar este trabajo.
- Los auditores internos serán los encargados de realizar el procedimiento de auditoría de los controles en cada uno de los riesgos establecidos, esta auditoría se puede realizar de la siguiente manera:
- Revisar la tabla de tasación de activos 3.6 y comprobar con el personal del área de Sistemas Internos que se encuentren todos los activos establecidos, en caso de

haber aumentado algún activo colocarlo en la tabla y definir cada uno de sus valores.

- Revisar la tabla de activos por proceso 3.7 y comprobar con el personal del área de Sistemas Internos que se encuentren todos los activos por proceso distribuidos en los procesos ya establecidos (Administración de la información, Monitorización, Aprovisionamiento y Mantenimiento), en caso de haber aumentado algún activo colocarlo en la tabla según el proceso al cual pertenezca.
- Revisar la tabla de Amenazas y Vulnerabilidades 3.8 y comprobar con el personal del área de Sistemas Internos que se encuentren todas las amenazas y vulnerabilidades distribuidas con cada uno de los activos informáticos en caso de haber aumentado algún activo colocarlo en la tabla y definir cada uno de sus valores.
- Revisar la tabla de Amenazas y Vulnerabilidades 3.9 y comprobar con el personal del área de Sistemas Internos que se encuentren todos los objetivos de control y los controles de la norma ISO27001, asociados con cada uno de los activos en caso de haber aumentado algún activo colocarlo en la tabla y definir cada uno de sus objetivos de control y los controles de la norma ISO27001
- Los controles establecidos para cada uno de los activos en donde su valor máximo supera a los 6 puntos, serán revisados con el Anexo A de la norma ISO27001, en caso de aumentar algún activo y sea necesario asociar un nuevo control a los antes ya establecidos, se procederá a realizar la revisión de la solución aplicable al nuevo control.
- Revisar la vigencia del control con la normativa establecida por la ISO 27001, se deberá tomar en cuenta cuál es la última versión de la norma que se encuentre publicada.
- Revisar que se encuentre cumpliendo y llevando a cabo la ejecución del control.
- Realizar un informe que permita conocer los pasos realizados para la auditoría de los controles, así como las observaciones encontradas en ellos.
- En caso de existir observaciones establecer un tiempo prudencial para corregir estas observaciones así como responsables encargados de ejecutar un plan de acción que corrija lo hallado.

- Una vez que ha pasado la fecha límite para corregir las observaciones revisar si se ha llegado a cumplir con la corrección del hallazgo.

3.8.8 RIESGOS RESIDUALES

Los riesgos residuales son todos aquellos riesgos permanentes que aun cuando se haya implementado todos los controles necesarios no dejan de existir por a o b motivo, un ejemplo claro de esto es el riesgo que existe en la pérdida de información o acceso a un determinado sistema por parte del usuario pues a pesar que se maneje todos los controles el usuario es la única persona que actúa directamente con el sistema y ya sea por descuido o mal manejo de la información se debe educar al usuario para que haya cada vez menos incidentes de esta naturaleza.

Una vez realizado el diseño del SGSI es necesario obtener la aprobación por parte de la gerencia de la empresa esto se realizará mediante una propuesta formal descrito en un documento a manera de resumen ejecutivo, dicho documento se procede a realizar en el siguiente capítulo.

3.8.9ENUNCIADO DE APLICABILIDAD:

Según la descripción de la norma ISO27001 en donde menciona se debe tener los siguientes campos dentro del enunciado de aplicabilidad: los objetivos de control y los controles seleccionados anteriormente, razones para su selección, objetivos de control, controles implementados actualmente, exclusión de cualquier objetivo de control.

Con esa premisa se procede a realizar la siguiente tabla:

Objetivos de control	**Controles Seleccionados**	**Razones para su selección**	**Controles implementados actualmente**
Elegir una técnica de autenticación adecuada para verificar la identidad del usuario.	Identificación y Autenticación del Usuario	Permitirá tener un orden establecido para la identificación.	Políticas de seguridad de la empresa
Restringir el acceso de los usuarios y personal de soporte al sistema de	Restricción al acceso a la información	No todos los usuarios tienen la necesidad de ingresar a todos los sistemas de la	Políticas de seguridad de la empresa

información		empresa.	
Recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales	Capacitación y educación en seguridad de la información	El conocimiento es una parte esencial dentro de cualquier empresa, permitirá un mejor entendimiento de hacia a donde se quiere llegar.	Políticas de seguridad de la empresa
Detectar cualquier corrupción de la información	Control de procesamiento interno	Se puede prevenir la pérdida de la información.	Políticas de seguridad de la empresa
Evaluar la exposición de la organización ante las vulnerabilidades	Control de Vulnerabilidades técnicas	El realizar un análisis de vulnerabilidades permite la prevención a la ocurrencia de cualquier incidente.	Políticas de seguridad de la empresa
Proteger el intercambio de información	Procedimientos y políticas de información y software	Se debe controlar el porqué del intercambio de información, pues no siempre es necesario realizar copias de la información de la empresa.	Políticas de seguridad de la empresa
EXCLUSIONES DEL OBJETIVO DE CONTROL			
En este punto se debe proceder a la explicación de el por qué no es tomado en cuenta algún objetivo de control propuesto por el área de Sistemas Internos o algún control sugerido por la gerencia una vez que ya se haya realizado la propuesta formal para la implementación del sistema.			

Tabla 3. 13 Enunciados de aplicabilidad
Fuente: Los autores

Cabe destacar que cuando se encuentra implementado el SGSI se debe realizar un plan de acción para establecer responsables para la implementación de cada uno de los objetivos de control así como fechas límites para poder llegar a cumplir los objetivos del control descritos anteriormente, una vez ejecutado el plan de acción deberá tener la aprobación por la gerencia de la empresa para la inmediata ejecución.

Los siguientes puntos descritos se abarcarían una vez realizada la implementación, pero como parte del presente estudio se procede a describir premisas generales que permitan tener una idea clara y concreta de cómo se puede llegar a realizar los puntos indicados.

3.9 MONITOREAR Y REVISAR EL SGSI

El monitoreo del SGSI consiste en que por medio de un delegado por el área realice un proceso de revisión en cada uno de los activos mediante la tabla de Amenazas y Vulnerabilidades fijándose en cada uno de los puntos descritos y observando incidencias que puedan ser agregadas en dicha tabla para luego proceder con el proceso de adición en cada una de las tablas descritas en el diseño, es importante que se realice dicha revisión con una frecuencia de por lo menos una vez al mes, o cuando se instale una nueva aplicación, o haya un cambio significativo en la infraestructura de la organización que implique cambios en los equipos en donde se encuentra almacenada la información sensible de la organización.

La revisión será establecida por medio de la gerencia de la empresa, al establecer una frecuencia de un mes para el monitoreo, de la misma forma se deberá pedir informes que muestren como se está avanzando en cada uno de este proceso, esto con el fin que todas las partes involucradas se encuentren al tanto de cómo se está llevando a cabo el SGSI.

Una vez realizado el monitoreo y realizada la revisión se debe proceder con una reunión en donde se conozcan los resultados obtenidos en la revisión mensual esta reunión puede realizarse en un periodo de tres meses, en donde se podrá tener una clara idea de los cambios establecidos en caso de que se hayan producido y la consecuencia de cada uno de ellos.

3.10 MANTENER Y MEJORAR EL SGSI

Para poder mantener y mejorar un SGSI se debe tomar en cuenta en primer lugar las auditorias las mismas que nos ayudarán a darnos cuenta si los objetivos de control se están cumpliendo a cabalidad. El mejoramiento del SGSI consistirá en el compromiso de cada uno de los usuarios en tener claro las políticas de control antes ya establecidas así como las nuevas políticas a publicarse, además el compromiso del área de Sistemas internos para que proceda a un constante análisis de cada uno de los activos que se han detectado con cierto grado de afectación esto permitirá que los riesgos

sean mitigados y no permitan la ocurrencia de ninguno de ellos, el compromiso de la gerencia permitirá que se pueda establecer nuevos controles mediante su aprobación, todo este funcionamiento en conjunto permitirá el manejo de un SGSI de forma clara y ordenada sin que en ningún momento exista un punto de fallo en donde se pueda afectar directamente a la continuidad del negocio.

Las auditorías internas son realizadas por los empleados de la empresa los mismos quienes han recibido una previa capacitación acerca de la norma ISO27001 y tienen una certificación de auditor interno en la norma ISO27001, otorgado por una empresa certificadora de la norma ISO27001. Se puede proceder con la auditoría interna de la siguiente manera:

1. Comunicado por parte del representante de los directores de área con una semana de anticipación las fechas y horario en las cuales se procederá a realizar la auditoría.
2. Reunión de apertura.- en esta reunión se encontrarán las siguientes personas: directores de área, auditores internos, dueños de los procesos a ser auditados (Administración de la información, Monitorización, Aprovisionamiento y Mantenimiento), se realiza la reunión de apertura describiendo la agenda con las tareas establecidas para el día de la auditoría.
3. Inicio de la auditoria.- Los auditores internos se dirigirán hacia los puestos de trabajo de los dueños de los procesos.
4. Desarrollo de la auditoría.- Los auditores están en pleno derecho de pedir a los auditados toda la información necesaria para la justificación de lo establecido por la norma ISO27001 se encuentre cumpliendo en su totalidad, en caso de que por cualquier motivo el auditado no pueda justificar algún punto de la ISO27001 preguntado por el auditor, el auditor se encuentra en todo el derecho de establecer una acción correctiva AC, una acción preventiva AP, una oportunidad de mejora, definiendo tiempos de finalización, persona a cargo para solucionar cualquiera de los hallazgos antes mencionados.
5. Finalización de la auditoría.- En esta reunión se encontrarán las siguientes personas: directores de área, auditores internos, dueños de los procesos auditados, se procederá a la lectura de los hallazgos encontrados en cada uno de los

procesos, y por medio del representante de las direcciones se redactará un informe de la auditoría realizada.

6. Los hallazgos encontrados se revisarán una cuando se haya terminado la fecha de finalización para corregir dicho hallazgo, en caso que no se haya completado.
7. la actividad se deberá justificar por medio de un informe para los directores de área el por qué no se completó la actividad.

Las Auditorías Internas sirven para corregir cualquier hallazgo en la norma ISO27001 establecida en la empresa, y de esta forma estar preparados para que en la Auditoría Externa sean mínimas las observaciones.

A continuación se presenta una tabla en donde se puede registrar los hallazgos obtenidos el momento de realizar una auditoría interna.

Número	**Fecha de Apertura**	**Tipo**	**Origen**	**Área**	**Hallazgo**	**Responsable**	**Acciones Preventivas**	**Acciones Correctivas**	**Plazo**
1	5-26-2012	AC	Sistemas Internos	Sistemas	Los full backups de las máquinas de los usuarios no se están ejecutando debido a la falta de espacio en el servidor de respaldos	Sistemas		Ampliar el espacio en el servidor de respaldos para poder ejecutar los backups cada fin de mes.	6-26-2012

Tabla 3. 14 Auditoría Interna
Fuente: Los autores

3.11 AUDITORÍAS EXTERNAS

Las auditorías externas son realizadas por una empresa certificada en la norma ISO 27001, esta auditoría es planificada por la empresa certificada por lo general los pasos son similares a los descritos en la auditoría interna.

A continuación se procede a realizar la propuesta formal hacia la gerencia para el diseño del SGSI, en un documento redactado a manera de resumen ejecutivo.

CAPITULO IV

PROPUESTA DE IMPLEMENTACIÓN DEL PROYECTO

4.1 PRESENTACIÓN

Comware cuenta actualmente con la norma ISO 9001 2008, por más de 6 años, la cual está enfocada al manejo de todos los procesos que son:

Gerencial:
Dirección General
Soporte:
Finanzas
Sistema de Gestión de Calidad
Talento Humano
Remuneraciones y Compensaciones
Salud y Seguridad Ocupacional
Sistemas Internos
Ejecución:
Ventas
Servicios
Logística

En el caso de la Norma ISO 27001, veremos que esta netamente enfocada al proceso de Sistemas Internos (Tecnologías de la Información y Comunicación "TIC"), pero cabe recalcar que el impacto será dentro del funcionamiento de todos los procesos. Por tanto, es un punto positivo que la compañía ya cuente con una certificación, por lo que la implantación de la norma propuesta será más sencillo, y al mismo tiempo algunos procedimientos no deben ser ejecutados, ya que, al ser ya certificados podemos omitirlos , y esto se encuentra documentado en la matriz de compatibilidad de la

normas. Sin duda, los frutos que nos generará costo- beneficio este proyecto, será evidenciado en los resultados.

El siguiente diagrama muestra claramente cómo funciona el Sistemas de gestión de Calidad de Comware.

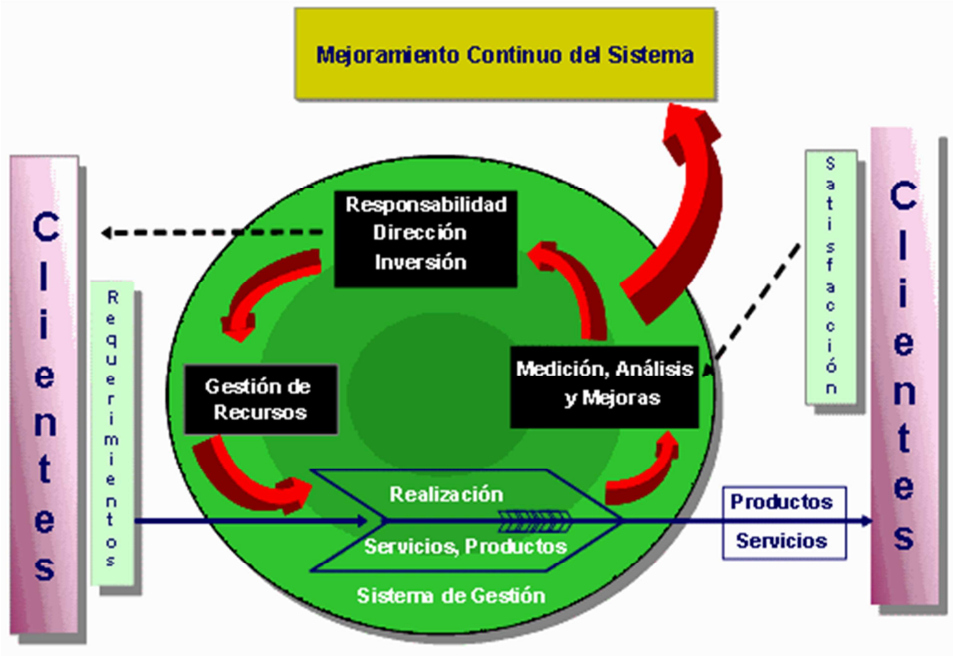


Fig. 4. 1 Diagrama de Sistemas de Gestión de Calidad
Fuente: http://www.monografias.com/trabajos55/evaluacion-economica-proyectos/Image9540.gif

4.2 PROPUESTA DEL PROYECTO

Objetivo:

Implementación de un Sistema de Gestión de Seguridad de la Información para la empresa Comware S.A en la ciudad de Quito, basado en la Norma ISO 2700:2005.

Metodología:

En primera instancia se realizará el análisis de la red por medio de varias herramientas de software, con el fin de poder evidenciar claramente las amenazas y riesgos, que se encuentran presentes dentro de las tecnologías de la información y comunicación (TIC)

y de este modo reducir el impacto que puede generar el mal funcionamiento de los equipos de tecnología de la organización.

Por lo dicho, el análisis de riesgos de seguridad en la red serán identificados, minimizados, prevenidos y solucionados en base a los procedimientos establecidos para el tratamiento de los mismos, poniendo énfasis en la mejora continua.

Además, mediante este proyecto proporcionaremos los lineamientos básicos para el desarrollo de la seguridad de la información, identificando así los activos más importantes para la empresa mediante un análisis, evaluación y control de vulnerabilidades. Es importante nombrar que para realizar una gestión de riesgos adecuada, necesitamos contar con diferentes alternativas para el tratamiento de los mismos, y de este modo, definir los controles adecuados, y alineados a la estrategia de la empresa.

Impacto:

El impacto que esperamos lograr con este proyecto, está enfocado a la mejora de todos los procesos de la compañía (ejecución, soporte y gerenciales), por tanto, al implementar este proyecto Comware S.A., podrá ver un impacto positivo en los siguientes aspectos:

- Mejora en la satisfacción del cliente interno y externo
- Reducción de costes, ya que los riesgos serán analizados y solucionados antes de que generen problemas dentro de la compañía.
- Contar con sistemas seguros, que ayudarán a reducir los impactos y riesgos dentro de la seguridad de la información.
- Al ser una certificación de calidad, genera un plus dentro del mercado, ya que, los competidores dentro del segmento como Maint, Desca, Totaltek, Sinetcom, TeUno, Binaria, AndeanTrade, La Competencia, Akross , Vonext , no poseen esta certificación, lo cual nos genera automáticamente un mayor posicionamiento dentro del mercado tecnológico.

- Reducción dentro de los gastos de infraestructura tecnológica, esto sin duda se podrá evidenciar en las variaciones del presupuesto asignado a esta área, ya que, al implementar este proyecto, los gastos que actualmente se tiene con proveedores , bajarán, puesto que, Comware, cuenta actualmente con estos servicios, para la solución de los problemas suscitados dentro de la plataforma tecnológica.
- Al procesar los requerimientos de forma oportuna y eficaz, sin duda la imagen de la compañía subirá, y con esto las ventas aumentarán.

Diagrama de Impactos:

Fig. 4. 2 Diagrama de Sistemas de Gestión de Calidad

Fuente: http://calidadavanzada.blogspot.com/2010/10/mejora-continua.html&docid=zFu8TcgWz6J2oM&imgurl

4.3 DEMOSTRACION DE RESULTADOS

En base al análisis del realizado, los resultados encontrados están descritos en la siguiente tabla:

Objetivos de control	**Controles Seleccionados**	**Razones para su selección**	**Controles implementados actualmente**
Elegir una técnica de autenticación adecuada para verificar la identidad del usuario.	Identificación y Autenticación del Usuario	Permitirá tener un orden establecido para la identificación.	Políticas de seguridad de la empresa
Restringir el acceso de los usuarios y personal de soporte al sistema de información •	Restricción al acceso a la información	No todos los usuarios tienen la necesidad de ingresar a todos los sistemas de la empresa.	Políticas de seguridad de la empresa
Recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos	Capacitación y educación en seguridad de la información •	El conocimiento es una parte esencial dentro de cualquier empresa, permitirá un mejor	Políticas de seguridad de la empresa

organizacionales		entendimiento de hacia a donde se quiere llegar.	
Detectar cualquier corrupción de la información	Control de procesamiento interno	Se puede prevenir la pérdida de la información.	Políticas de seguridad de la empresa
Evaluar la exposición de la organización ante las vulnerabilidades	Control de Vulnerabilidades técnicas	El realizar un análisis de vulnerabilidades permite la prevención a la ocurrencia de cualquier incidente.	Políticas de seguridad de la empresa
Proteger el intercambio de información	Procedimientos y políticas de información y software	Se debe controlar el por qué del intercambio de información, pues no siempre es necesario realizar copias de la información de la empresa.	Políticas de seguridad de la empresa
• EXCLUSIONES DEL OBJETIVO DE CONTROL			
• Las exclusiones son las siguientes: • Control A.8.2.2 de la norma Iso 27001 • Capacitación y educación en seguridad de la información. • Control A.11.5.2 de la norma Iso 27001			

- Identificación y Autenticación del Usuario.

Control A12.2.2 de la norma Iso 27001

Control de procesamiento interno**.**

- Las exclusiones de los objetivos de control se han debido a que según los análisis realizados en la tabla 3.12 Amenazas y Vulnerabilidades, no son relevantes dentro del estudio debido a que el puntaje para ser tomado en cuenta un control es mayor a 6 puntos.

Tabla 4. 1 Demostración De Resultados
Fuente: Los autores

En base a la fase de análisis/ evaluación, podremos detectar las oportunidades mejora, en base a los resultados, los cuales serán reportados tanto a la jefatura de Sistemas Internos como a la Dirección del área. Por otro lado, los resultados serán entregados en base al desarrollo del proyecto, ya que en primera instancia los resultados, serian una herramienta clave para la toma decisiones en la implantación.

Es importante nombrar que la retroalimentación, debe tener un objetivo clave, que es prevenir futuros problemas y al mismo tiempo, tomar acciones objetivas (plan de acción) en base a los resultados que este proyecto genere en todas sus fases.

4.4 GENERACIÓN Y ENTREGA DE INFORMES.

Entrega de informes por fase	**Tipo de informe**
1. **Detección de necesidad o problema:**	Informes de status actual de la compañía
• Análisis funcional	Informe de los estudios ejecutados
• Evaluación	Informe de resultados
• Validación	Informe de pruebas realizadas de los sistemas
• Implementación / ejecución	Informe del plan y documentación
• Seguimiento y Control	Informes periódicos en base al desarrollo del proyecto
• Mejora continua	Informes de auditorias
• Presupuesto	Plan anual

Tabla 4. 2 Demostración De Resultados
Fuente: Los autores

La entrega de informes, deberá ser después de la finalización de cada fase, en el caso de ser necesario para cualquier cambio de políticas organizacionales, procedimientos y/o manuales, se deberá emitir un informe para la Dirección General, ya que, sin duda esto afecta a la estrategia de la organización, y la decisión debe ser por parte de la dirección.

Las herramientas, que utilizaremos para la generación de informes, serán el Jd Edwards y Project, las cuales nos permitirán gestionar los resultados de manera más viable y real. Por otro lado, debemos estar conscientes que al manejar dichas herramientas, es necesario que se vaya ingresando la información, a la par que se va desarrollando el proyecto.

4.5 FASES Y OBJETIVOS:

1. **Detección de necesidad o problema:**

Complementar el sistema ISO 9001:2008, con un sistema de gestión de seguridad de la información basado en la norma ISO 27001, y de esta manera poder posicionarse como una empresa líder en integración de servicios de computación y comunicaciones.

2. **Análisis funcional:**

Analizar la necesidad de Comware S.A., por medio de los diferentes estudios ejecutados dentro de los procesos que tiene la empresa para gestión de la seguridad informática.

3. **Evaluación:**

Evaluar cada uno de los análisis realizados acorde al criterio del área encargada de Sistemas internos, mediante una exhaustiva revisión de los sistemas para que se pueda tener mayor afectación en la continuidad y estrategia del negocio.

4. **Validación:**

La validar la viabilidad del proyecto mediante la matriz de compatibilidad de la ISO en donde indica que las normas ISO 9001:2008 e ISO 27001:2005 son compatibles, además que se pueden obviar ciertos pasos que ya se encuentran establecidos en la norma ya certificada.

5. **Implementación / ejecución:**

Implementar en base al documento que precede este informe, tomando en cuenta los lineamientos establecidos por la norma ISO 27001:2005

6. **Seguimiento y Control:**

Hacer el respectivo seguimiento y control, una vez realizada la implementación, y que se deberán hacer seguimientos, y controles periódicos del correcto funcionamiento de la norma establecida. El plazo para estos seguimientos será designado por las direcciones de la empresa

7. **Mejora continua:**

Priorizarla mejora continua, por lo que todo sistema de calidad está enfocado al análisis de cada uno de los procedimientos establecidos, para determinar un plan de acción y de este modo obtener mayores beneficios e impactos de la norma.

Diagrama de funcionamiento de fases:

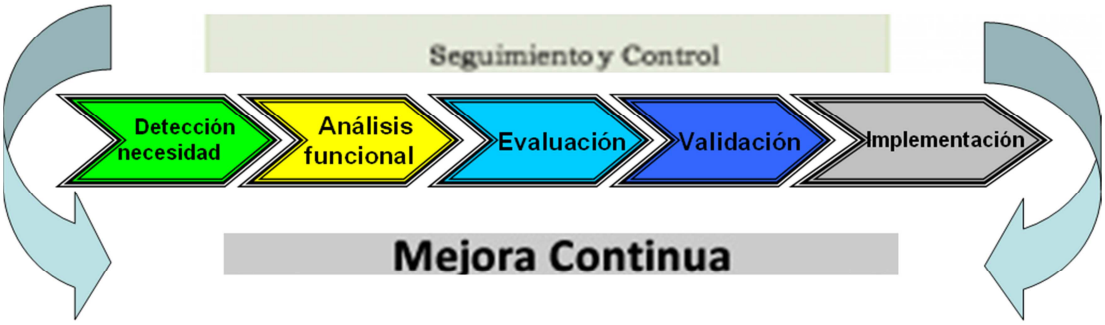


Fig. 4. 3 Diagrama de Sistemas de Gestión de Calidad
Fuente: La Empresa

La detección de fases es en base al negocio, y estrategia de Comware S.A

PRESUPUESTO.

PLANTILLA PRESUPUESTO IMPLANTACIÓN ISO 27001 AÑO 2013					
PLAN DE PROYECTO ISO 27001	Q1	Q2	Q3	Q4	TOTALES
CAPACITACIÓN DE INDUCCION Y AUDITORES INTERNOS IN COMPANY		1,500		3,000	4,500
IMPLEMENTACIÓN	300	300			600
CERTIFICACIÓN POR SGS	3,000				3,000
CONSULTORÍA	250		250		500
AUDITORÍA	150		150		300
EQUIPOS DE SOFTWARE , HARDWARE/ ACTUALIZACIONES	250	250	250	250	1,000
				TOTAL	9,900

Fig. 4. 4 Plantilla presupuesto de Implementación
Fuente: Los autores

El presupuesto fue, realizado en base a propuestas enviadas por el proveedor SGS, por otro lado es importante recalcar que los valores son sin IVA, y dichos costos son en base a los requerimientos, que tiene actualmente Comware S.A. para la implantación de este proyecto.

Sin duda el Retorno de la inversión “ROI” de este proyecto, está planificado para que sea en menos de un año, ya que al reducir los costes de los servicios que nos prestan nuestros proveedores al año que es un valor presupuestado de $15.000, podemos deducir que la inversión de este proyecto tendrá un retorno a corto plazo, con el ahorro en los servicios que nos prestan los proveedores ,y de este modo generará una utilidad medible dentro de los ratios financieros que posee actualmente Comware S.A.

4.7 CRONOGRAMA ANUAL

A continuación, se describe el cronograma de la planificación del proyecto en donde cada Q representa un trimestre, cabe aclarar que el cronograma se encuentra realizado para un periodo a corto plazo de un año.

	Q1			Q2			Q3			Q4		
FASES	MES 1	MES 2	MES 3	MES 1	MES 2	MES 3	MES 1	MES 2	MES 3	MES 1	MES 2	MES 3
DETECCION DE NECESIDADES	X											
ANALISIS FUNCIONAL		X	X	X								
EVALUACIÓN					X							
VALIDACION						X						
IMPLEMENTACION / EJECUCIÓN							X	X	X	X	X	
SEGUIMIENTO Y CONTROL			X			X			X			X
MEJORA CONTINUA												X
PRESUPUESTO					X							

Fig. 4. 5 Cronograma Anual
Fuente: Los autores

El resumen de los tiempos empleado en el proyecto es representado en la siguiente tabla

RESUMEN DE TIEMPOS	
FASES	TIEMPO EN MESES
DETECCION DE NECESIDADES	1
ANALISIS FUNCIONAL	3
EVALUACIÓN	1
VALIDACION	1
IMPLEMENTACION / EJECUCIÓN	5
SEGUIMIENTO Y CONTROL	4
MEJORA CONTINUA	1
PRESUPUESTO	1

Tabla 4. 3 Resumen de Tiempos
Fuente: Los autores

Fase crítica es aquella en donde el proyecto tiene mayor riesgo, por tanto requiere mayor atención y cuidado ya que, una falla dentro de dichas fases puede hacer que el proyecto fracase, es por ello, que la detección de fases criticas nos permiten tener

mayor énfasis dentro de las mismas, para así lograr reducir el riesgo y tomar acciones inmediatas dentro de cualquier desfase.

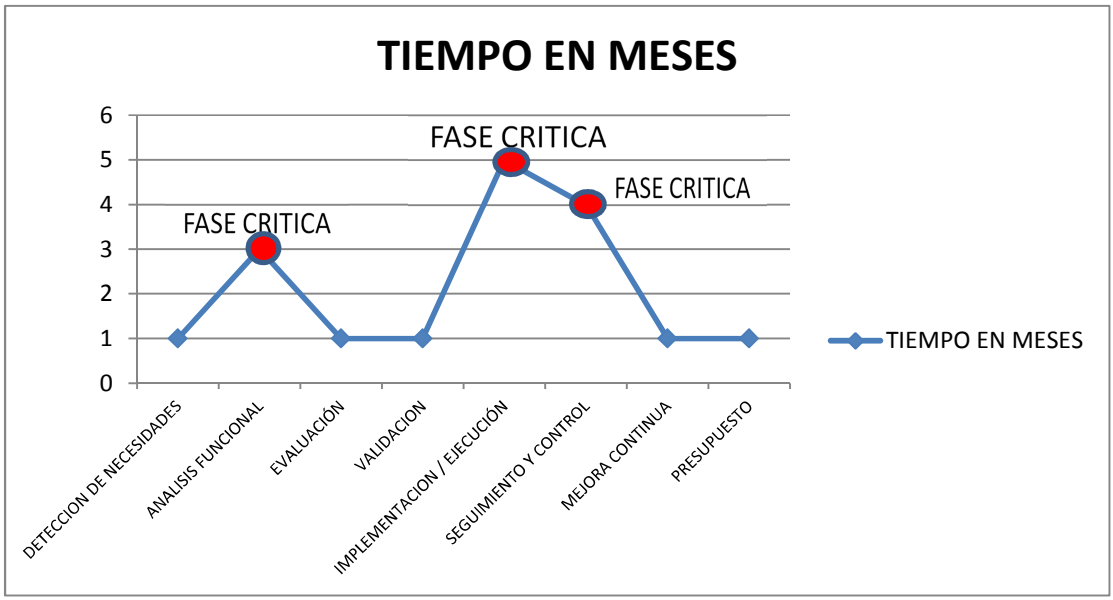


Fig. 4. 6 Tiempo en meses
Fuente: Los autores

Este cronograma puede variar en base al desarrollo del proyecto, pero cabe recalcar, que todo será manejado en los tiempos planificados, y las fases críticas contarán con un plan B, para que no afecten el desenvolvimiento del mismo.

4.8 Conclusiones:

En base a todo el análisis realizado, podemos afirmar que la viabilidad económica, y de gestión de este proyecto, es positiva, por tanto, al implementar la propuesta que detallamos en este informe, Comware S.A., mejorará su funcionamiento, y lo más importante es que todo esto será reflejado objetivamente en la satisfacción al cliente.

Conclusiones y Recomendaciones

CONCLUSIONES.

- Por medio del diseño de un SGSI basado en la Norma ISO 27001:2005 la empresa tiene una guía clara en donde puede basarse para la posterior implementación de dicha Norma.
- A través del uso de herramientas de software, se realizó el estudio de análisis de vulnerabilidades y riesgos en los sistemas informáticos para clasificarlos y puntuarlos según la incidencia ocurrida basado en la Norma ISO 27001:2005.
- La selección de los controles adecuados posteriormente al análisis de amenazas permitieron mitigar los riesgos existentes en base al estudio realizado.
- El mantener informado a las unidades gerenciales de la empresa y el estar conscientes de puntos de fallo dentro de los sistemas informáticos establece un compromiso para la mejora continua y compromiso de certificarse en la Norma ISO 27001:2005
- Al realizar un análisis de varios equipos informáticos se puede llegar a determinar que por diferentes motivos se han dejado en ocasiones puertos abiertos sin ningún control, lo cual puede ser causante de una brecha de seguridad muy grande dentro de la empresa, es importante que cada cambio realizado para pruebas sea registrado y luego borrado para asegurar que no existan brechas en la seguridad
- El momento que la empresa desee implementar un SGSI certificado bajo la norma ISO 27001:2005, esto no quiere decir que se cuenta con una seguridad máxima en la información de la organización, significa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además estará en continua mejora

- El mantener la información de los activos correctamente clasificada y ordenada permite al administrador de sistemas detectar los puntos de fallo de una forma más rápida y clara, de esta forma se puede reducir los tiempos de atención para la corrección y mitigación de riesgos

RECOMENDACIONES.

- El siguiente paso después del diseño es la implementación del sistema esto se debería realizar en un plazo no mayor a 6 meses por medio de una empresa calificada para que pueda realizar y certificar la norma ISO 27001:2005
- Se deberá capacitar a cada uno de los empleados en el uso de la norma y de preferencia tener auditores internos calificados para que los costos en las auditorías externas sean menores y no se encuentren tantos hallazgos.
- Se debe realizar análisis periódicos de los riesgos y monitorear continuamente, esto permitirá que cada vez se mitiguen más los riesgos y mejorara la continuidad del negocio.
- La persona encargada de la administración de sistemas debe documentar cada uno de los procesos dentro de la operación del negocio pues esto ayudará a que se maneje de una manera ordenada cada uno de los incidentes que puedan ocurrir en la empresa además de contar con una fuente de conocimiento de problemas resueltos en los incidentes registrados.
- Mantener una cultura de cambio en la empresa sabiendo que toda la información y procesos realizados por cada una de las áreas es vital para la continuidad del negocio.

ANEXOS

ANEXO 1

Para evitar que cualquier usuario o tercera persona ingrese directamente a la red de la empresa se propone utilizar el siguiente protocolo:

Protocolo AAA

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados:

Autenticación

La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, computador) y la segunda un servidor. La Autenticación se consigue mediante la presentación de una propuesta de identidad y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, o los números de teléfono en la identificación de llamadas.

Autorización

Autorización se refiere a la concesión de privilegios específicos a una entidad o usuario basándose en su identidad, los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son: filtrado de direcciones IP, asignación de direcciones,

asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Contabilización

La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

AAA es una pieza crítica de la infraestructura de red. AAA es lo que mantiene la red segura asegurándose de que sólo los usuarios adecuados son autenticados, que los usuarios sólo tienen acceso a los recursos de red adecuados, y que los usuarios se registran a medida que van sobre su negocio.

Configuración de AAA en el IOS de Cisco

Estos son los pasos a la configuración de la AAA:

- Activar la AAA
- Configuración de la autenticación, mediante RADIUS o TACACS +
- Definir las listas de método de autenticación
- Aplicar el método de las listas por línea / por interfaz

Es importante tener en cuenta que el software Cisco IOS intenta la autenticación con el método de autenticación de la próxima lista sólo cuando no hay respuesta por parte del método anterior. Si el servidor de seguridad o base de datos de usuario responde al negar el acceso de los usuarios, el proceso de autenticación y el usuario recibirá un usuario ha denegado el símbolo del sistema. Los comandos a utilizar son los siguientes:

Router (config) # aaa nuevo modelo

Router (config) por defecto de autenticación de inicio de sesión # aaa permiten

Router (config) # aaa autenticación PPP por defecto de grupo en grupo +TACACS radio locales

Router (config) # aaa autenticación PPP de manzana del grupo de radio en grupo + TACACS ninguno locales

Router (config) # interfaz asíncrona 3

Router (config-if) # pppauthenticationchap de manzana

También se puede realizar la autenticación RADIUS en Routers CISCO con integración de Active Directory

Instalar el servicio de IAS, para ello nos dirigimos al panel de control y luego a la opción de agregar o quitar programas y seleccionamos la opción de agregar o quitar componentes de Windows y nos posicionamos sobre la opción de servicios de red.

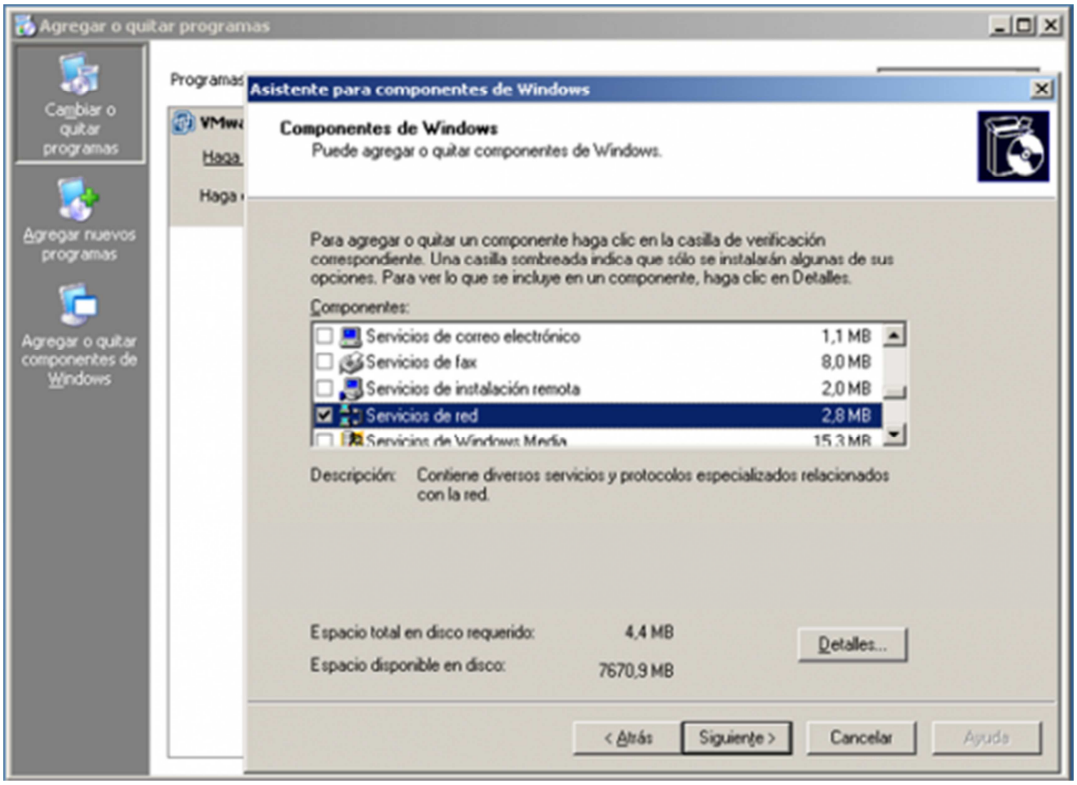


Figura A. 1 Asistente para componentes de Windows
Fuente: Los autores

Seleccionar la opción de servicios de autenticación de Internet, con ello se procede a instalar el servicio IAS, en el proceso de instalación se pedirá ingresar el disco de instalación de WindowsServer 2003.

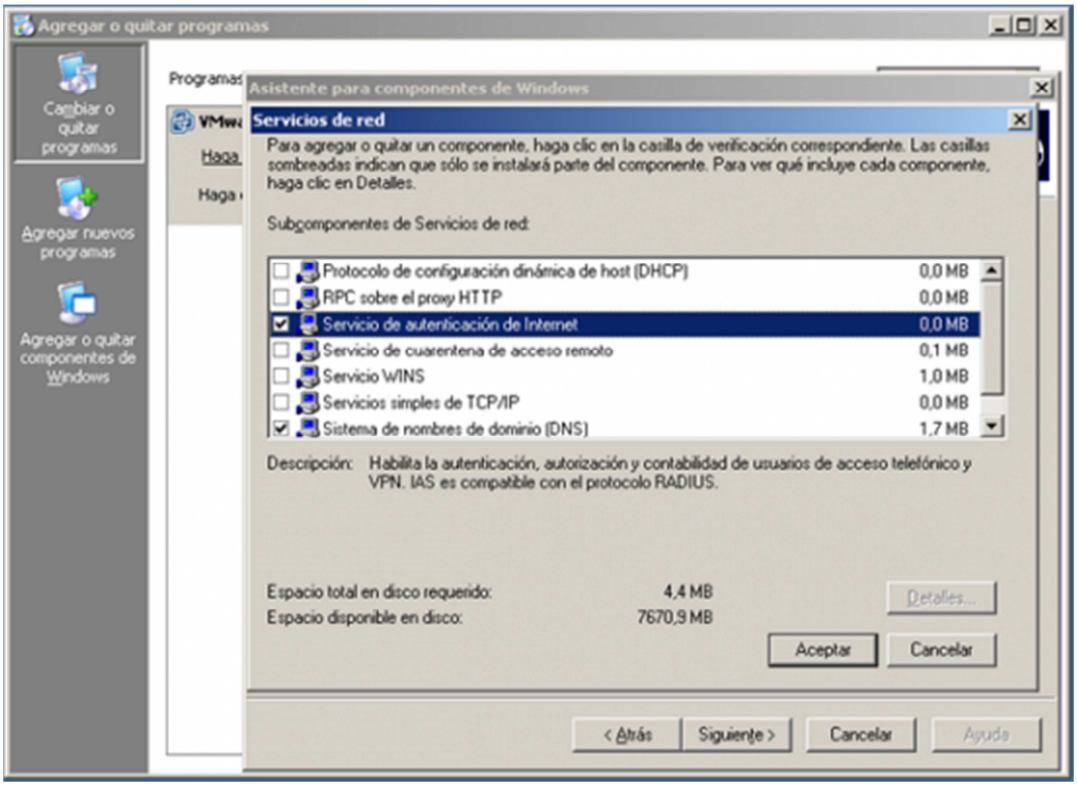


Figura A. 2 Servicios de Red
Fuente: Los autores

Ejecutar el servicio de la siguiente forma:

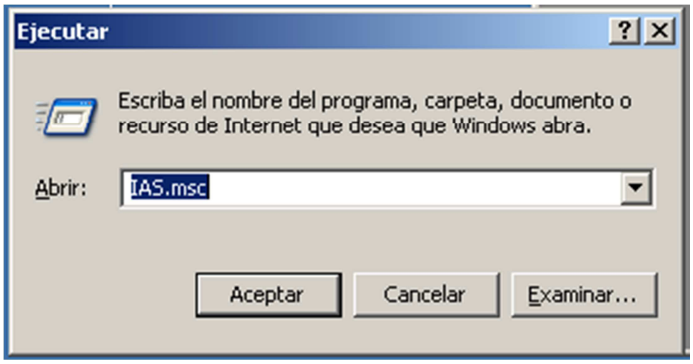


Figura A. 3 Ejecutar
Fuente: Los autores

Se habilitara la ventana de administración del servicio, desde donde se configurará el cliente, para poder autenticarnos contra un usuario que se encuentre en el Active

Directory, para este caso se puede utilizar un usuario de prueba y asociarlo al grupo CISCO ADMINS dentro del Active Directory.

PASO 1: Habilitar el servicio para que se utilice el Active Directory previamente configurado

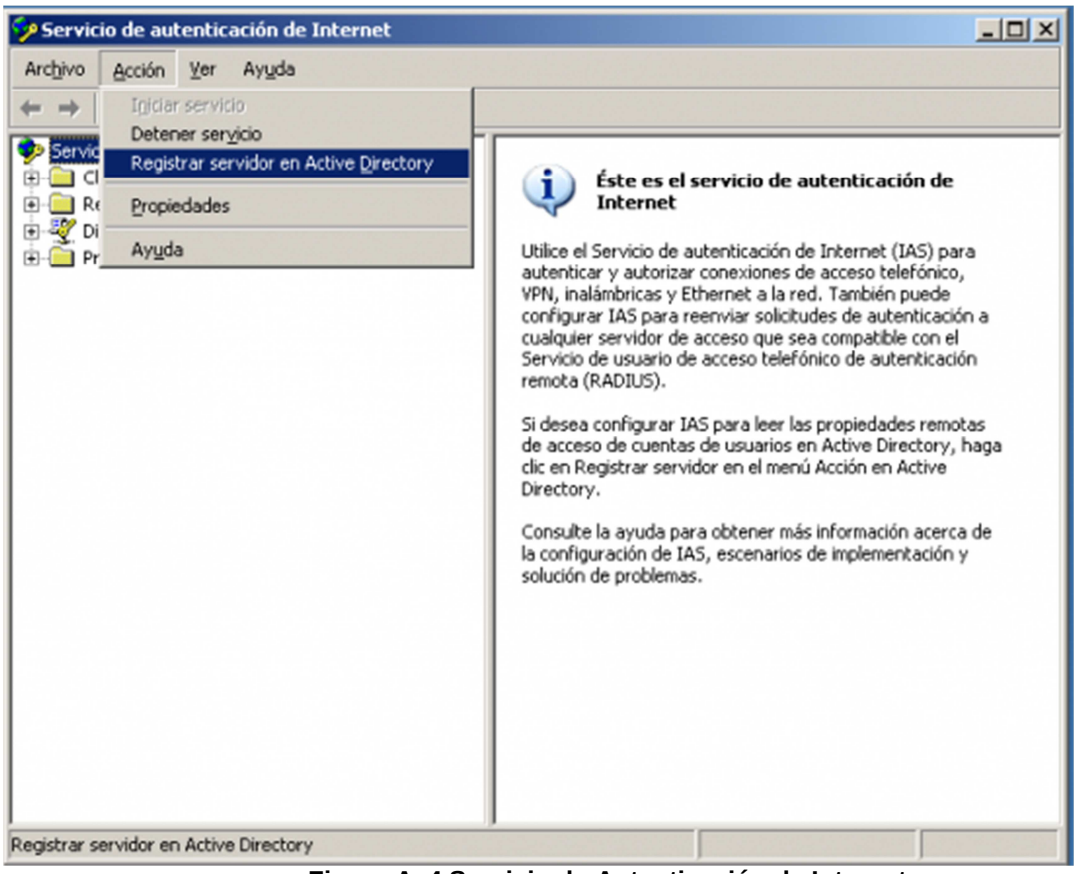


Figura A. 4 Servicio de Autenticación de Internet
Fuente: Los autores

Ubicamos la pestaña de clientes RADIUS y dentro de la ventana donde se muestran los clientes previamente registrados, click con el botón derecho y seleccionamos la opción de nuevo cliente RADIUS.

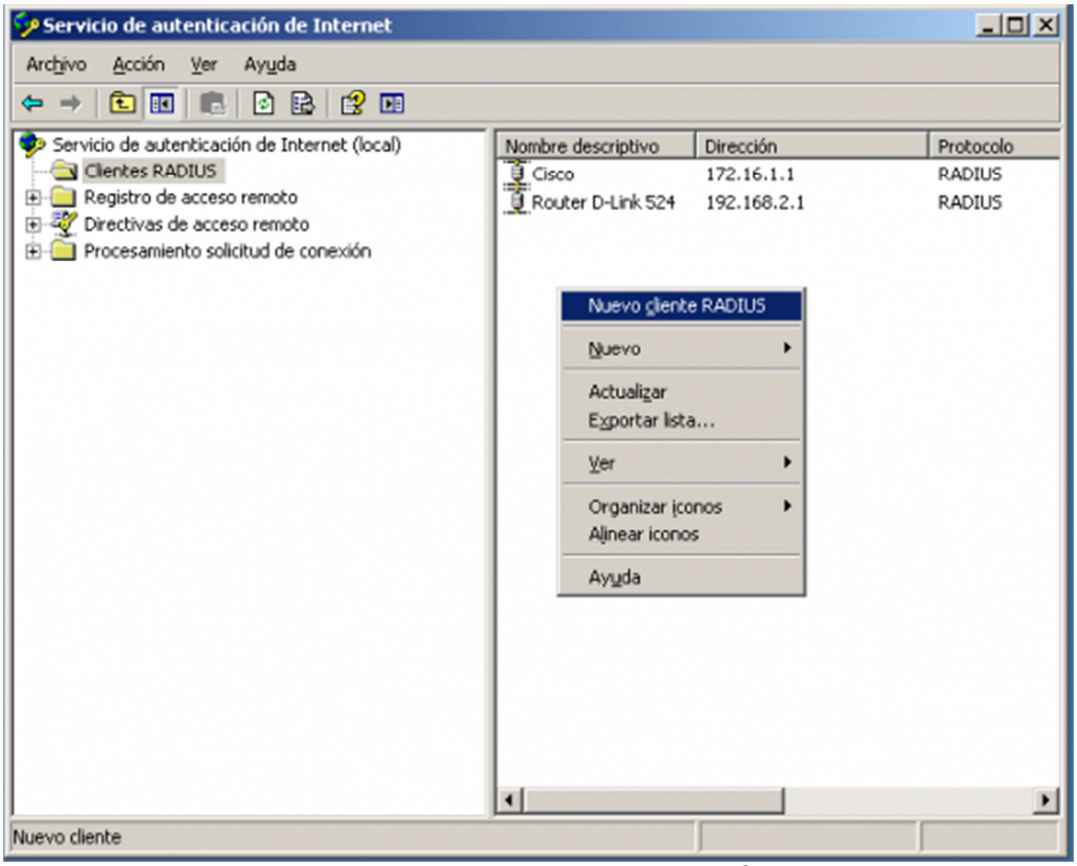


Figura A. 5 Servicio de Autenticación de Internet
Fuente: Los autores

Se debe colocar un nombre descriptivo que nos permita identificar al cliente y la dirección IP que este tenga asignado, para este ejemplo el router CISCO que se autenticara contra el servidor RADIUS tiene asignada la dirección IP 172.16.1.2, click en siguiente.

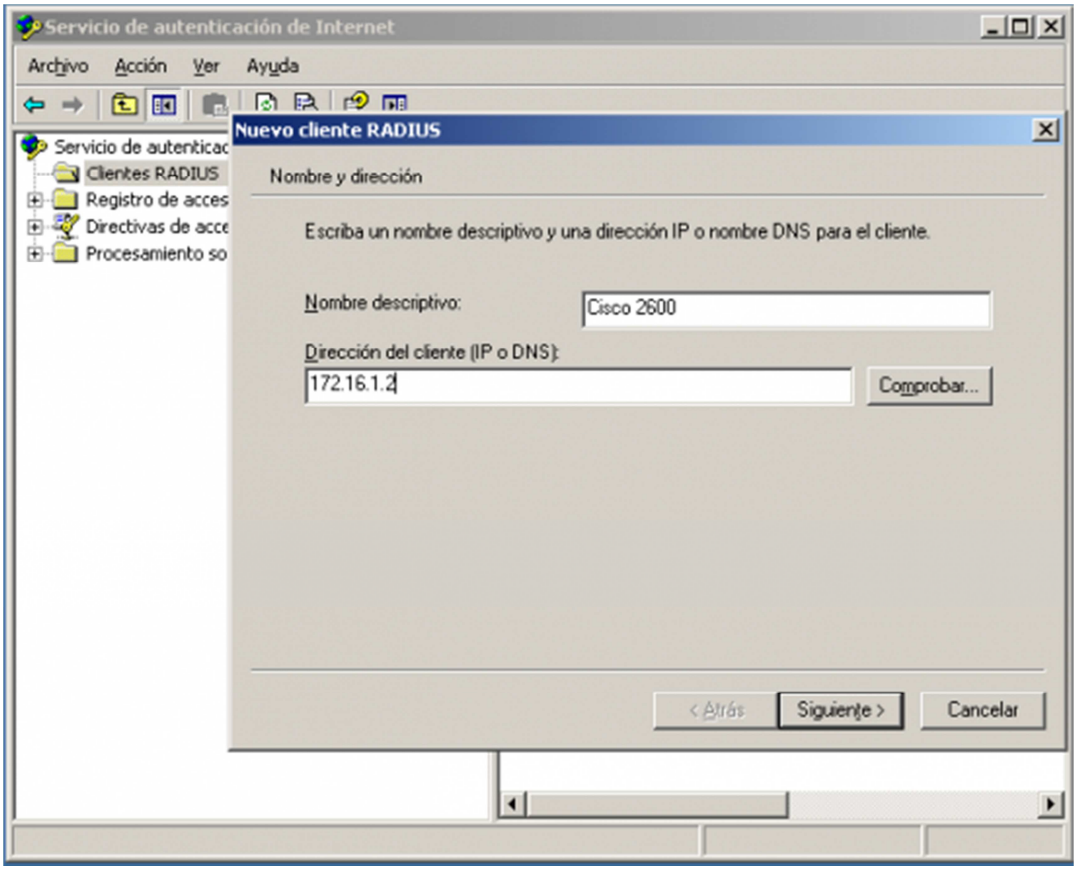


Figura A. 6 Nuevo cliente RADIUS
Fuente: Los autores

Finalmente seleccionar al cliente proveedor, para este caso el proveedor: CISCO y la clave pre compartida que será “cisco” y click en finalizar.

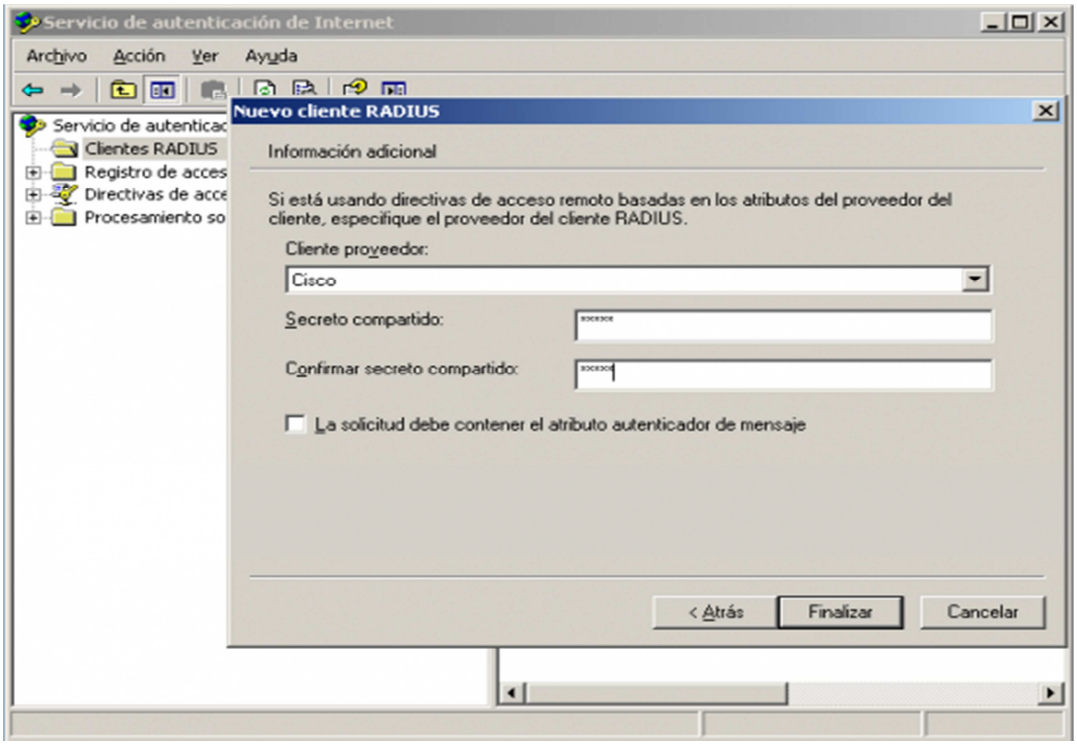


Figura A. 7 Nuevo cliente RADIUS
Fuente: Los autores

PASO 2: El segundo paso para configurar el servicio es crear la directiva de acceso que utilizara el servidor RADIUS para autenticar a los usuarios, para ello se tiene que ubicar en opción de Directivas de acceso remoto y dentro de la pantalla donde se muestran las políticas previamente configuradas seleccionamos la opción de Nueva directiva de acceso remoto.

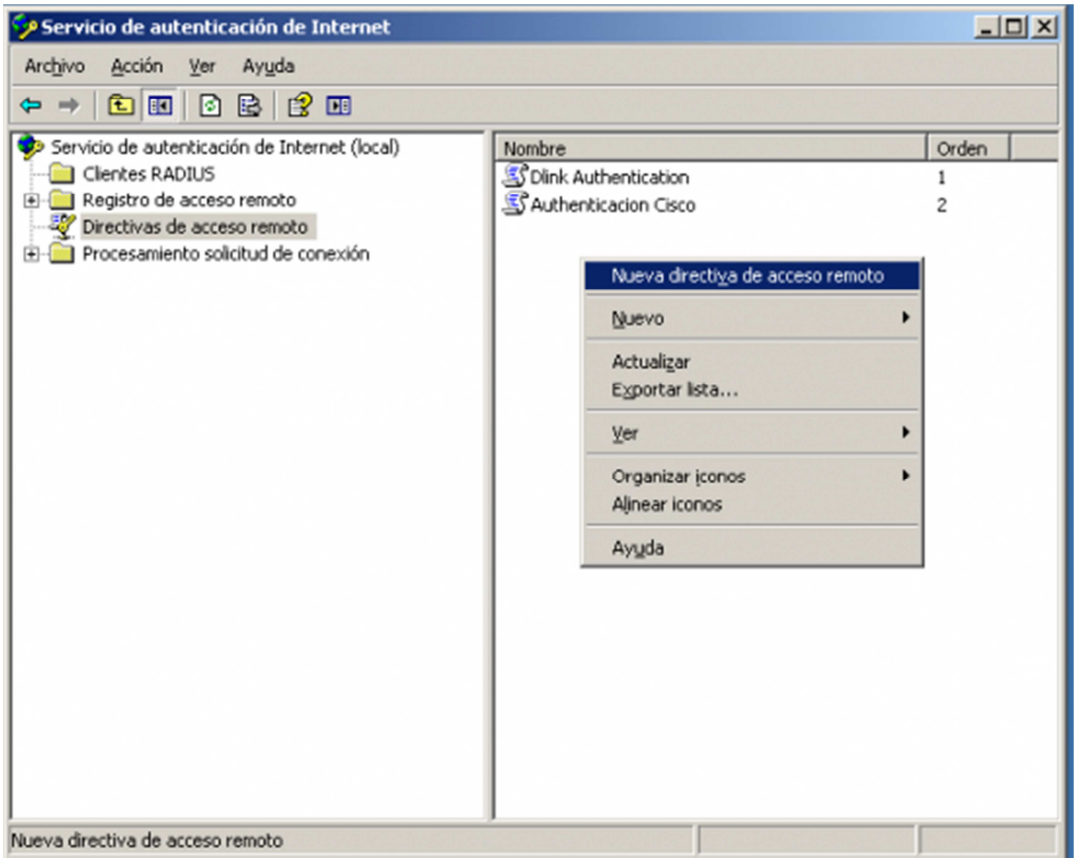


Figura A. 8 Nueva directiva de Acceso Remoto
Fuente: Los autores

Se desplegara el asistente para crear una nueva directiva, click en siguiente en la primera página, lo cual nos llevara a la siguiente pantalla donde seleccionaremos la opción de crear una directiva personalizada y en el nombre de directiva que haga referencia a esta política.

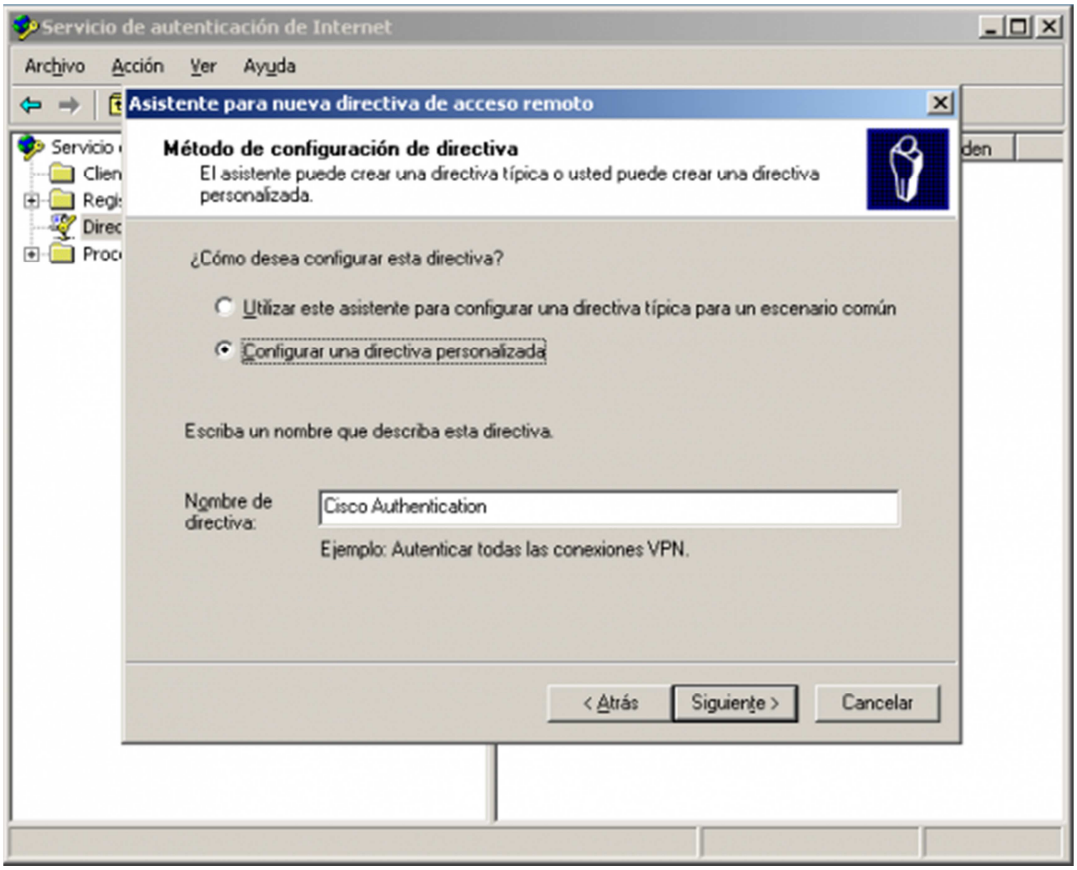


Figura A. 9 Nueva directiva de Acceso Remoto
Fuente: Los autores

Se desplegara la pantalla para agregar una nueva directiva, se debe seleccionar los siguientes atributos: Windows Group y NAS-IP-Address

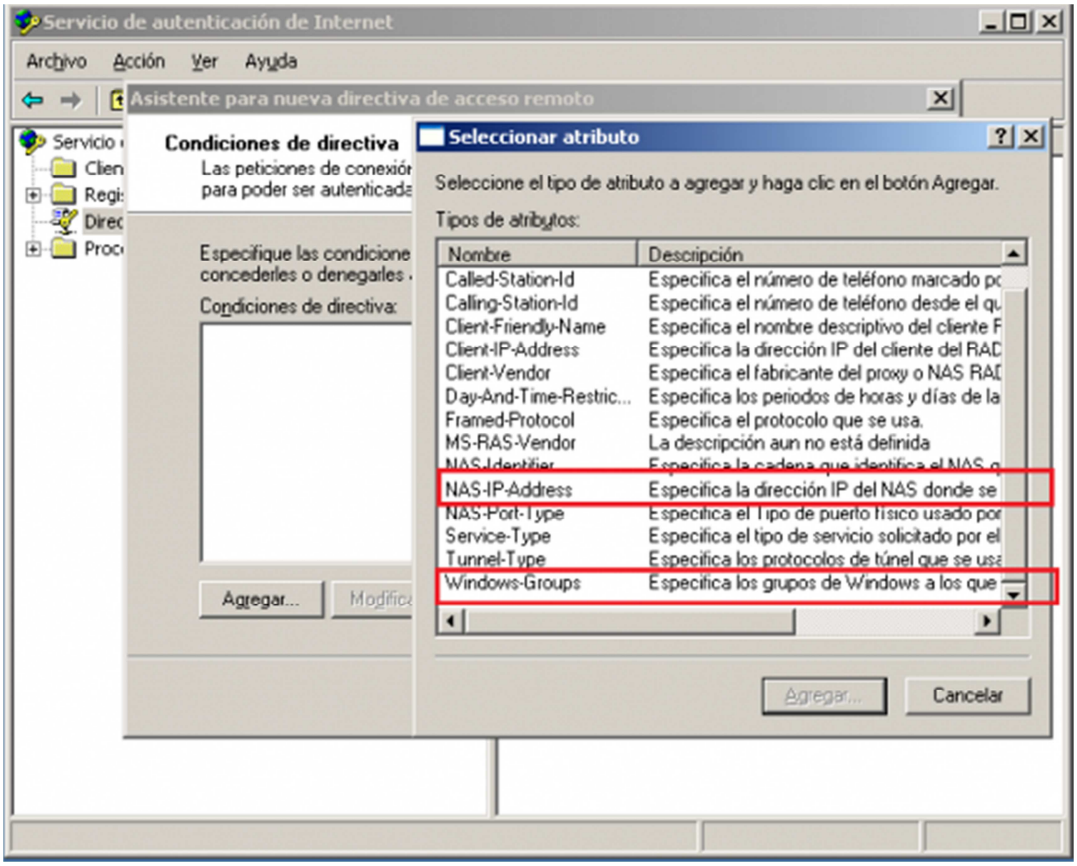


Figura A. 10 Seleccionar atributo
Fuente: Los autores

Para el atributo NAS-IP-Address, se debe colocar la IP del cliente desde donde se originara la autenticación que utilizara el servicio de RADIUS

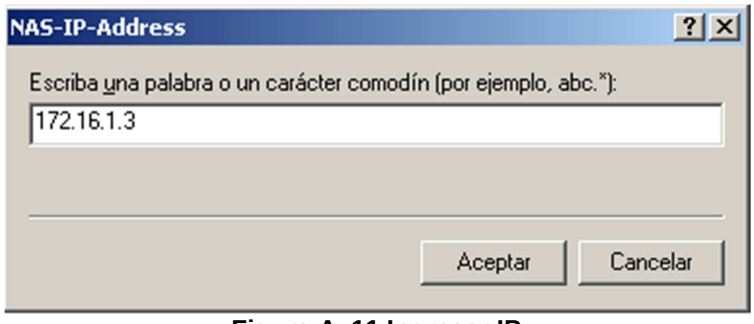


Figura A. 11 Ingresar IP
Fuente: Los autores

Para el atributo Windows Groups, seleccionar el grupo al que pertenecen los usuarios que podrán ser autenticados al momento de iniciar una conexión remota

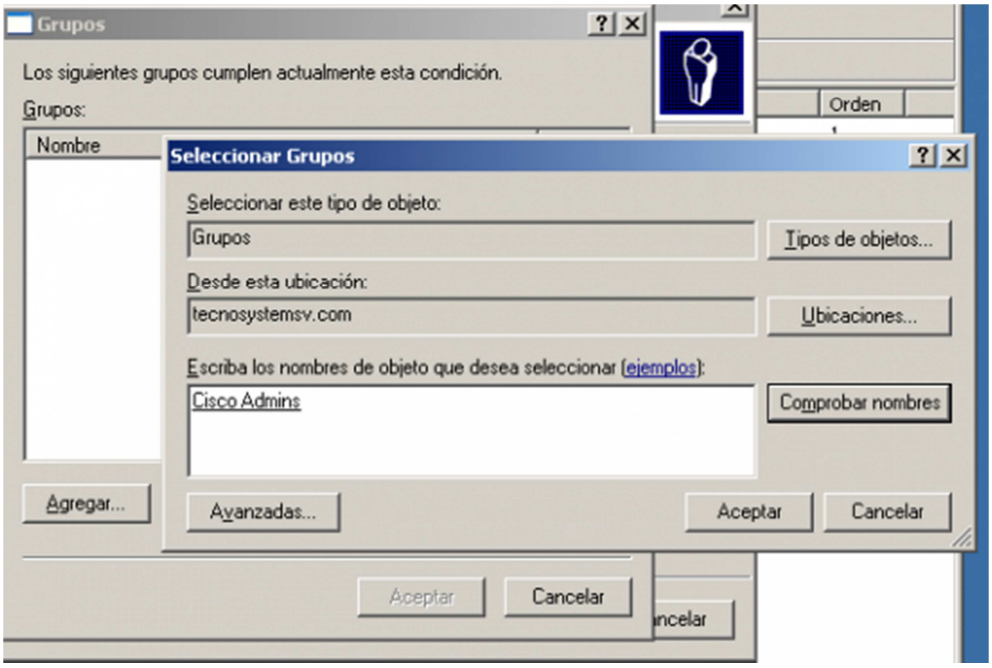


Figura A. 12 Seleccionar Grupos
Fuente: Los autores

Click en siguiente seleccionar la opción de Conceder permisos de acceso remoto

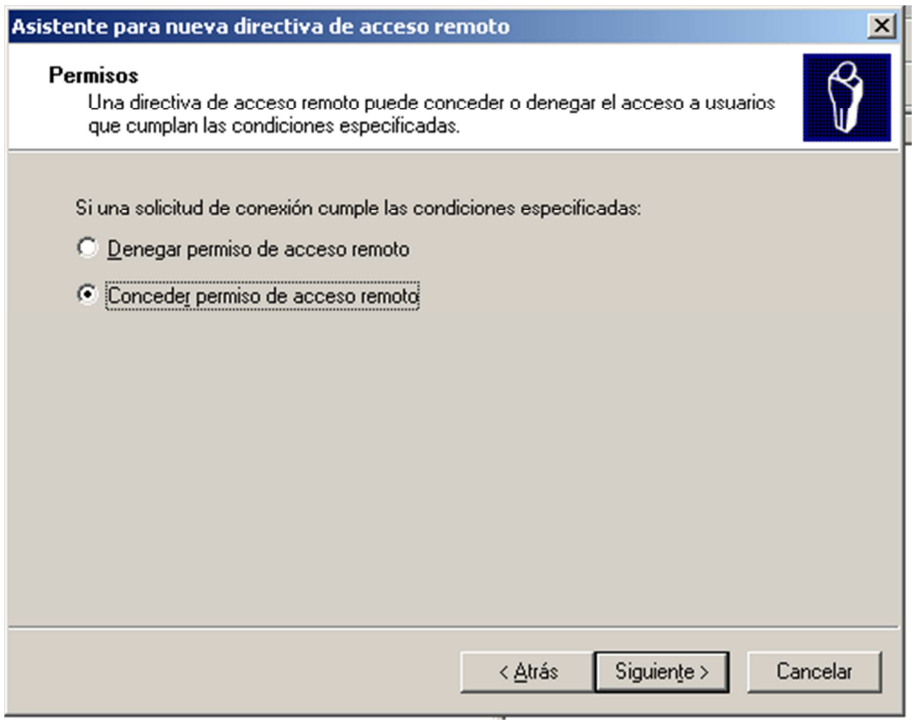


Figura A. 13 Nueva directiva de Acceso Remoto
Fuente: Los autores

Para crear la directiva, solo está pendiente editar el perfil de marcado, click en la opción editar perfil y seleccionar la pestaña de autenticación y asegurarnos que solamente este marcada la opción de autenticación sin cifrado.

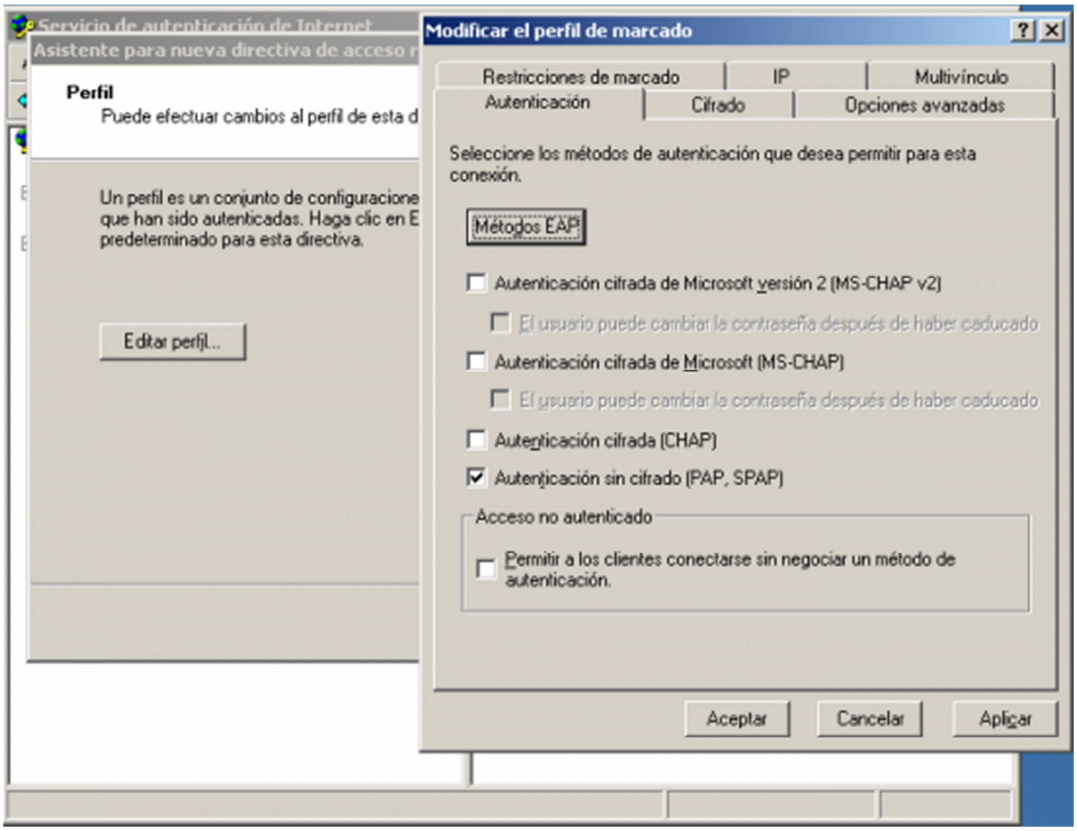


Figura A. 14 Modificar perfil de marcado
Fuente: Los autores

En opciones avanzadas asegurarse que las opciones habilitadas queden como se muestran en la siguiente imagen.

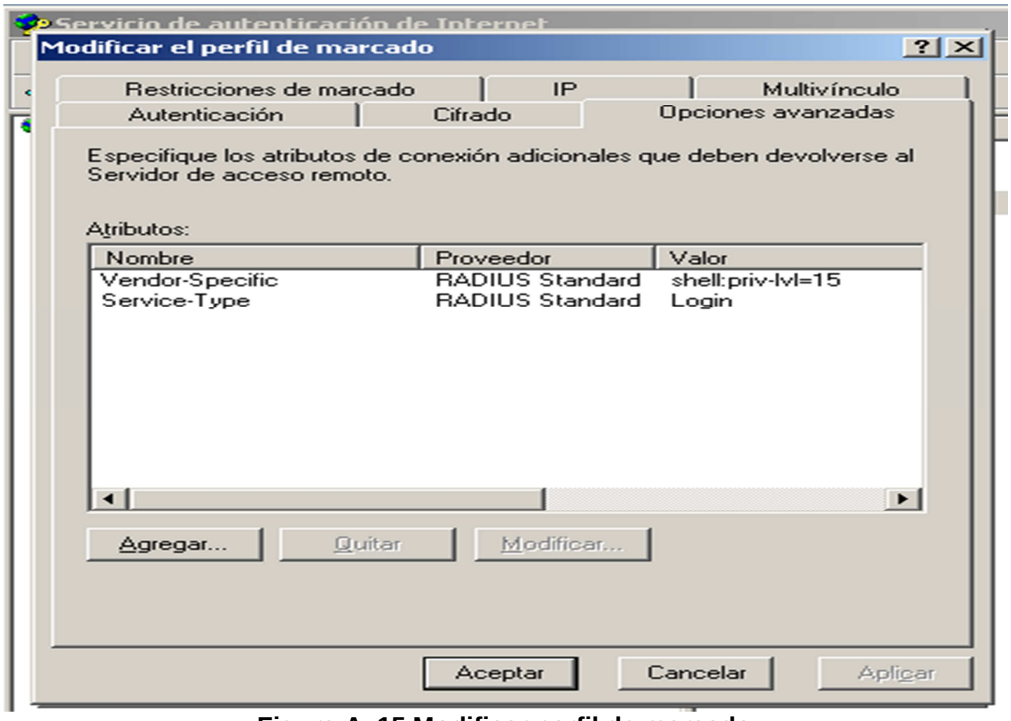


Figura A. 15 Modificar perfil de marcado
Fuente: Los autores

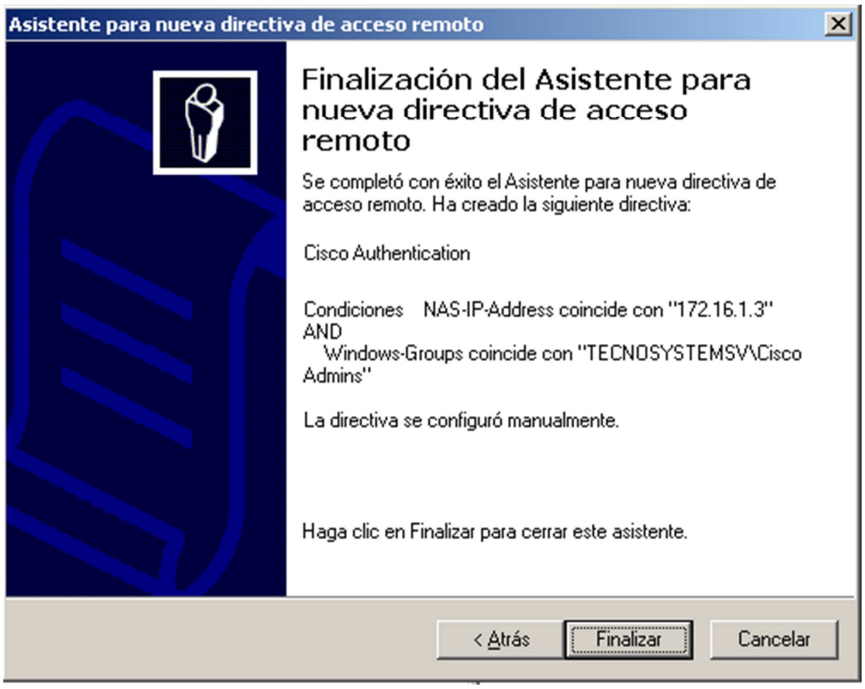


Figura A. 16 Finalizar Directiva de Acceso Remoto
Fuente: Los autores

PASO 3: Configuración del router.

C2611(config)# aaa new-model

Habilita la opción para que el router se pueda autenticar mediante el uso de un servidor RADIUS

C2611(config)# aaa authentication login default group radius local

La primera parte del commando aaaauthenticationlogin habilita al router para que se autentica mediante diferentes métodos, la palabra default indica que será la política por defecto para autenticar a los usuarios, la parte groupradius indica que la primera prioridad es autenticar mediante un servidor RADIUS, la palabra local indica que la segunda prioridad de autenticación es la base de datos local del router en caso no se tenga conexión con el servidor RADIUS

C2611(config)# aaa authorization exec default group radius if-authenticated local

El comando aaaauthorizationexec permite que los usuarios que se autentiquen mediante el servidor RADIUS tengan acceso directamente al modo EXEC privilegiado

C2611(config)# ip radius source-interface Ethernet0/0

Le indica al router la interfaz que esta conectada directamente al servidor RADIUS

C2611(config)# radius-server host 172.16.1.2 auth-port 1645 acct-port 1646 key cisco

Con este comando indicamos la dirección local que tiene configurado el servidor RADIUS y los puertos que están configurados para establecer la comunicación, la parte del comando donde se involucra la palabra key indica que este es el secreto compartido entre el servidor RADIUS y el cliente.

ANEXO 2

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento de política de seguridad de la información

1. SEGURIDAD LÓGICA

IDENTIFICACIÓN

En el sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos para cada uno de los usuarios dentro de la organización:

- Identificación del usuario será identificado por la primera letra de su primer nombre seguida de su apellido completo en caso que haya homónimos se deberá tomar la primera letra del segundo nombre seguida por el apellido del usuario
- Password, debe ser personal, se colocará un password inicial para un primer ingreso a la cuenta del usuario luego el usuario tendrá la potestad de cambiarlo.
- Nombre y apellido completo, deberá ser llenado en la identificación en el Active Directory
- Grupo de usuarios al que pertenece, esto permitirá un mejor manejo en la ubicación por medio de los diferentes departamentos
- Fecha de expiración del password, mantendrá la seguridad en el ingreso al sistema se recomienda que la fecha de expiración del password sea después de 30 días
- Fecha de anulación de la cuenta, en caso de que un empleado salga de la empresa deberá tener un periodo de gracia que no sea más de 10 dias para la eliminación total de la cuenta
- Autorización de imprimir, cada uno de los empleados deberá contar una clave para realizar las impresiones que sean necesarios para sus labores diarias.
- Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, a menos que exista una autorización por la dirección encargada.
- Durante las vacaciones o licencias las cuentas de usuarios deben desactivarse, o en su defecto colocar un correo que permita saber a los demás usuarios o clientes que el usuario se encuentra ausente, dejando a otra persona como contacto para la asignación de labores previamente autorizado por el jefe inmediato.

- El administrador del sistema deberá realizar un chequeo mensual de los usuarios del sistema, en el servidor de Active Directory para mantener una base de datos depurada y asegurarse que solamente se encuentran los usuarios autorizados para el acceso al sistema.
- El área de talento humano será la encargada de notificar al administrador del sistema que movimiento de personal va a existir para que todas las cuentas del usuario sean creadas en elos diferentes sistemas, así mismo el administrador del sistema deberá asegurarse de realizar todas las pruebas necesarias para que el usuario solo tenga acceso a las aplicaciones indicadas y con los permisos respectivos a fin de que no exista ningún error cuando un usuario nuevo ingrese a la empresa.
- Cuando un empleado es despedido o renuncia la cuenta debe desactivarse más no eliminarse por un periodo superior no mayor a 10 dias en este periodo se colocará un mensaje en el correo para informar tanto a los usuarios internos como a los clientes que el usuario ya no pertenece a la empresa, una vez pasado este periodo la cuenta se eliminará.
- Por medio del active directory se deberá bloquear el perfil de todo usuario que no haya accedido al sistema durante un período razonable de tiempo.
- No debe existir otra cuenta que no sea Administrados y la cuenta propia de cada usuario, las cuentas de invitado no se deben crear en ningún momento.
- Para la modificación de los privilegios en una cuenta el jefe inmediato de la persona en cuestión deberá enviar una petición formal al administrador del sistema para que los privilegios de dicha cuenta sean cambiados, explicando el por qué se requiere el cambio de privilegio.

CONTRASEÑAS

Las reglas de contraseña listadas a continuación están de acuerdo a los requerimientos y estándares internacionales.

- Ser de al menos 8 caracteres de longitud

- Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
- No contener su user ID como parte la contraseña.
- Todos los sistemas y aplicaciones que contengan información clasificada cambie la contraseña al menos cada mes. Si alguna aplicación requiere solo de la manipulación del usuario final sin la intervención del administrador del sistemas es obligación de cambiar la contraseña en un periodo no mayor a los 3 meses, dicho password tiene que ser diferente por lo menos a los últimos 3 passwords ingresados.
- Es importante que se pueda realizar un bloqueo en el sistema a todo usuario que haya querido acceder al sistema sin éxito por más de 5 intentos
- El usuario estará en la libre potestad de poder realizar cambios en su password todas las veces que considere necesario, sin que exista una notificación a un jefe o al administrador del sistema.
- Absolutamente todos los passwords predefinidos que vengan en los equipos nuevos deberán ser cambiados una vez que se haya realizado la configuración inicial
- Ningún usuario debe guardar su contraseña en archivos que sean de fácil acceso así como no deben escribirla en papel y dejarla a vista de todos o en sitios donde pueda ser encontrada. Si por alguna razón el usuario cree que su contraseña posee otra para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.

2. SEGURIDAD DE COMUNICACIONES

TOPOLOGÍA DE RED

Deberá existir documentación detallada sobre los diagramas topológicos de la red, esto permitirá la fácil ubicación de una falla en la comunicación en la red informática.

CORREO ELECTRÓNICO

Para el correo electrónico se deberán tener en cuenta los siguientes datos a almacenarse:

Correo entrante y saliente, esto deberá estar en cada uno de los computadores bien identificados en un archivo .pst

- Hora de envío
- Contenido del mail
- Asunto del mail
- Archivos adjuntos
- Direcciones de máquina destino y fuente
- Tamaño del mensaje.

Todos estos datos antes mencionados se podrán visualizar en el servidor de Microsoft Exchange el mismo que es el encargado de gestionar el correo empresarial.

UTILIZACIÓN DE LA RED INFORMÁTICA

Para la utilización de la red informática se deberán tener en cuenta los siguientes datos a almacenarse:

- Ancho de banda utilizado y cuellos de botella en el tráfico de red
- Tráfico generado por las aplicaciones
- Recursos de los servidores que utilizan las aplicaciones
- El estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta)
- Intentos de intrusión
- Uso de los protocolos
- Los cambios tanto en la central telefónica como en servidores y equipos de red, instalación de nuevo software, cambio de direcciones IP, la reconfiguración de equipos de comunicación, deben ser documentados y debidamente aprobados, esto para poder tener una fuente de conocimiento de los cambios realizados por el administrador del sistema, todo esto se realizará sin autorización solo y únicamente

si se trata de una situación de emergencia debidamente justificada en un informe posterior al cambio.

- Todo el tráfico de la red deberá poder ser visualizado y posteriormente medido mediante herramientas que permitan el ingreso a la red de la empresa.

USO DE LOS SISTEMAS DE COMUNICACIÓN

Los sistemas de comunicación sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con sus actividades.

CONEXIONES EXTERNAS

La conectividad para salida a internet debe asegurarse que absolutamente todo el tráfico entrante y saliente esté siendo filtrado por medio de un firewall, en dicho firewall se deberá configurar todo aquello que única y exclusivamente sea necesario para el uso de los empleados en sus labores diarias de ser posible definir perfiles de acceso para identificar usuarios y jefaturas

El monitoreo a las diferentes páginas en la web deberá ser monitoreado constantemente y tener un reporte mensual en donde se pueda identificar al usuario y las páginas que ha visitado esto con el fin de poder identificar si hay una disminución en la productividad de los usuarios debido al ingreso de páginas que no estén aportando a la continuidad del negocio.

El acceso a los buzones de correo de cada uno de los usuarios por parte del administrador del sistema se dará previo a la autorización del usuario en caso que exista algún problema con el correo o en caso de que exista spam y se tenga que eliminar los correos por medio de Microsoft Exchange, cabe destacar que los únicos que tienen la potestad de revisar los correos de los usuarios sin previo consentimiento son las gerencias en caso de que lo requieran.

INFORMACIÓN PERSONAL SENSIBLE

Es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Toda esta información sobretodo los datos bancarios y contraseñas por ningún motivo deben estar visibles en los computadores peor aún escritos en los puestos de trabajo si es necesario mantener esta información en la oficina tendrán que consultar con el administrador del sistemas alguna forma de encriptar sus datos.

CONFIGURACIÓN LÓGICA DE RED

Cuando se conecte un equipo a una red interna, se debe considerar los siguientes puntos:

- El equipo debe estar claramente identificado por el administrador del sistema.
- Deberá contar con una dirección ip que será asignada por dhcp.
- No deberá tener una dirección ip estática.
- Todo equipo personal de los usuarios antes de ser conectados en la red interna deberá pasar por el departamento de sistemas para que se realice un chequeo previo para saber si el equipo se encuentra libre de cualquier virus que puedan afectar a la red.
- No está autorizado la utilización de ninguna herramienta de monitoreo de red por parte de los usuarios de la empresa.

ANTIVIRUS

En todos los equipos de la empresa se debe instalar y correr el antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción realizada por un software malicioso en tiempo real.
- Ejecutar el escaneo del antivirus todos los días a una hora determinada.

- Debe ser un producto totalmente legal es decir el producto debe contar con todas las licencias tanto para servidores como para los computadores.
- No deben usarse medios de almacenamiento en cualquier computador a menos que se haya previamente verificado que están libres de virus.

3. SEGURIDAD DE LAS APLICACIONES

SOFTWARE

No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado por el administrador del sistema.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el administrador del sistema. .

Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

Todo software tiene que ser instalado únicamente por el administrador del sistema el mismo que se encargará de crear las claves y la definición de perfiles para cada uno de los usuarios.

CONTROL DE APLICACIONES EN PC'S

Se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

Antes de hacer un cambio en la configuración de los servidores se deberá hacer un backup de la configuración existente. Realizar un protocolo de pruebas que demuestre

que el cambio en la aplicación no afectó a la aplicación Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.
Se deberán documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se realicen.
Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados. Esto permitirá llevar un mejor control para la continuidad del negocio.

CONTRATOS DE APLICACIONES CON TERCEROS

Los contratos con terceros deberán contener una cláusula que indique "Derecho de auditar el desempeño del contratado". Para que de esta forma se pueda verificar que todo el trabajo que se está realizando en la empresa se lo esté realizando de la mejor manera
Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del sistema será el encargado de realizar el seguimiento para los cambios que se requieran hacer en un sistema teniendo en cuenta los siguientes parámetros:

- Sistema que afecta,
- Fecha de pedido de la modificación
- Fecha de la modificación
- Desarrollador que realizó el cambio.
- Empleado que solicitó el cambio.
- Descripción global de la modificación.
- Protocolo de pruebas de funcionamiento

Finalmente el desarrollo de toda aplicación realizada por terceras personas deberá ser debidamente entregada con los siguientes datos:

- Aplicación ejecutable
- Código fuente de la aplicación
- Documentación del desarrollo

- Manuales de uso.
- Capacitación tanto en la administración del sistema como en la ejecución para usuarios finales.

ANEXO 3

OCS Inventory

Open Computer and Software InventoryNextGeneration es una aplicación diseñada para ayudar a un administrador de red o sistema de seguimiento de la configuración de la computadora y el software instalado en la red.

También permite la distribución de paquetes en computadoras Windows y Linux. Diálogo entre los equipos cliente y el servidor de gestión se basa en los estándares actuales, Protocolo HTTP / HTTPS y formato de datos XML.

El servidor de administración se ejecuta en Apache / MySQL / PHP / PERL del servidor, bajo Linux o equipos con Windows basados en NT.

Equipos inventariados cliente puede ejecutar Microsoft Windows 95/98/Me/NT4/2000/XP/2003/Vista o sistemas operativos Linux. También hay agentes contribuyeron para Sun Solaris, * BSD, IBM AIX 5.X, HP-UX y Mac OS X.

OCS Inventory es software GPL, es decir, libre de usar y copiar (Fuente http://www.opensource.org/licenses/gpl-license.php). Es también Open Source, esto significa que si desea modificar las fuentes que usted puede, sin embargo, si desea actualizar el código fuente para su distribución, debe proporcionar las actualizaciones en términos de la licencia GPL.

Soporta los siguientes idiomas:

Portugués brasileño

- Inglés
- Francesa
- Alemán
- Hungría
- Italiana
- Polaca
- Portugués
- Español

- Rusia
- Turca

Se utiliza con el software de gestión de activos, tales como GLPI (http://www.glpi-project.org), deberá tener un inventario de gran alcance y software de información de gestión de recursos con cambio automático cambios de configuración del equipo, la gestión de licencias, mesa de ayuda, base de conocimientos y más.

Instalación y configuración en Windows:

Hemos optado por el paquete de inventario servidor OCS NG para Windows como un paquete integrado que contiene todos los componentes necesarios. Como sea, los 3 principales componentes de Management Server (servidor de base de datos, servidor de comunicaciones web y el servidor web de administración) se instalan en el mismo equipo.

OCS Inventory NG Server 1.0 para Windows se basa en la versión XAMPP 1.5.5 ApacheFriends (Http://www.apachefriends.org/index-en.html) que configurar los siguientes componentes en un solo equipo:

- Apache 2.2.3
- MySQL 5.0.27
- PHP 5.2.0 + PHP 4.4.4 + PEAR
- PHP-Switch win32 1.0
- Control de XAMPP Versión 2.3 de www.nat32.com
- XAMPP Security 1.0
- SQLite 2.8.15
- OpenSSL 0.9.8d
- phpMyAdmin 2.9.1.1
- ADOdb 4.93
- Correo Mercurio Sistema de Transporte para Win32 y NetWare Systems v4.01b

- FileZilla Server 0.9.20 FTP
- Webalizer 2.01-10
- Zend Optimizer 3.0.2
- eAccelerator 0.9.5 RC1 para PHP 5.1.6 (como comentario en el php.ini)
- Perl 5.8.8
- mod_perl 2.0.2

INSTALACIÓN DE SERVIDOR DE ADMINISTRACIÓN

Usted debe tener privilegios de administrador para configurar el servidor OCS Inventory NG bajo Windows NT4, Windows 2000, Windows XP o Windows Server 2003.

Descargar "OCSNG_WIN32_SERVER_1.01.zip" desde el sitio web de OCS Inventory ", descomprimirlo y ejecutar" OcsWin32ServerSetup.exe.

Figura B. 1 Seleccionar Lenguaje
Fuente: Los autores

Si los componentes XAMPP (servidor y el complemento de perl) no están instalados, el programa de instalación le indicará que usted tiene que configurar. De lo contrario, el programa de instalación automáticamente instala el servidor OCS Inventory en los directorios de XAMPP.

Figura B. 2 Iniciar Instalación
Fuente: Los autores

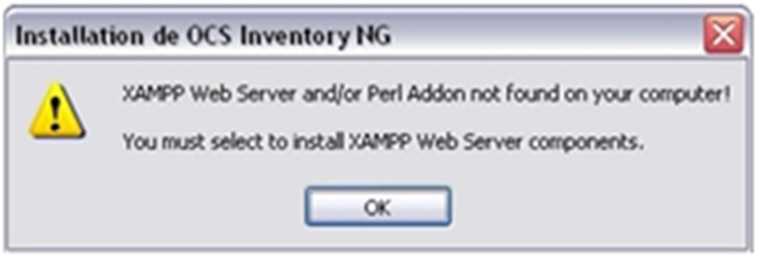


Figura B. 3 Mensaje de Instalación
Fuente: Los autores

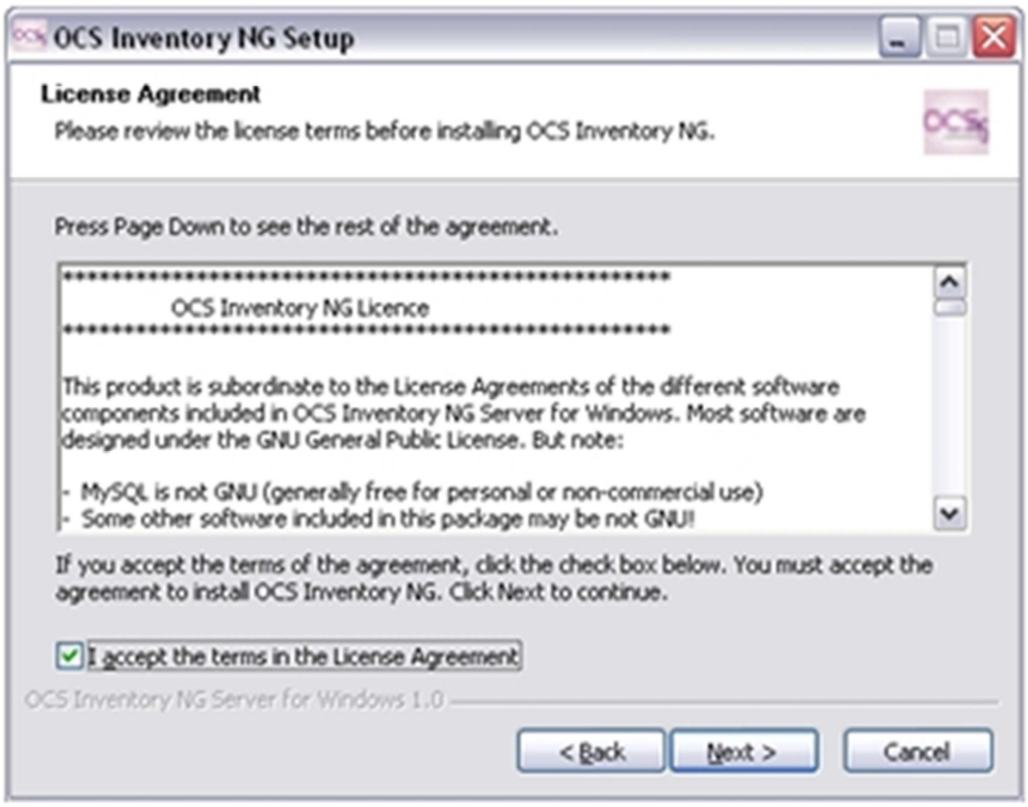


Figura B. 4 Licencia de Contrato
Fuente: Los autores

Haga clic en botón "Siguiente" y acepte el acuerdo de licencia.

Elija el directorio de instalación, por defecto "C: \ Archivos de programa \ OCS Inventory NG". Usted necesita 400 MB de espacio libre en disco duro si los componentes XAMPP no están instalados, de lo contrario, sólo se requieren 10 MB.

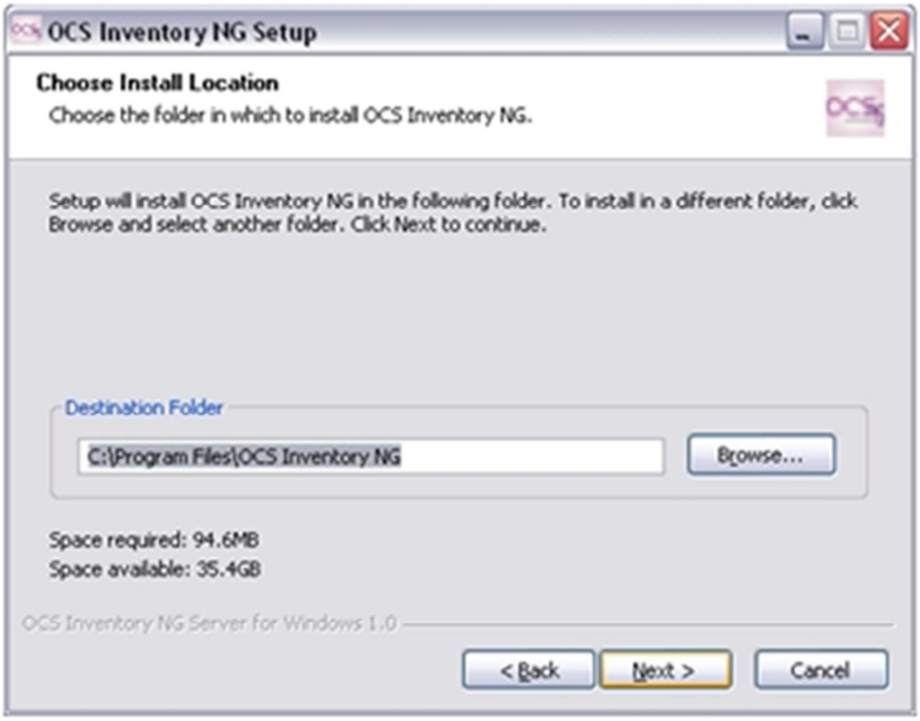


Figura B. 5 Directorio de Instalación
Fuente: Los autores

Entonces, usted tiene que validar los componentes a instalar. Sólo "OCS Inventory NG Server" se requiere, si los componentes de XAMPP ya están instalados.

A continuación, usted tiene que elegir el nombre del grupo de programas en el menú de inicio, donde OCS Inventory NG iconos se crearán y haga clic en "Instalar" para iniciar la instalación.

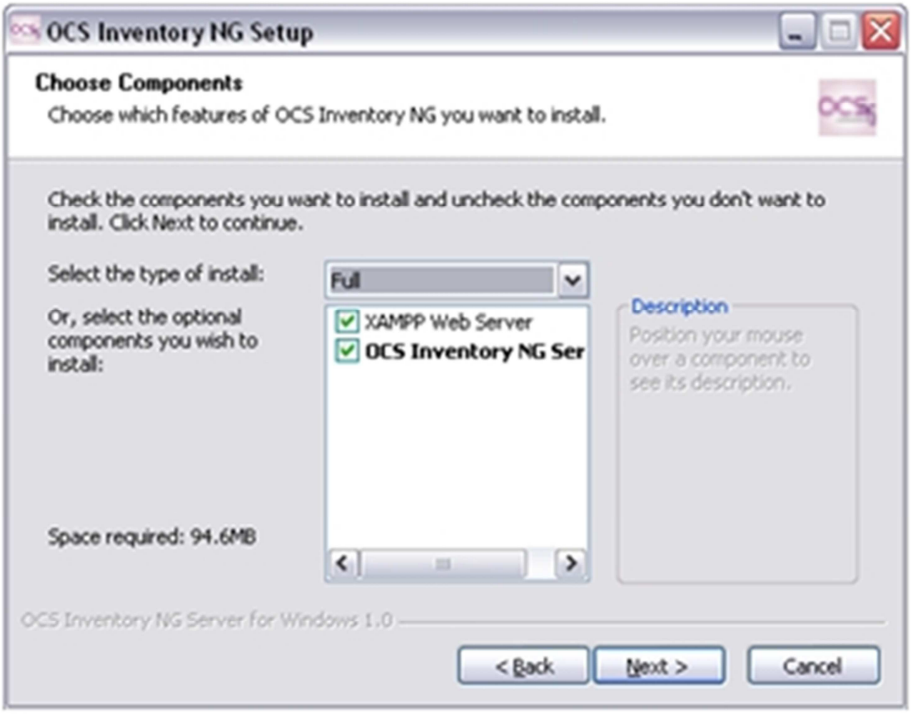


Figura B. 6 Componentes a Instalar
Fuente: Los autores

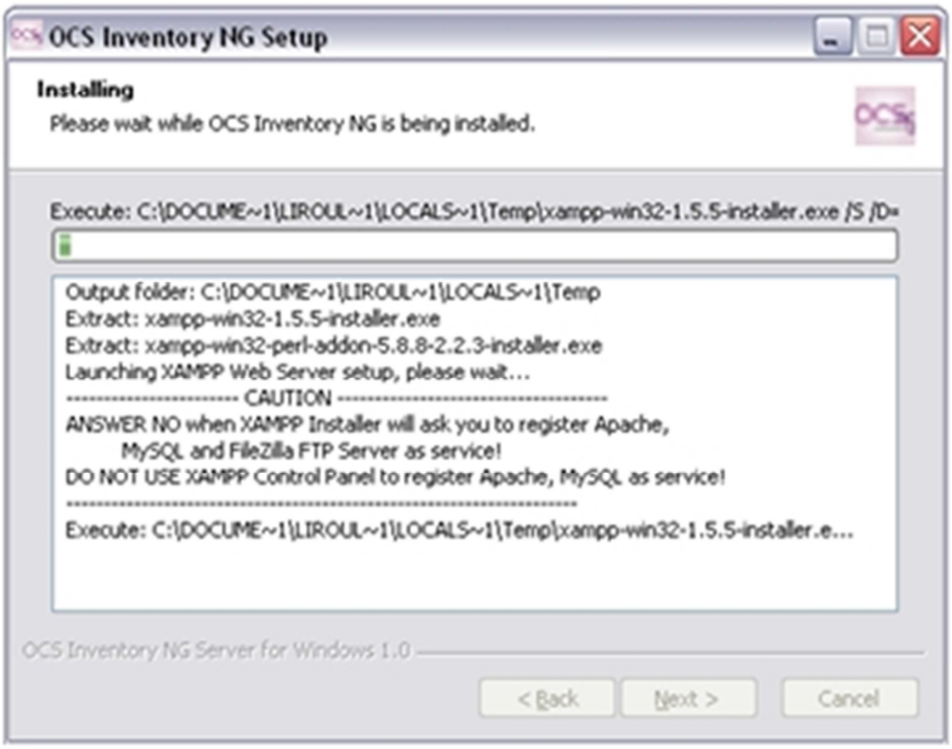


Figura B. 7 Progreso de Instalación
Fuente: Los autores

Si la configuración de XAMPP seleccionada, el programa de instalación primero pondrá en marcha XAMPP 1.5.5 instalación en modo silencioso. Esto creará una carpeta "xampp" bajo la carpeta de destino, y un grupo de programas "Apache Friends" en el menú de inicio.

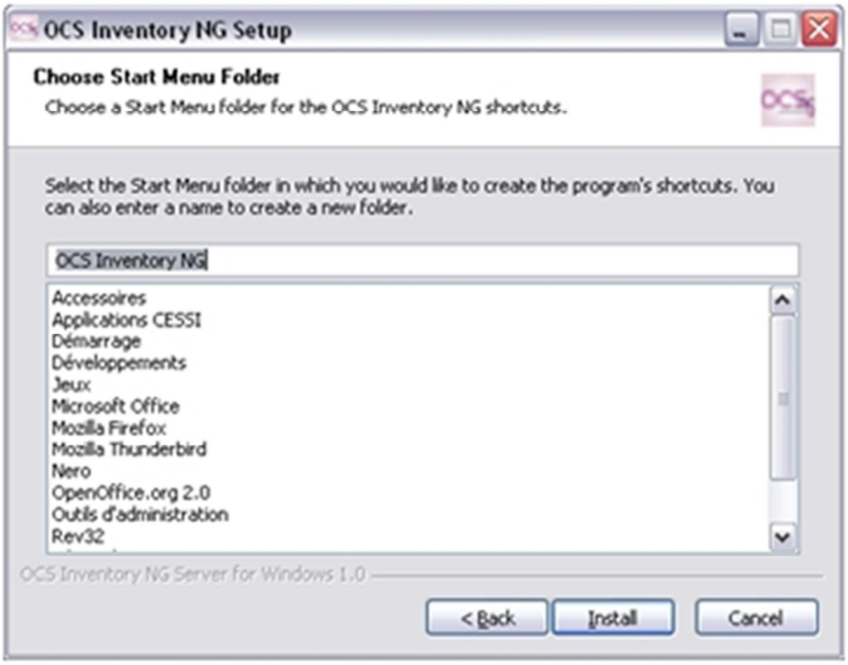


Figura B. 8 Creación de carpeta en Menú Inicio
Fuente: Los autores

Se le pedirá que inicie el Panel de Control de XAMPP. Por favor, responda "No". A continuación, se iniciará la instalación de XAMPP perladdon en modo silencioso.

Última configuración, se instalarán los archivos del servidor OCS Inventory NG, configurar XAMPP Apache y MySQL para el inventario de los servidores del servidor OCS NG, y se inicia automáticamente servidores MySQL y Apache.

Al final del proceso, el programa de instalación abrirá su navegador predeterminado para iniciar OCS Inventory NG La configuración del servidor (véase § 3.2.2 Configuración del servidor de administración.).

El programa de instalación ya está terminado y usted puede hacer clic en botón "Cerrar".

Figura B. 9 Fin de Instalación
Fuente: Los autores

Configuración del servidor de administración.

Abra su navegador web favorito en el servidor y apuntar en la dirección "Http://localhost/ocsreports" para conectar el servidor de administración.

Se le pedirá información para conectar con el servidor de base de datos MySQL con un usuario que tiene la capacidad de crear bases de datos, tablas, índices, etc:

MySQL nombre de usuario, "root" por defectocontraseña de usuario de MySQL (contraseña en blanco por defecto) MySQL nombre de host "localhost"

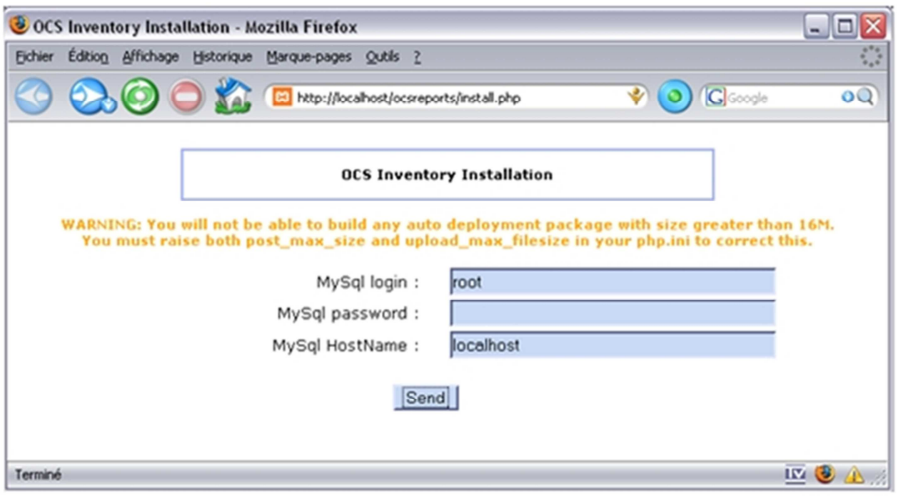


Figura B. 10 Configuración de OCS
Fuente: Los autores

Por último, puede rellenar un texto que describe el TAG, una cadena que se muestra en el primer lanzamiento de la agente pedirá al usuario que introduzca el valor del tag. Es un dato genérico que le permite ordenar las nuevas computadoras. Si usted no desea esta función, simplemente dejar en blanco.

Figura B. 11 Configuración de OCS
Fuente: Los autores

Configuración del servidor de administración ya está terminada.

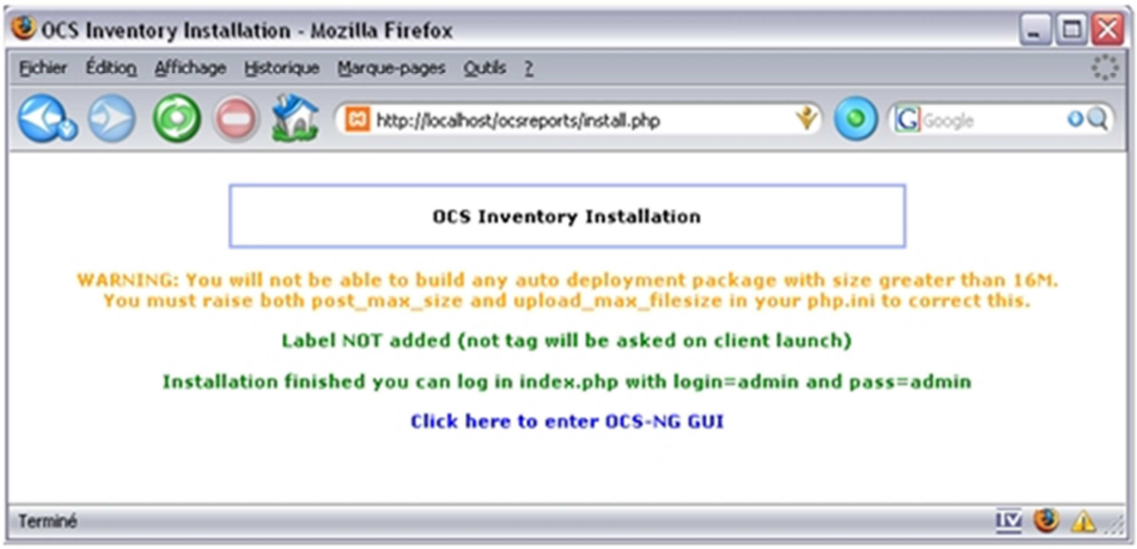


Figura B. 12 Configuración de OCS
Fuente: Los autores

Inicio de sesión predeterminada del administrador es "admin" como usuario y "admin" como contraseña.

Figura B. 13 Configuración de OCS
Fuente: Los autores

Creación de Agente para equipos:

El uso de OCS InventoryPackager es la manera más rápida de instalar y configurar el Agente OCS Inventory NG, localmente o en un dominio. Se basa en las herramientas NSIS script y RemCom. Genera un archivo llamado ocspackage.exe basado en sus parámetros, lo que permite una instalación de usuario de un solo clic, silenciosa o no. En combinación con el parámetro OcsLogon / instalar hace del servicio de distribución de software bajo sistemas operativos Windows algo fácil de lograr.

En este documento se hacen varias asunciones:

- Asumimos que conoce la cuenta administrativa local o de dominio de sus computadores.
- Debería también conocer cómo generar u obtener un archivo de certificado, así como también estar familiarizado con tareas administrativas de Windows.

Descargue el empaquetador y el instalador más reciente OcsAgentSetup.exe desde el sitio web de OCS Inventory.
Prepare su certificado.

Ejecute OcsPackager.exe y acepte el Acuerdo de Licencia.
Aparecerá la siguiente ventana.

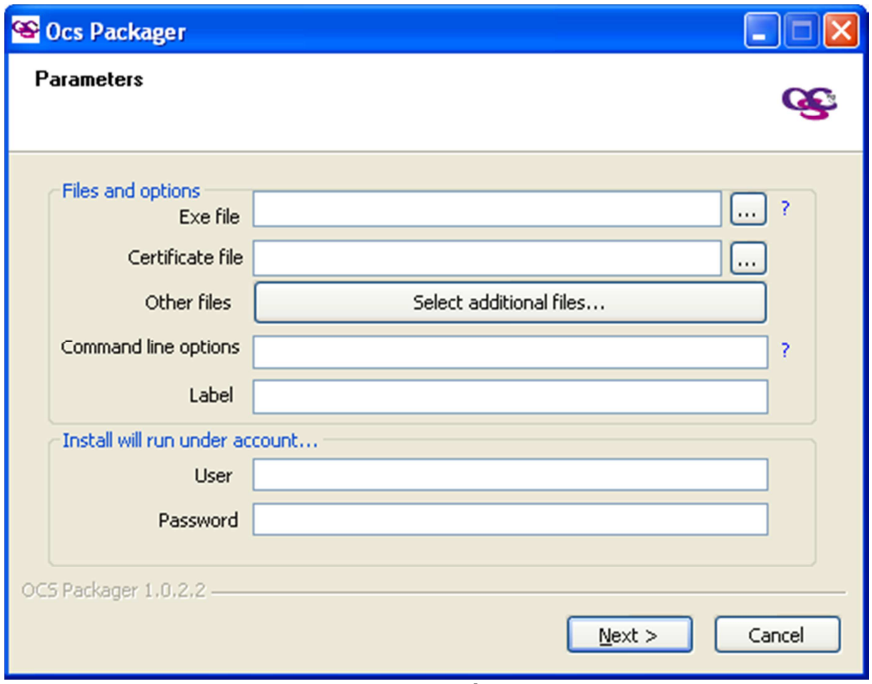


Figura B. 14 Creación de Paquete
Fuente: Los autores

"Archivos y Opciones" group box:

- En la línea "Archivo Exe", seleccione el programa **OcsAgentSetup.exe** recién descargado. ¡Esta entrada es requerida!
- En la línea de "Archivo de certificado", seleccione su archivo **cacert.pem**.
- La línea "Otros archivos" permite especificar archivos adicionales a copiar en su carpeta de instalación.
- En la línea "Opciones de línea de comandos" debería introducir todas las opciones necesarias del programa de configuración OcsAgent, por ejemplo (/servidor:mi_servidor /pnum:8081 ***/S***). No olvide especificar la opción ***/S*** para realizar una instalación silenciosa.
- La línea "Etiqueta" creará un archivo "etiqueta" que contiene la etiqueta escogida. La primera vez que OcsInventory.exe arranca, aparecerá una ventana emergente mostrando esa etiqueta. El valor que introduce el usuario es llamado "TAG".

“Instalar correrá bajo cuenta” group box:

- En la línea “Usuario”, introduzca la cuenta admin local o una cuenta administrativa de dominio. Utilice **“@”** para separar el usuario del nombre de dominio, por ejemplo (administrador@mi.dominio.com). En dominios NT4 utilice la sintáxis “dominio\usuario”.

- Tenga cuidado cuando introduzca la contraseña. **No se validará en este punto** !

Debería tener algo como esto:

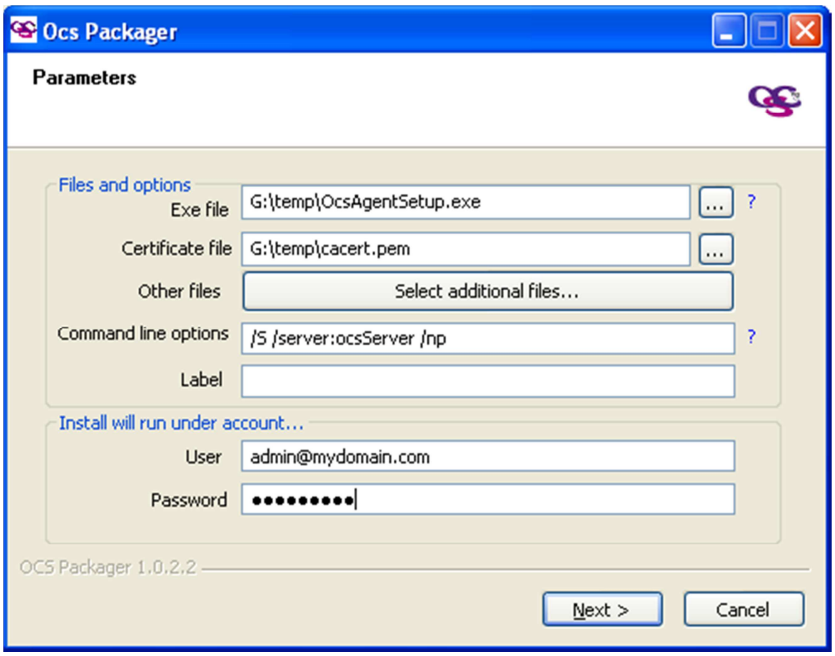


Figura B. 15 Creación de Paquete
Fuente: Los autores

Haga clic en el botón “Siguiente”.

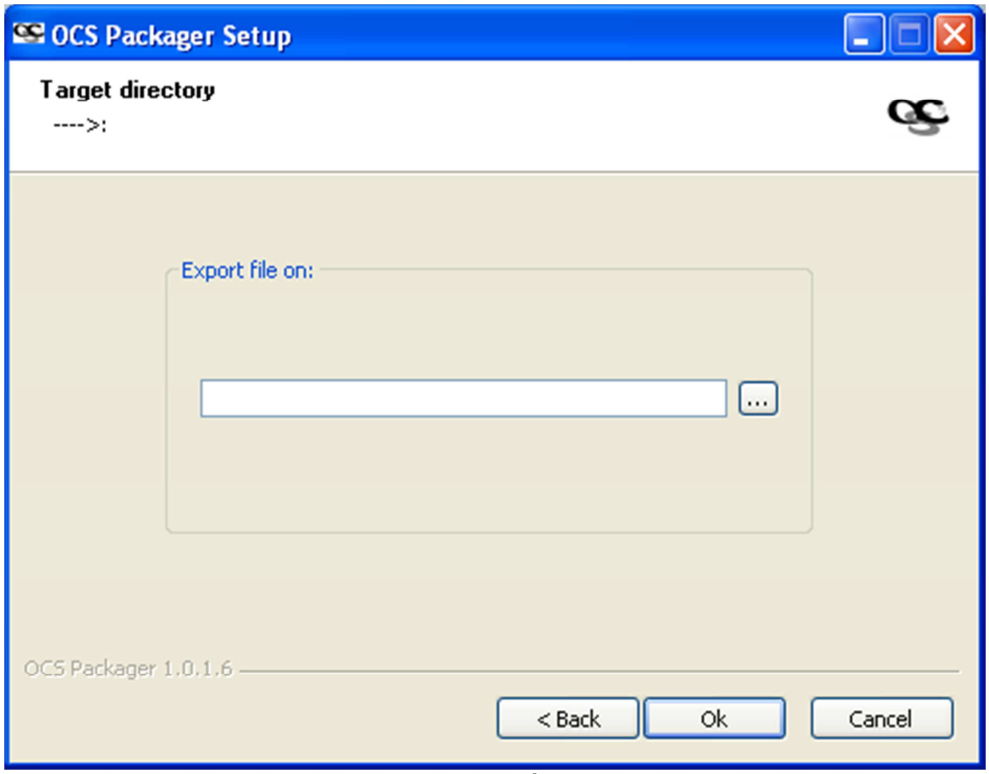


Figura B. 16 Creación de Paquete
Fuente: Los autores

Seleccione la carpeta destino y haga clic en Ok.

En este punto aparecerá momentáneamente para generar ocspackage.exe

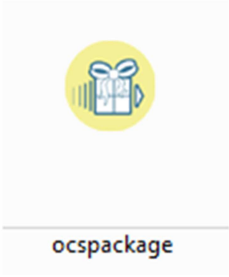


Figura B. 17 Creación de Paquete
Fuente: Los autores

Ahora puede probar ocspackage.exe ejecutándolo desde una cuenta normal de usuario (sin privilegios administrativos).

Un breve mensaje de OcsInventory puede aparecer indicando que el servicio configurado está corriendo.

Figura B. 18 Instalación de Paquete
Fuente: Los autores

Al momento de instalación se crea un archivo log llamado ocspackage.log.

Al ejecutarse el paquete en los equipos clientes, el sistema nos las iras listando de la siguiente manera:

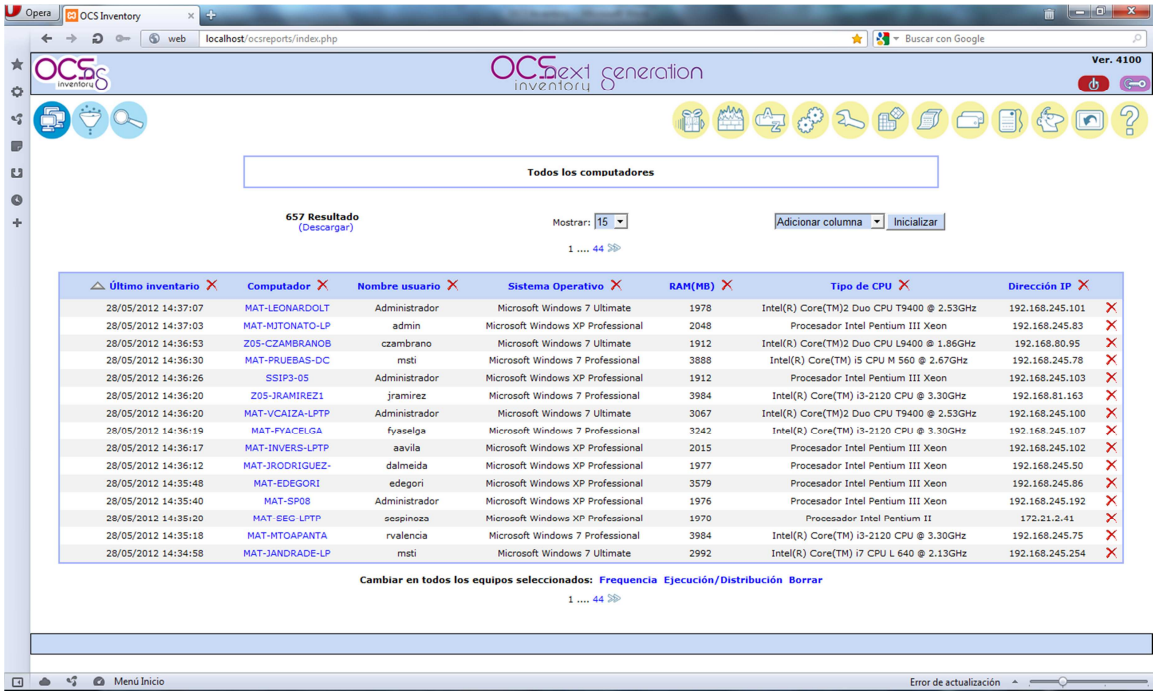


Figura B. 19 Sistema Ejecutándose
Fuente: Los autores

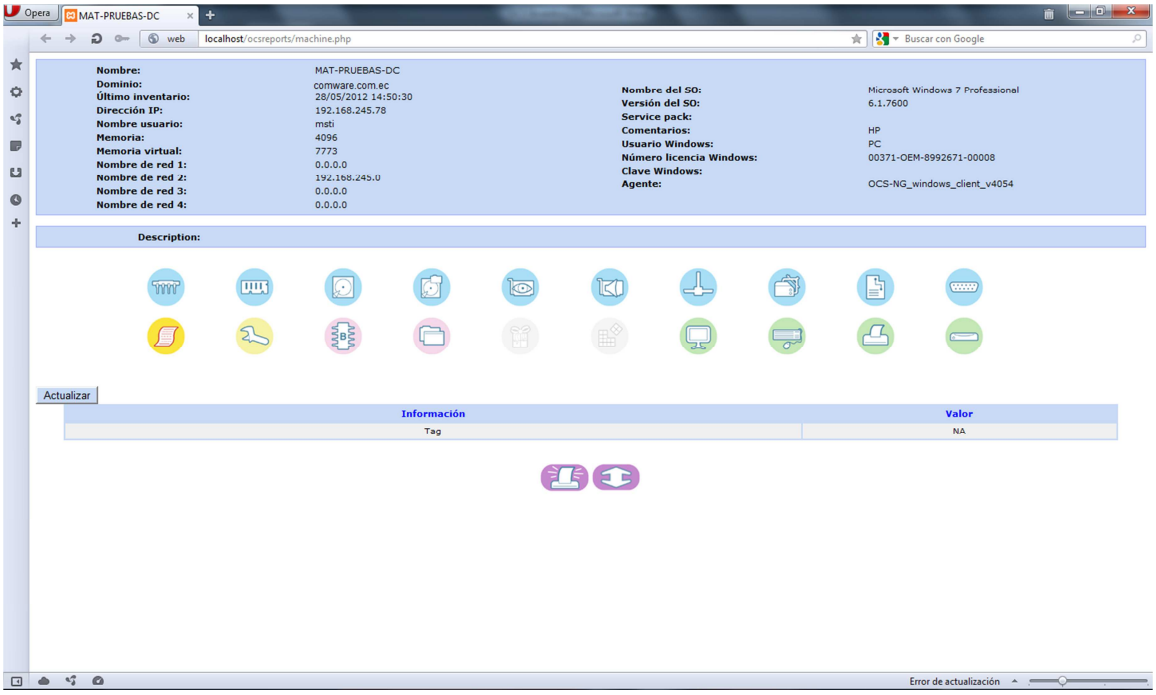


Figura B. 20 Sistema Ejecutándose
Fuente: Los autores

ANEXO 4

GUÍA DE SEGURIDAD INFORMÁTICA BASICA PARA USUARIOS

Con el fin de reducir la probabilidad de fallas y daños causados por problemas de seguridad, los usuarios deberán considerar siempre las siguientes recomendaciones:

1.-Utilice la información y los sistemas sólo para propósitos que apoyen el trabajo de la Institución.

2.- Se debe evitar utilizar los equipos institucionales para tareas como: bajar videos, música, juegos, etc. Ya que estos, son la principal fuente de malware para los computadores (virus, spywares, adwares, etc.).

3.- Se debe evitar el uso de dispositivos de almacenamiento portátiles externos a la Institución como pendrives, CDs o DVDs que no hayan sido revisados y protegidos por Sistemas Internos.

4.- Reporte los eventos no usuales que usted observe, ante las personas responsables de Informática:

4.1.- Informe cualquier cambio extraño encontrado en la información que usted tenga a cargo.

4.2.- Reporte cualquier archivo que resulte en su disco duro que usted no haya copiado o creado.

4.3.- Comunique inmediatamente a su jefe y a Sistemas Internos cualquier pérdida de datos o programas (deje constancia escrita del caso).

5.- Utilice medidas que reduzcan el riesgo de pérdida, daño e intrusión de información:

5.1.- Proteja su equipo contra humedad, fuego, daño, etc.

5.2.- Asegúrese que NADIE coma, beba o fume junto al computador. Los restos de comida, líquidos y cenizas dañan las piezas electrónicas.

5.3.- Mantenga a las personas no autorizadas y desconocidas lejos de su equipo.

5.4.- No comparta para la red directorios o archivos de manera innecesaria, especialmente aquellos que contienen información confidencial.

5.5.- No cuente sus claves a terceros y cámbielas a menudo.

5.6.- NUNCA deje su equipo desatendido con su clave activada. Utilice a lo menos el bloqueo de usuario o de salvapantallas con clave.

5.7.- No utilice software "pirata" (software sin licencia de uso). La empresa cuenta con licencias para diversos productos y recomendaciones de software gratuitos útiles para tareas diversas

ANEXO 5

INSTALACION DE SOWFTARE BACK TRACK3

El software a instalar es Back Track3, se procede a descargar el software de la siguiente página http://www.backtrack-linux.org/downloads/ el cual pesa 694MB, es un live cd, se lo instala en un computador con las siguientes características: procesador Intel Core 2 Duo, memoria de 2gb, disco de 20 GB; a continuación se muestra el proceso de instalación del software:

Se escoge la opción BT· Graphicsmode (KDE)[127], esta opción permite ingresar al modo gráfico de la aplicación.

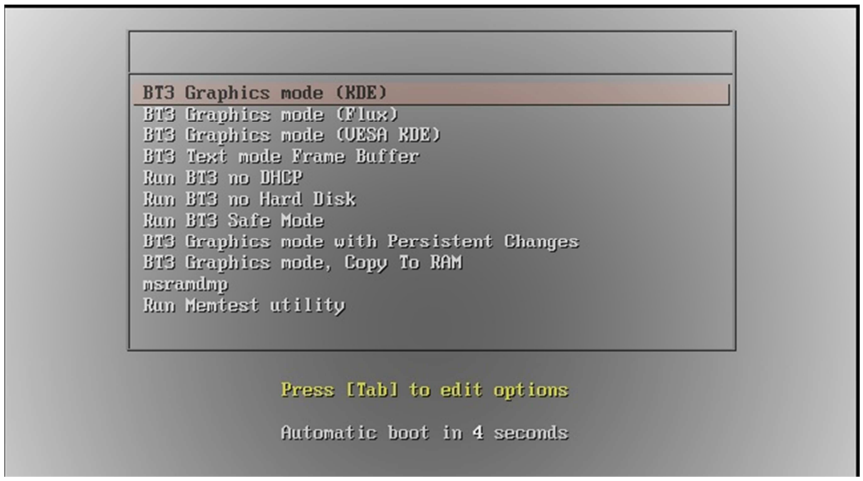


Figura C. 1 BackTrack
Fuente: Los autores

Los procesos para el ingreso al equipo empiezan a cargar.

[127]KDE es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

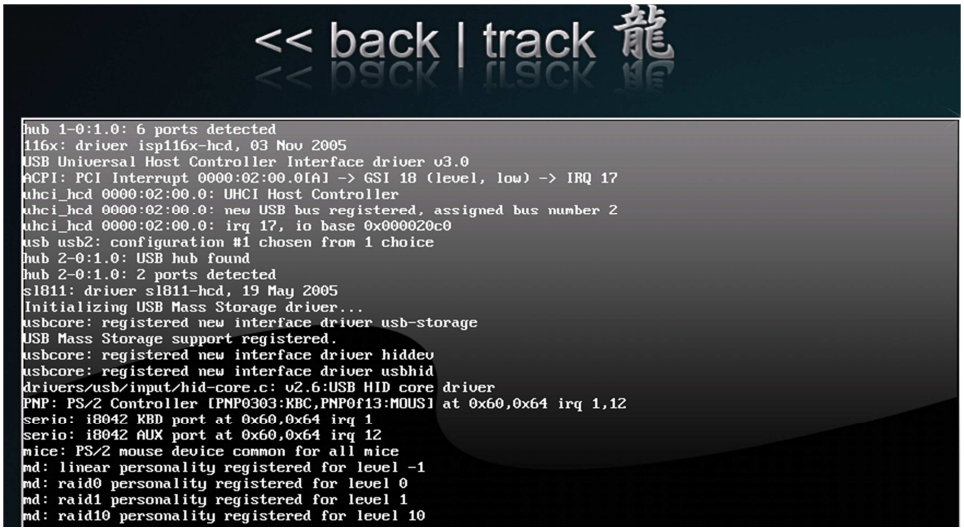


Figura C. 2 BackTrack
Fuente: Los autores

Creación y montaje de los filesystems[128] del software.

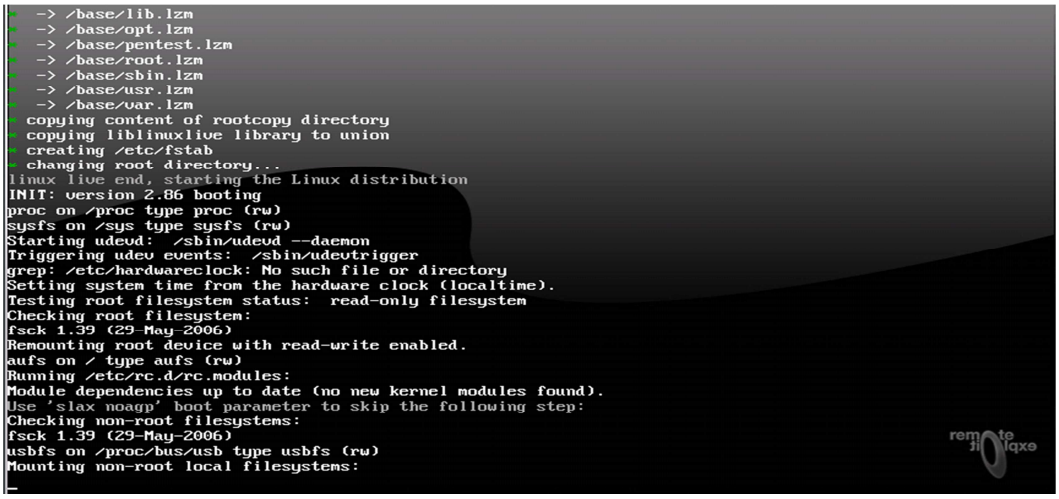


Figura C. 3 BackTrack
Fuente: Los autores

En la siguiente imagen, se puede visualizar la carga del entorno gráfico.

[128]Un sistema de archivos (o archivos) es un medio para organizar los datos que se espera se mantenga después de que un programa termina proporcionando los procedimientos para almacenar, recuperar y actualizar los datos, así como gestionar el espacio disponible en el dispositivo (s) que lo contienen.

Figura C. 4 BackTrack
Fuente: Los autores

La correcta carga del software es mostrada en la siguiente imagen:

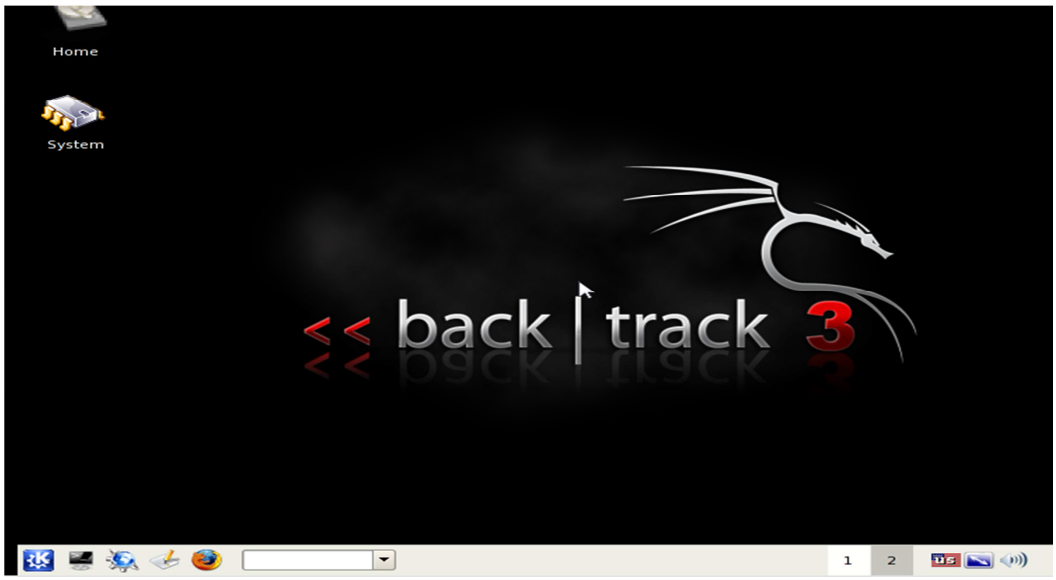


Figura C. 5 BackTrack
Fuente: Los autores

BIBLIOGRAFÍA

- TRIPOD.***Cómo funciona una red***, de http://joan004.tripod.com/clatop.htm
- vulnerabilityTEAM. ***GuiaEscencial para el Escaneo de Vulnerabilidades***, dehttp://vulnerabilityteam.wordpress.com/contenidos/guia-escencial-para-el-escaneo-de-vulnerabilidades/
- EL PORTAL DE ISO 27001 EN ESPAÑOL. ***Sistema de Gestión de la Seguridad de la Información,*** de http://www.iso27000.es/sgsi.html#section2
- WIKIPEDIA. ***Aircrack-ng,*** de http://es.wikipedia.org/wiki/Aircrack-ng
- WIKIPEDIA. ***BackTrack,*** de http://es.wikipedia.org/wiki/BackTrack
- WIKIPEDIA. ***Nessus,*** de http://es.wikipedia.org/wiki/Nessus
- NMAP.org. ***Guía de referencia de Nmap (Página de manual),*** de http://nmap.org/man/es/
- WIKIPEDIA. ***OpenVas,*** de http://es.wikipedia.org/wiki/OpenVAS
- GFI LANGUARD. ***Comprehensive network security for businesses,*** de http://www.gfi.com/network-security-vulnerability-scanner
- NMAP.org. ***Zenmap,*** de http://nmap.org/zenmap/
- International Standard Organization,***ISO/IEC 27001:200,***de http://www.iso.org/iso/catalogue_detail?csnumber=42103
- Alexander Alberto Ph.D, ***Diseño de un Sistema de Gestión de Seguridad,*** Editorial Alfaomega, Colombia, 2007
- British Standard Institute, ***Seguridad de la Información ISO/IEC 27001,***de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/
- Javier Cao Avellaneda, ***Sistemas de Gestión Seguridad de la Información***, de sgsi-iso27001.blogspot.com/

Otros sitios Web:

- http://www.comware.com.ec/jsp/user/go.do?sectionCode=20
- http://www.angelfire.com/cantina/oronaweb/topologia.htm
- http://ww1.activeweb.es/cybersolution/pagina5.html
- Intranet: iso.comware.com.ec
- http://www.monografias.com/trabajos82/que-es-red/que-es-red.shtml
- http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- http://www.yaguarete-sec.com/the-news/49-amenazas.html
- http://www.iso27000.es/download/doc_iso27000_all.pdf
- https://www.ccn-cert.cni.es/publico/herramientas/pilar43/magerit/index.html
- www.imfperu.com/.../standard__adm_risk_as_nzs_4360_1999.pdf
- http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- http://rm-inv.enisa.europa.eu/methods_tools/t_ebios.html
- http://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/
- http://www.icd.go.cr/sitio/downloads/uploads/web_icd_pdf/gestionriesgo/gr_004.pdf.pdf
- http://www.dspace.espol.edu.ec/bitstream/123456789/8080/1/Implementaci%C3%B3n%20del%20primer%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf
- www.docstoc.com/docs/103232605/Gesti n-Directiva
- www.iso27000.es/faqs.html
- dspace.espoch.edu.ec/bitstream/123456789/1533/1/18T00474.pdf