SOPORTE TÉCNICO Y DE USUARIOS, MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE SOFTWARE, EQUIPOS Y SERVIDORES, IMPLEMENTACIÓN Y CONFIGURACIÓN DE SOFTWARE LIBRE PARA EL MEJORAMIENTO DE PROCESOS, INVESTIGACIÓN Y DOCUMENTACIÓN DE LA INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS DE LA EMPRESA A.T.H. A TODA HORA S.A. CON ÉNFASIS EN LA SEGURIDAD INFORMÁTICA.

LUIS CARLOS GÓMEZ DÍAZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2010

SOPORTE TÉCNICO Y DE USUARIOS, MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE SOFTWARE, EQUIPOS Y SERVIDORES, IMPLEMENTACIÓN Y CONFIGURACIÓN DE SOFTWARE LIBRE PARA EL MEJORAMIENTO DE PROCESOS, INVESTIGACIÓN Y DOCUMENTACIÓN DE LA INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS DE LA EMPRESA A.T.H. A TODA HORA S.A. CON ÉNFASIS EN LA SEGURIDAD INFORMÁTICA

LUIS CARLOS GÓMEZ DÍAZ

Trabajo de grado presentado como requisito para optar por el título de Ingeniero de Sistemas

Director: Ing. Manuel Guillermo Flórez Becerra M.Sc.
Docente
ESCUELA DE INGENIERIA DE SISTEMAS E INFORMÁTICA – UIS

Tutor: Juan Carlos Marciglia Llanos
Ingeniero de Soporte a la Infraestructura
A TODA HORA S.A.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2010

DEDICO ESTE PROYECTO

A DIOS por ser la fuerza que me guía en mi camino y por darme la Sabiduría, la fuerza y el coraje que me acompañaron en los momentos más difíciles, para poder seguir adelante con todas las metas que me propongo superando todos los obstáculos.

A mi padre y a mi madre que son las personas que más quiero, por darme ese apoyo incondicional que me ha hecho la persona que soy, por los sacrificios que han hecho por mí y por mis hermanos, porque gracias a ellos he logrado realizar este gran sueño y gracias a ellos es que tengo tantas bendiciones en la vida.

A mis hermanos, por estar a mi lado, por todos los buenos momentos que hemos compartido, por ser las personas que son, y por ser un apoyo y una alegría fundamental en mi vida.

A mi mamá Hilda porque ha sido como una segunda mamá para mí, porque siempre he contado con ella, porque me ha dado su apoyo y me ha acompañado en muchos momentos esenciales de mi vida.

A mi nona Matilde que ahora está en el cielo, por regalarme sus bendiciones y oraciones y por el cariño que me brindo en el poco tiempo que estuvimos juntos, tiempo en que la aprendí a querer por ser la maravillosa persona que fue, que Dios la tenga en su gloria.

A todas las demás personas que quiero, que me han apoyado, que creyeron en mi y que hicieron posible que pudiera ser lo que soy en este momento.

AGRADECIMIENTOS

A mi Director de proyecto Manuel Guillermo Flórez, por haber confiado en mí, por haberme guiado y asesorado, y por haberme brindado la ayuda necesaria para poder emprender y seguir este gran proceso.

A mi tutor Juan Carlos Marciglia, por compartirme sus conocimientos y por apoyarme durante el periodo de la práctica.

A mis compañeros de práctica Luisa Fernanda Arenas, Zander Alejandro Otero, Daniel Rodrigo Quintero y Cristian Camilo, porque ellos aportaron para que la práctica fuera una grata experiencia, y con ellos compartí alegrías y conocimientos.

A mi jefe Angélica Lara, por haberme brindado un gran apoyo durante la práctica en los momentos que más lo necesite, ayudándome a cumplir mis objetivos y haciendo que esta experiencia aportara muchas cosas a mi vida profesional.

A todas las personas de la empresa que aportaron sus conocimientos en diferentes campos y me brindaron su apoyo cuando los necesite.

A la empresa ATH, por brindarme la oportunidad de emprender esta experiencia de trabajo tan importante para mis aspiraciones profesionales, donde adquirí muchos conocimientos y de donde me llevo muy buenos recuerdos.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

GLOSARIO

ATAQUES DOS: (Denial of Service). Ataques de denegación de Servicios. Ataques a sistemas informáticos que producen que algunos elementos dentro de éste pierdan su propiedad de disponibilidad, afectando así, el funcionamiento del sistema.

BACKUP: También conocido en español como copia de respaldo. Técnica utilizada para la protección de la disponibilidad de los datos que consiste en generar copias redundantes de determinada información digital con el fin de prevenir su pérdida o afectación.

BLADE: Servidores Físicos de gran capacidad acoplados especialmente para el aprovechamiento de espacios en los centros de cómputo empresariales.

CLÚSTER: Conglomerado de recursos hardware independientes que se comportan como si fueran un único computador, compartiendo todos sus recursos y permitiendo que estos estén disponibles para cualquier proceso que se ejecute dentro del conglomerado. Esta unión se hace con el objetivo de tener mayor capacidad de procesamiento de datos y es utilizado en software crítico y aplicaciones de supercomputación.

CUCHILLA BLADE: Hace referencia a cada servidor físico dentro de un Blade. Cada cuchilla contiene recursos Hardware entre los que están procesadores, memoria y disco duro.

DATACENTER: También conocido como Centro de procesamiento de datos (CDP) o Centro de Cómputo. Es la ubicación donde se concentran la mayoría de los recursos tecnológicos más importantes para el procesamiento de la información en una Organización.

DATASTORE: Base de datos implementada para almacenar datos de múltiples fuentes.

DIRECCIÓN IP: Identificador lógico y jerárquico de una interfaz de red en un dispositivo dentro de una red de comunicaciones que utilice el protocolo de internet IP.

ESX: Sistema Operativo ligero en modo texto, utilizado por VMware Infrastructure como base para la implementación de la infraestructura virtual.

GATEWAY: Conocido en español como puerta de enlace. Es un dispositivo informático configurado y con tecnología necesaria, para dotar a las máquinas de una red local (LAN) conectadas a éste, de acceso hacia una red exterior.

KERNEL: Conocido en español como Núcleo. Es la parte principal de un sistema Operativo y el encargado de la gestión de recursos del sistema y de la comunicación a bajo nivel con el hardware.

LIVE CD: Disco autoejecutable con un sistema operativo y diferentes aplicaciones, que no necesita de su instalación para ser ejecutado.

LUN: (Logical Unit Number). Identificador de una unidad de disco dentro del conjunto de discos que conforman una RAID.

MBR: (Máster Boot Record). Es el primer sector de un disco duro físico que usualmente es utilizado para almacenar la tabla de particiones del sistema.

NIC: (Network Interface Card). Conocida en español como tarjeta de interfaz de red. Permite la interfaz física de comunicación entre los dispositivos y los medios de red. Se encarga generar las señales que representen los datos a transmitir por los medios de comunicación. Cada NIC se identifica con un número único denominado MAC.

NTP: (Network Time Protocol). Protocolo de internet utilizado para la sincronización de relojes de dispositivos en redes informáticas con latencia variable.

PnP: (Plug And Play). Tecnología que permite a un dispositivo informático ser reconocido por un equipo al conectarlo, sin necesidad de ser configurado ni tener que realizar ninguna otra acción.

PROTOCOLO: Conjunto de reglas normalizadas utilizadas para determinado procedimiento.

PROXY: Hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado a una red externa.

PUERTO: interfaz para la recepción, conversión y reenvío de datos en diferentes formatos, para que puedan ser interpretados por diferentes dispositivos en un sistema informático.

RAID: (Redundant Array of Independent Disks). Unión lógica de discos independientes con el objetivo de implementar tolerancia a fallos, mejor rendimiento y mayor capacidad a un sistema de información.

RHEL: (Red Hat Enterprise Linux). Distribución comercial del sistema operativo Linux para entornos empresariales desarrollada por la compañía Red Hat.

ROUTER: Conocido en español como enrutador. Dispositivo de red intermedio que permite el direccionamiento de paquetes dentro de una red informática para que estos puedan transportarse desde su origen hacia su destino a través de los medios de red.

SAN: (Storage Area Network). Red concebida para conectar servidores, RAIDs y librerías de soporte. Su función es conectar de manera rápida, segura y fiable los elementos que la conforman.

SCRIPT: Archivo de comandos simple (por lo general archivo de texto plano), que se utiliza para ejecutar una instrucción informática.

SERVIDOR APACHE: Servidor web multiplataforma que funciona bajo el protocolo de internet http, y provee a los clientes de la posibilidad de visualización de páginas web.

SHELL: Interfaz de línea de comandos. Aplicación que sirve para ejecutar comandos mediante la inserción de códigos en texto simple.

SWITCH: Conmutador de red que se encarga de interconectar dos o más segmentos de red), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

VIRTUALIZACIÓN: Abstracción de recursos hardware físicos con el fin de crear elementos lógicos formados como si fueran recursos físicos independientes para su utilización en diferentes fines, como por ejemplo, creación de múltiples sistemas operativos independientes dentro de un solo servidor físico.

VLAN: (Virtual LAN). Conocida en español como red de área local virtual. Son redes creadas lógicamente, independientes dentro de una misma red física.

VMFS: (Virtual Machine File System). Tipo de Sistemas de Archivos propio de los Sistemas Operativos ESX. Este tipo de sistemas de archivo fue diseñado específicamente para cumplir con todos los requerimientos de la solución VMware Infrastructure.

VMWARE: Firma de productos software para virtualización de equipos e infraestructuras.

VMWARE DPM: (Distributed Power Management). Utilidad de administración de consumo de energía que ofrece la solución tecnológica VMware Infraestructure. Esta utilidad administra de manera inteligente el consumo de energía dentro de la infraestructura virtual permitiendo ahorros de hasta 50% de energía de la que normalmente consume una infraestructura virtual VMware que no tenga esta utilidad.

VMWARE DRS: (Distributed resource Scheduler). Utilidad de la solución tecnológica VMware Infrastructure que permite la distribución inteligente, automática y personalizada de recursos físicos disponibles que han sido asignados a un conjunto de recursos lógicos para su utilización.

VMWARE HA: (High Availability). Utilidad de Alta disponibilidad que ofrece la solución tecnológica VMware Infrastructure , para proporcionar continuidad de ejecución de las máquinas virtuales en caso de presentación de fallas o caída de un servidor físico dentro de la infraestructura virtual o fallas de Sistema Operativo en una máquina virtual. Esta propiedad es posible con ayuda de las utilidades VMware VMOTION y VMware DRS que responden en caso de necesitarse la propiedad de HA.

VMWARE INFRASTRUCTURE: Solución tecnológica propiedad de la compañía de software de virtualización VMware, que permite realizar virtualización de completas infraestructuras empresariales, generando diferentes beneficios a las empresas en donde se implementa.

VMWARE VMOTION: Utilidad de la solución tecnológica VMware Infrastructure que permite la migración de maquinas virtuales de un servidor físico a otro incluso con las máquinas en caliente (encendidas y operando).

VPN: (Virtual Private Network) Tecnologia que permite extender una red local sobre una red pública (como Internet), para permitir acceso remoto de forma segura a la red local utilizando para ello la infraestrucura de la red pública.

VSMP: (Virtual Symmetric Multiprocessing). Método de Multiprocesamiento simétrico en el cuál dos o más procesadores virtuales son mapeados a una misma máquina virtual. Con este sistema múltiples aplicaciones que tengan sistema operativo y memoria en común, pueden ser ejecutados por dos o más procesadores.

XAMPP: Solución Web independiente de plataforma que incluye el servidor Web Apache, el manejador de base de datos MySQL, y los intérpretes PHP y PERL.

RESUMEN

TITULO: SOPORTE TÉCNICO Y DE USUARIOS, MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE SOFTWARE, EQUIPOS Y SERVIDORES, IMPLEMENTACIÓN Y CONFIGURACIÓN DE SOFTWARE LIBRE PARA EL MEJORAMIENTO DE PROCESOS, INVESTIGACIÓN Y DOCUMENTACIÓN DE LA INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS DE LA EMPRESA A.T.H. A TODA HORA S.A. CON ÉNFASIS EN LA SEGURIDAD INFORMÁTICA[*].

AUTOR: LUIS CARLOS GÓMEZ DÍAZ[**].

PALABRAS CLAVES: MANTENIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA, VMWARE INFRASTRUCTURE, SOFTWARE LIBRE, SEGURIDAD DE LA INFORMACIÓN.

CONTENIDO:

Este proyecto ha sido desarrollado a partir de la necesidad de la empresa A Toda Hora S.A de proteger y mejorar los procesos dependientes de la infraestructura tecnológica empresarial. El proyecto está dirigido a personas que requieran conocer acerca de aspectos relacionados con la administración de la Infraestructura Tecnológica empresarial y el mejoramiento de procesos afines a los sistemas de Información.

Los Principales objetivos de la práctica fueron el mantener en las mejores condiciones posibles los sistemas informáticos empresariales, llevando a cabo procedimientos creados en la empresa para prevención y resolución de problemas presentados en estos, aportar propuestas y colaborar en la investigación de proyectos para el mejoramiento de los procesos involucrados con la infraestructura tecnológica, revisar la implementación de la seguridad de la información en la organización haciendo énfasis en la seguridad de los Sistemas Operativos, y además involucrarse con otras áreas de la empresa en proyectos o gestiones que tuvieran que ver con el soporte a la Infraestructura tecnológica empresarial y los sistemas de información.

Durante la práctica se realizaron varios logros en concreto. Se consiguió que los elementos informáticos utilizados por los recursos humanos empresariales en la sede de la práctica y en las sedes regionales de la empresa permanecieran en correcto funcionamiento durante el transcurso de la práctica empresarial. Se mejoró el proceso de inventariado de la infraestructura empresarial y algunos otros procesos, mediante la investigación e implementación de la herramienta OCS Inventory Agent. Se consiguió realizar la virtualización de los servidores transaccionales de la empresa, con la ayuda de muchas otras personas que participaron en el proyecto, mediante la implantación de la solución tecnológica Vmware Infraestructure. Se elaboró un manual que puede ser útil para cualquier persona que desee abordar temas relacionados con la seguridad de la información empresarial, que está enfocado en la seguridad de los sistemas operativos Windows y en infraestructuras de empresas de tipo financieras.

---

[*] Proyecto de Grado

[**] Facultad de Ingenierías Fisicomecánicas, Escuela de Ingeniería de Sistemas e Informática. Director: Ing. Manuel Guillermo Flórez Becerra M.Sc.

ABSTRACT

TITLE: TECHNICAL AND USERS SUPPORT, CORRECTIVE AND PREVENTIVE MAINTENANCE OF SOFTWARE, EQUIPMENT AND SERVERS, IMPLEMENTATION AND SETUP OF FREE SOFTWARE FOR IMPROVEMENT OF PROCESSES, RESEARCH AND DOCUMENTATION FOR THE INSTALLATION AND SETTING OF THE A TODA HORA S.A COMPANY OPERATING SYSTEMS WITH EMPHASIS ON INFORMATION SECURITY[*].

AUTHOR: LUIS CARLOS GÓMEZ DÍAZ[**].

KEYWORDS: MAINTENANCE OF TECHNOLOGICAL INFRASTRUCTURE, VMWARE INFRASTRUCTURE, FREE SOFTWARE, INFORMATION SECURITY.

CONTENT:

This project has been developed from the A Toda Hora S.A Company need for protect and improve the dependent processes of enterprise technology infrastructure. The project is guided at people who require knowing about aspects related to the administration of the enterprise technology infrastructure and the improvement of processes related to information systems.

The main objectives of the practice were, to keep in the best possible conditions the company information systems, carrying out procedures created in the company for prevention and resolution of problems presented in these, make proposals and collaborate on research projects for the improvement of the processes involved with technology infrastructure, review the information security implementation in the organization with an emphasis on the security of the operating systems, and also get involved with other areas of the company in projects or managements that have to do with the support of enterprise technological infrastructure and information systems.

During the practice several achievements in particular were realized. There was obtained that the computing elements used by enterprise human resources in the practice place and the regional places of the company remain in proper functioning during the course of enterprise practice. Was improved the process of inventory of enterprise infrastructure and some other processes through research and implementation of the OCS Inventory Agent tool. There was obtained virtualizing the transactional servers of the company, with the help of many others who participated in the project, through the introduction of the VMware infrastructure technological solution. There was developed a manual that may be useful for anyone who wants to address issues related to the security of enterprise information, which is focused on the security of the Windows operating systems and infrastructure of financial enterprises.

[*] Work of degree

[**] Physical-Mechanical Engineering College. Systems and Informatic Engineering School. Director: Ing. Manuel Guillermo Flórez Becerra M.Sc.

INTRODUCCIÓN

La empresa ATH es una empresa prestadora de servicios de carácter financiero y se enfoca en la administración de la red de cajeros automáticos del Grupo Aval en toda Colombia. La sede principal de la empresa se encuentra ubicada en la ciudad de Bogotá y se encuentra dividida en varias áreas las cuales cumplen un papel específico dentro de la organización. El área de Soporte a la infraestructura cuenta con cinco personas (coordinador de soporte, jefe de soporte, practicante de soporte y dos personas de outsourcing) encargados de mantener en buen funcionamiento toda la infraestructura, utilizando las herramientas adecuadas para el buen mantenimiento de los equipos como antivirus y herramientas de eliminación de virus (con la ayuda del personal de soporte de Symantec) atendiendo todas las eventualidades que se presentan en los equipos, tales como fallas en sistemas operativos de la empresa (se utilizan sistemas operativos Windows, la mayoría XP), fallas en los aplicativos (a causa de virus, perdida de archivos, permisos sobre archivos, etc.), también es la encargada de administrar los permisos de usuarios de la empresa, tanto locales como de dominio, de hacer inventario de software autorizado de la empresa, de la configuración y administración del antivirus en los equipos y de la asesoría a los usuarios de la empresa localmente y de las regionales. El área también está encargada de colaborar con otras áreas como telecomunicaciones, soporte técnico y seguridad de la información para proyectos como migración de ip's para segmentación o virtualización de la infraestructura en pro de mejorar la el manejo y la seguridad de los procesos de la empresa, de analizar que necesidades nuevas tiene la empresa en cuanto a tecnología y herramientas software, y así sacar adelante cualquier proyecto de nuestra área o las demás en colaboración mutua aportando propuestas de soluciones y apoyando a éstas.

1. DESCRIPCIÓN DE LA PRÁCTICA EMPRESARIAL.

1.1 DESCRIPCIÓN DE LA EMPRESA

1.1.1 Nombre de la Empresa

A Toda Hora S.A.

1.1.2 Presentación de la empresa

A TODA HORA S.A., ATH[1], es una empresa de los Bancos de la Red de Grupo Aval, que orienta sus labores al desarrollo y soporte tecnológico de canales electrónicos por medio de los cuales se efectúan transacciones bancarias, tanto para los mencionados bancos como para las demás entidades del sector financiero colombiano y del exterior.

A TODA HORA S.A. ha sido catalogada por la Superintendencia Financiera como una entidad de Pago de Bajo Valor y en consecuencia entró bajo su vigilancia a partir del año 2005. ATH busca el liderazgo de servicios de banca electrónica, principalmente en lo correspondiente a dispositivos de auto-servicio. Los resultados obtenidos se reflejan en importantes beneficios y economías de escala en la operación, para sus Accionistas. ATH tiene como objetivo dar servicios más ágiles y oportunos a los Clientes de las Entidades financieras, servicios que se basan en brindar una operación confiable y segura mediante tecnología adecuada, innovación, productividad en la operación y un alto posicionamiento de marca y calidad, con un equipo humano especializado. El reto que significan los cambios tecnológicos en el mercado ha implicado que la investigación y desarrollo de nuevos servicios sea una constante.

1.1.3 Misión y Visión Corporativa

- ✓ Misión

La empresa A Toda Hora S.A tiene como propósito Proveer a los clientes los mejores servicios de banca electrónica con alta disponibilidad y seguridad, utilizando tecnología acertada para entregarlos con el nivel de servicio acordado y la eficiencia esperada por los accionistas.

- ✓ Visión

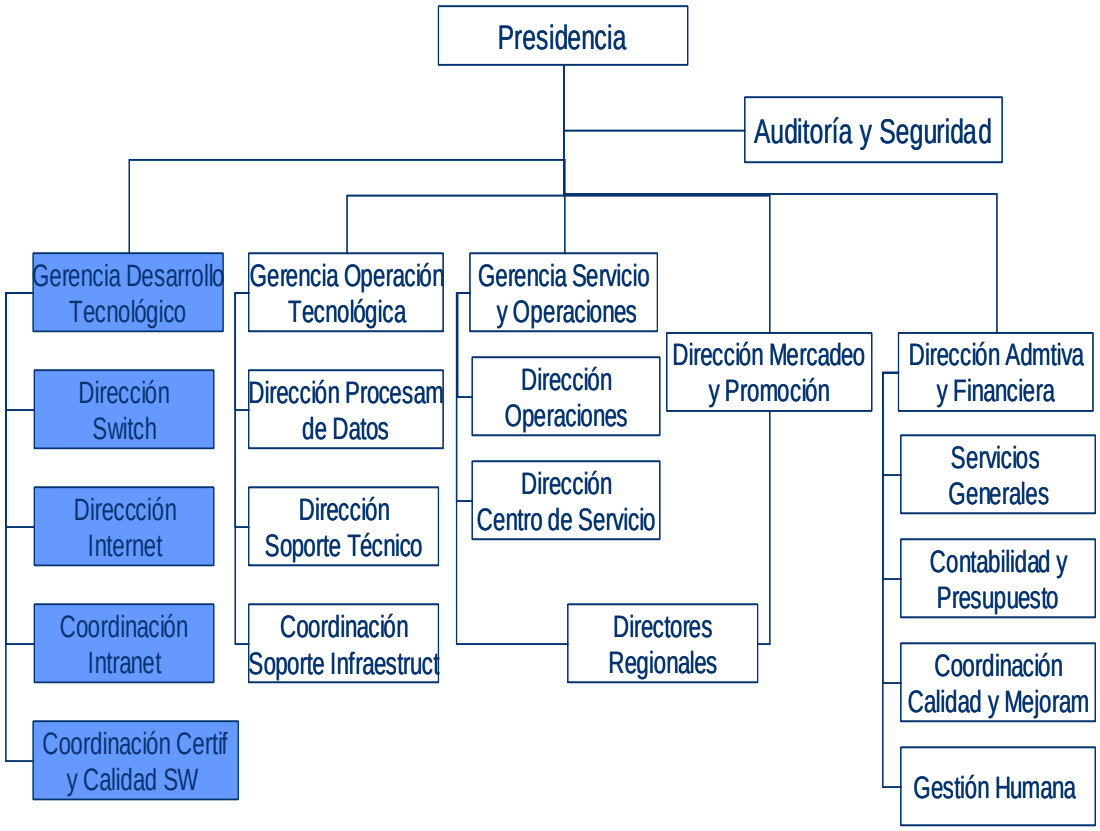
Consolidarse como el núcleo tecnológico y operativo de los canales electrónicos para las Entidades del Grupo Aval, dando soporte a las estrategias que conlleven prestar

[1] A Toda Hora S.A.

servicios con un alto componente de tecnología y/o carácter corporativo, para lograr el liderazgo y posicionamiento en la banca colombiana.

1.1.4 Organigrama

Figura 1. Organigrama de ATH



Fuente. ATH

1.1.5 Reseña histórica

ATH Inicio operaciones el 29 de agosto de 1991, cuando se ve la necesidad por parte del grupo financiero más importante del país "EL GRUPO AVAL[2]" de crear una entidad que administrara la red de cajeros electrónicos y transmitiera datos del grupo financiero a nivel nacional. Gracias a la ley 45/90 de la reforma financiera, la cual autorizó a las entidades del sector para poder conformar compañías de servicios

[2] Grupo Aval Acciones y Valores S.A. tiene como objeto social la compra y venta de acciones, bonos y títulos valores de entidades pertenecientes al sistema financiero y de otras entidades comerciales. Entre las filiales se encuentran Banco de Bogotá S.A., Banco de Occidente S.A., Banco AV Villas S.A., Banco Popular S.A., Porvenir S.A., Leasing de Occidente S.A.

técnicos y administrativos, y realizar funciones en el campo de la sistematización, administración, organización y conexión de redes de cajeros, manejo de información, procesamiento y transferencia de fondos e información, nace A TODA HORA S.A. "ATH Cajeros Automáticos" enfocada a prestar el mejor servicio al cliente a todos los tarjetahabientes afiliados a redes a nacionales e internacionales en el país. Promesa que ha venido cumpliendo hasta el momento.

La red ATH se convirtió en la mejor alternativa del mercado para satisfacer las necesidades de modernización electrónica y de auto servicios financieros a través del uso de tarjetas débito y crédito por medios electrónicos.

Así ATH logró brindar una operación rentable para los asociados, sin dejar de lado la innovación y la calidad que día a día ponemos a su servicio.

1.991: Nace ATH como Red con Banco AV Villas, Banco Bogotá y Banco de Occidente.

1.993: Inicia operación el Equipo Central ATH.

1.997: se unen a la Red, Ahorramás y Banco Popular, logrando realizar 3.5 millones de transacciones.

1.997: Se habilita el primer cajero del país con la opción de Pago de Servicios Públicos.

1.998: Nacen los servicios Interaval apoyados por ATH.

2.000: Inicia operación de la infraestructura de Internet para las entidades AVAL.

2.001: Se habilita el pago de servicios por Internet en los portales de las entidades con la opción de domiciliar.

2.001: ATH desarrolla para las entidades el Sistema de Pagos Seguros en Internet B2C, ofreciendo a las empresas realizar sus negocios a través de este medio.

2.002: Nace MAX y con él se reestructura ATH.

2.003: ATH crea el Centro de Servicios con el objetivo de canalizar las solicitudes de las Entidades.

2.004: ATH llega al cajero 1.000 con el cajero Banco Popular Centro Comercial Caobos.

2.004: Se instala el primer cajero con depositario Inteligente de cheques.

2.004: ATH es la primera Red en Latinoamérica con Encriptación 3DES.

2.005: Se crea el Centro de Monitoreo de Seguridad, quienes manejan las cámaras de TV.

2.005: ATH desarrolla un nuevo canal: Los Agilizadores Electrónicos.

2.006: ATH instala el primer cajero con Depósito de efectivo.

2.007: ATH desarrolla un nuevo canal: Los Corresponsales No Bancarios o Puntos de Servicio.

2.007: ATH llega al cajero 2.000. Banco AV Villas Almacén SAO Sincelejo.

2.007: ATH lanza el programa SERVICIO SUPERIOR SIEMPRE y con él, una cultura de servicio hacia sus clientes internos y externos.

2.008: ATH llega a más de 2.008 cajeros, siendo así la Red de cajeros más grande del País.

2.008: ATH implementa un nuevo sistema mejorando los niveles de seguridad para las Entidades de la Red de Servicios Aval: Autenticación más fuerte.

2.008: ATH brinda soporte técnico a los nuevos servicios implementados en los canales electrónicos para las Entidades de la Red de Servicios Aval: Banca Móvil.

1.2 DESCRIPCIÓN DEL PROYECTO

1.2.1 Planteamiento del problema

Para evitar interrupciones en los procesos y con el fin de que todas las actividades de la empresa funcionen correctamente es necesario contar con un adecuado manejo de los elementos tales como la infraestructura, y las herramientas que se estén utilizando para procurar sacar el mayor provecho de estos y así todas las actividades resulten tal y como se han planeado. Para esto son necesarias las labores de soporte técnico y a usuarios, las cuales facilitan y mejoran las labores y los procesos en la empresa, y dan solución a inconvenientes presentados. Para la realización de estas labores como primer paso se debe recibir la solicitud de tarea y analizar el modo en el que debe dar respuesta a la petición realizada. Después de esto como resultado del análisis de la solicitud se acuerda el método más óptimo para asegurar la correcta resolución de la petición.

También es necesario el mantenimiento preventivo y correctivo de los equipos. El mantenimiento preventivo se trata de hacer los ajustes, modificaciones, cambios, limpieza y reparaciones (generalmente sencillos) necesarios para mantener cualquier herramienta o equipo en condiciones seguras de uso, con el fin de evitar posibles daños al operador o al equipo mismo y es realizado con el fin de conservar los equipos, herramientas y software en un óptimo estado y así evitar ineficiencias en los

sistemas y aplicaciones o evitar daños que pueden ser irreparables si no se les da el debido manejo. El correctivo se trata de reparar, cambiar o modificar cualquier herramienta, maquinaria o equipo cuando se ha detectado alguna falla o posible falla que pudiera poner en riesgo el funcionamiento seguro de la herramienta o equipo y de la persona que lo utiliza. Se utiliza también cuando existen daños que afectan el funcionamiento normal de los elementos mencionados, los cuales pueden ser reparados siguiendo un debido proceso.

En el ámbito empresarial es indispensable el utilizar métodos y herramientas adecuadas para optimizar los procesos y mejorar la productividad del tiempo y del trabajo, y además, en la actualidad las empresas le están perdiendo el miedo al software libre, entre otras causas porque las empresas, hasta ahora, pensaban que el software libre iba a disminuir su volumen de negocio, pero ya se han dado cuenta las empresas que muy al contrario, con el software libre éstas pueden ofrecer servicios de mantenimiento, de actualizaciones o modificaciones, entre otras líneas de negocio. Por esto se trabajará en la investigación e implementación de software libre disponible que pueda ser adaptable a las necesidades de la empresa, ya que éste ofrece muchas ventajas como la libertad de uso y distribución, la economía, independencia tecnológica, corrección de fallos, etc. Esta investigación se realiza en búsqueda de mejorar los procesos y dar apoyo a las actividades del área de soporte técnico.

Otra gran problemática son las amenazas a la seguridad de la información, que debido a su gran importancia, debe ser protegida de la mejor manera posible de todos los ataques a los que está expuesta, y que afectan aspectos de la información como la confidencialidad, integridad o uso ilegítimo de ésta, que podrían evitarse con un análisis de riesgos y el uso de políticas de seguridad, con la ayuda de todas las herramientas posibles, corrigiendo la mayor cantidad de vulnerabilidades en la seguridad de los equipos sin afectar su desempeño en las tareas para que se utilizan, por esto se trabajara en el manual de instalación y configuración de sistemas operacionales de la empresa con énfasis en la seguridad de la información.

1.2.2 Objetivos

1.2.2.1 Objetivo General

Brindar soporte y asesoría técnica a todas las dependencias de la empresa A Toda Hora S.A, hacer mantenimiento preventivo y correctivo de software y equipos, dar apoyo en la investigación y la implementación de software libre, realizar informes de todas las actividades desempeñadas, elaborar un manual de usuario para la instalación y configuración segura de los de sistemas operativos de la empresa.

1.2.2.2 Objetivos Específicos

- ✓ Dar soporte técnico preventivo y correctivo a la infraestructura tecnológica de todas las dependencias.

- ✓ Instalar, reparar y actualizar Sistemas Operativos, software, aplicativos y herramientas.

- ✓ Instalar, ubicar y entregar al usuario los equipos llevando a cabo un procedimiento específico.

- ✓ Atender a los usuarios y dar solución a cualquier tipo de problema técnico en el momento que se requiera.

- ✓ Como resultado de las prácticas, condensado en los informes, quedará un manual de mantenimiento.

- ✓ Documentar los casos que se investiguen y amerite tenerlos consignados en una base de datos para luego consultarlos.

- ✓ Dar apoyo a diferentes proyectos que este implementando la compañía y requiera de nuestra colaboración.

- ✓ Gestionar con otras áreas de la empresa cuando sea necesario para apoyar actividades que necesiten la acción de distintas áreas.

- ✓ Investigar, Implementar y configurar software libre que permita mejorar los procesos en el área.

- ✓ Como resultado de la investigación en software libre quedará un informe de investigación sobre este tema.

- ✓ Analizar los aspectos utilizados en la instalación y configuración de los sistemas operativos de la empresa y detectar posibles errores en el proceso, fallas o vulnerabilidades existentes.

- ✓ Hacer investigación sobre la instalación y configuración de sistemas operacionales haciendo énfasis en la seguridad de la información y en los sistemas utilizados en la empresa.

- ✓ Hacer un manual de seguridad como resultado de la instalación de sistemas operativos y la investigación de seguridad en la empresa ATH.

1.2.3 Justificación

Con la realización de esta práctica se buscó hacer un aporte analítico para asesorar a los usuarios en el manejo de las herramientas de trabajo, dar solución a los problemas técnicos que se presentaran con el fin de agilizar las operaciones, hacer implementación y configuración de software, realizar el mantenimiento de equipos para contar con su buen funcionamiento utilizando herramientas que facilitaran los procesos a realizar en cada caso. También se buscó apoyar la investigación de software libre en la empresa implementando el software para inventario de hardware-software e implementación de paquetes (OCS Inventory) que ayuda a facilitar varios procesos de control. También se buscó involucrarse junto con las áreas de soporte técnico, telecomunicaciones y seguridad de la información a proyectos en desarrollo, como el proyecto de virtualización de infraestructura (Vmware Infrastructure) para los servidores de la empresa. También estudiar las políticas y características de seguridad implementadas para los sistemas operativos y la infraestructura de la empresa con el fin de analizar y tratar de mejorar estos aspectos de seguridad con los requerimientos de la empresa.

En la práctica se aplicaron los conocimientos adquiridos durante la carrera y otros adquiridos durante la misma práctica para vincularse al ejercicio profesional en las actividades de soporte técnico y de usuarios en la empresa A.T.H, se hizo un aporte analítico y también con ayuda de los compañeros de trabajo, sus conocimientos, experiencia y además una base de datos que sirvió como guía en varias ocasiones donde se relaciona casos anteriormente resueltos de inconvenientes presentados y procedimientos a seguir en diferentes eventualidades en el área, se brindaron soluciones efectivas y rápidas a la mayoría de los problemas que se presentaron en la infraestructura, sistemas operacionales, aplicaciones, herramientas o procesos del área de soporte técnico y buscando la máxima eficiencia de cada uno de estos.

También se buscó la capacitación en el manejo de las herramientas utilizadas para el mantenimiento y la administración de los equipos de la empresa, manejando herramientas como UltaVnc, que es una herramienta de software libre para el acceso remoto a diferentes equipos y servidores tanto locales como regionales, con el fin de

agilizar los procesos del área y solucionar los posibles inconvenientes que se presentaron y que afectaban el desempeño normal de las tareas de trabajo, aumentando así, la productividad del tiempo y del trabajo en la empresa. Se hizo una documentación de algunos casos especiales que se investigaron, resolvieron y consignaron en una base de datos del área para que fueran útiles en el estudio de otros casos a futuro.

Se trabajó con el software libre OCS Inventory que está en uso en la empresa se implemento en los equipos de usuario de la empresa y se empezó a estudiar la viabilidad y a realizar los estudios para evaluar su posible implementación en los servidores. También se apoyo la reciente investigación de repositorios con subversión y Tortoise, otro software libre que podría ser útil en materia de seguridad de la empresa, todo con el fin de dar beneficiar los procesos del área de soporte técnico. También durante la práctica, se realizó una revisión acerca de los procesos de instalación y configuración de los sistemas operativos e infraestructura que maneja la compañía con énfasis en la seguridad de los mismos. Esto servirá como manual para la guía práctica de cualquier persona que tenga el interés en hacer instalaciones de sistemas operativos e infraestructura con los parámetros de seguridad que requiere la empresa. Este tema se hace necesario sobre todo en empresas de este tipo en las cuales la información y la seguridad son de vital importancia. Esta revisión realizada también se hizo con el fin de hacer un mejoramiento e innovación al nivel de seguridad de los sistemas de la empresa.

1.2.3.1 Impacto

- ✓ Los trabajadores de todas las áreas de la Empresa ATH de Bogotá y sus sucursales tuvieron el apoyo y asesoría necesarios en caso de presentarse cualquier inconveniente relacionado con la infraestructura empresarial, los sistemas operativos y las aplicaciones utilizadas en las labores cotidianas.

- ✓ Se mantuvieron en estado óptimo de funcionamiento todos los elementos de la infraestructura empresarial y se solucionaron todos los inconvenientes presentados de manera eficaz.

- ✓ Se mejoraron procesos y agregaron utilidades gracias a la implementación de herramientas de software libre.

- ✓ Se gestiono con diferentes áreas de la empresa cuando solicitaron nuestro apoyo en diferentes tareas de solución a inconvenientes presentados o implementación de proyectos agilizando las tareas.

1.2.3.2 Viabilidad

Tabla 1. Viabilidad del Proyecto

Técnica	Para la práctica se conto con la asesoría, experiencia y aporte de conocimientos de mi tutor Juan Carlos Marciglia y de mis compañeros de trabajo, Luisa Fernanda Díaz, Zander Alejandro Otero y Daniel Quintero. Se contó con la asesoría y apoyo del profesor Manuel Guillermo Flórez para la realización del proyecto. Se dispuso de todos los manuales, bases de datos y elementos de investigación de la empresa con información útil para las actividades realizadas.
Económica	El costo de la práctica empresarial fue accesible gracias a que la empresa contaba con varios de los recursos físicos y tecnológicos necesarios para los procesos. Los otros gastos representados en elementos de investigación, equipos y elementos de trabajo, papelería, sostenimiento y horas de trabajo para la realización del proyecto se tenían presupuestados antes de realizarla.
Social	La empresa ATH se benefició con la realización de la práctica, ya que el desarrollo de ésta fue un elemento fundamental para el óptimo desarrollo de las actividades organizacionales en temas de infraestructura, seguridad y proyectos laborales entre otros, contribuyendo con el logró de los objetivos y misión empresarial.

Fuente. Autor

1.2.4 Metodología

La planeación de una metodología de trabajo, es primordial para obtener los resultados esperados, en un tiempo determinado. Todas las actividades se realizaron bajo la supervisión y coordinación del tutor de la empresa y el director de proyecto de grado.

Se utilizaron todos los recursos disponibles en la empresa y también otros materiales externos que ayudaron a documentarse sobre el uso de las herramientas que se estaban utilizando para el desarrollo de las actividades. Para la parte de investigación y elaboración del manual se procedió a realizar la formulación e introducción al problema para delimitar al máximo el área a trabajar. Después de esto se inició la fase exploratoria donde se utilizaron todos los instrumentos de recolección de datos posibles para la revisión de literatura como libros, manuales, tutoriales, publicaciones y

otros que constituyeron la base de la información a examinar para la investigación. Con ésta literatura obtenida se procedió a consultarla y a hacer la extracción y recopilación de la información necesaria. Después de esto se inició la elaboración del marco teórico para el cual se necesitó realizar previamente un índice que ayudó a guiar la redacción. Finalizada la fase exploratoria se inició la elaboración y selección del diseño apropiado para la investigación. Después de esto se inició con el procesamiento y el análisis de los datos para ir desarrollando las especificaciones del manual a elaborar y profundizando en los detalles más importantes. Por último se realizó el trabajo de gabinete, donde se trabajó en la presentación de los datos de una forma ordenada, tabulada y elaborada incluyendo la síntesis, resultados y conclusiones generadas en el proceso de investigación.

1.2.5 Cronograma de actividades

Tabla 2. Cronograma del Proyecto

<table>
<tr><th>MES</th><th>SEMANA</th><th>ACTIVIDADES PROGRAMADAS</th><th>ACTIVIDADES COMUNES</th></tr>
<tr><td rowspan="4">MES 1</td><td>1</td><td>Inicio práctica. Capacitación e inducción a las actividades de la empresa. Documentación sobre el uso de las herramientas básicas de operación.</td><td rowspan="10">Soporte técnico preventivo y correctivo a la infraestructura tecnológica de todas las dependencias. Atención a los usuarios y solución de cualquier tipo de problema técnico en el momento que se requiera. Instalación, reparación y actualización de Sistemas Operativos, software, aplicativos y herramientas. Instalación, ubicación y entrega al usuario de los equipos llevando a cabo un procedimiento específico. Apoyo en proyectos de la empresa, investigación de software libre y gestión con diferentes áreas</td></tr>
<tr><td>2</td><td>Inicio de investigación sobre instalación de sistemas operativos, formulación y delimitación del problema.</td></tr>
<tr><td>3</td><td>Inicio de revisión de literatura útil para la investigación.</td></tr>
<tr><td>4</td><td rowspan="4">Realización y entrega del primer informe de avances. Análisis y documentación sobre herramientas y métodos utilizados en la instalación de sistemas operativos en la empresa.

Inicio recopilación de información para elaboración de manuales mantenimiento y software libre.</td></tr>
<tr><td rowspan="4">MES 2</td><td>1</td></tr>
<tr><td>2</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td><td rowspan="3">Realización y entrega del segundo informe de avances. Obtención y consulta de literatura útil revisada. Extracción y recopilación de información y datos necesarios para la investigación. Realización del índice guía para el</td></tr>
<tr><td rowspan="2">MES 3</td><td>1</td></tr>
<tr><td>2</td></tr>
</table>

		desarrollo del manual de usuario de S.O.	
	3	Construcción del marco teórico con aspectos que faciliten el proceso de elaboración manual S.O. Realización y entrega del 3er informe de avances.	
	4		
MES 4	1	Inicio realización de manuales de mantenimiento y de software libre.	
	2	Realización y entrega del cuarto informe de avances, desarrollo de especificaciones del manual S.O, ordenamiento de información, datos y tablas, desarrollo de la síntesis del manual, realización y entrega del quinto informe de avances.	
	3		
	4		
MES 5	1		
	2	Elaboración de presentación de los manuales, inclusión de resultados y conclusiones generadas en el proceso.	
	3		
	4		
MES 6	1		
	2	Realización y entrega del informe final de la práctica, entrega de manuales de mantenimiento, software libre y sistemas operativos seguros.	

Fuente. Autor

2. MARCO TEÓRICO

2.1 VIRTUALIZACIÓN VMWARE INFRASTRUCTURE

La mayoría de computadores hoy en día son diseñados para soportar un único sistema operativo y esto en la mayoría de veces conlleva a la subutilización de recursos hardware con que cuenta una organización, también, estos computadores están diseñados para soportar múltiples aplicaciones ejecutándose al mismo tiempo pero esto puede traer resultados inesperados ya que si se están ejecutando varias aplicaciones en un equipo y una de estas llega a fallar puede afectar al resto de aplicaciones produciendo tiempos de respuesta a procesos demasiado altos, bloqueos del sistema u otros resultados no deseables.

La subutilización de recursos también trae consigo el problema de la complejidad en la gestión y mantenimiento de la infraestructura tecnológica y de telecomunicaciones que se va a hacer cada vez más grande y difícil de manejar cada vez que la empresa va creciendo y se va a hacer necesidad de espacios adicionales para la infraestructura y nuevos equipos.

En una empresa que necesite una gran infraestructura para el procesamiento de datos como lo es el caso de la empresa de prestación de servicios tecnológicos y de cajeros automáticos ATH, este problema se vuelve de vital importancia, ya que esta subutilización de recursos se refleja en grandes pérdidas económicas y por esto se hace necesario encontrar e implementar opciones que mejoren la utilización de los recursos de la empresa minimizando costos y maximizando la capacidad de producción de los recursos empresariales.

Para este problema se implementa en la empresa la virtualización de servidores, que es una solución de inmensa utilidad y eficiencia, y aporta en muchos aspectos para el mejoramiento de los procesos empresariales.

2.1.1 Concepto de virtualización de servidores

La virtualización es un concepto muy utilizado en la actualidad y se refiere a la abstracción de recursos hardware con el objetivo de hacer posible la división de un recurso físico de gran capacidad en varios recursos lógicos de menor capacidad variable según las necesidades de procesamiento y funcionalidad hardware requeridas, para su posterior utilización en diferentes proyectos en el mismo tiempo. La virtualización forma una capa que divide los recursos físicos de forma que cada una

de los recursos lógicos funcionen de manera independiente y estén reservados para lo que va a ser su función, por ejemplo , es posible dividir recursos de almacenamiento, de procesamiento, memoria, dispositivos, etc.

El concepto de la virtualización empezó en la década de 1960 con los mainframes, los cuales eran computadores de gran capacidad y adaptables, diseñados especialmente para poder dividirlos lógicamente y así poder utilizarlos en diferentes proyectos, y esta ha tomado una vital importancia debido a que las tecnologías a través del tiempo han demostrado un inmenso desarrollo y cada vez es más fácil y resulta más económico adquirir equipos con una muy alta capacidad lo que en ocasiones conlleva a un desaprovechamiento de estos recursos que se podrían utilizar de una mejor manera.

El tipo de virtualización más utilizado actualmente es el de virtualización de servidores o maquinas virtuales, que se trata de dividir una maquina que cuenta con grandes recursos de computación incluyendo todos los recursos necesarios en un computador como CPU, memoria, discos, etc., y dividiéndola en varios recursos independientes según la función que vaya a desempeñar cada uno de estos en la organización.

Las arquitecturas de computadores predominantes hoy en día son las arquitecturas que utilizan tecnologías x86 y x64, ya que la gran mayoría de computadores en la actualidad manejan alguna de estas dos tecnologías, por esto, varias firmas de productos software se han dedicado a desarrollar aplicativos para la virtualización de este tipo de servidores entre las cuales las más conocidas son:

- VMware
- Sun Microsystems
- Microsoft
- Oracle

2.1.2 Propiedades de los Servidores Virtuales con VMware

- ✓ Compatibilidad.

  Los servidores virtuales VMware son compatibles con los dos sistemas operativos actualmente más utilizados Windows y Linux así como los controladores de hardware y aplicaciones creados para estos sistemas operativos. Estas también soportan todo tipo de aplicaciones creadas para sistemas operativos como Solaris y Netware. En este sentido una maquina lógica es idéntica a una maquina física y no se tendrá ningún problema al

instalar cualquier aplicación que también sea instalable en la máquina física sin necesidad de realizar ningún ajuste para esto.

- ✓ Aislamiento.

  Un servidor virtual VMware está aislado de los otros servidores virtuales al igual que si se estuviera trabajando con servidores físicos distintos .Las aplicaciones en cada servidor virtual utilizan únicamente los recursos asignados para cada servidor, y estos servidores tanto como las aplicaciones no saben ni siquiera que están trabajando sobre una máquina lógica sino que trabajan de la misma forma como si estuvieran en una máquina física con los mismos recursos que se le ha asignado al servidor virtual. Por ejemplo si hay 3 servidores virtuales dentro de una máquina física y alguno de los servidores presenta una falla, los otros dos servidores seguirán trabajando normalmente y seguirán trabajando de forma autónoma sin que esto les perjudique en su funcionamiento y estarán aislados de problemas de estabilidad y rendimiento de las aplicaciones en los otros servidores.

2.1.3 Encapsulamiento y portabilidad de los servidores Virtuales VMware

Muchas de las opciones que pueden ofrecer los ambientes virtuales y lo hacen atractivo en comparación de los ambientes meramente físicos son posibles gracias a las propiedades de encapsulación y portabilidad que poseen las máquinas virtuales. Gracias a estas ventajas es posible la sencilla movilidad de sistemas virtuales completos entre diferentes servidores físicos ya sea por cualquier problema presentado en el hardware o por necesidad de mejoramiento del hardware utilizado. Estas migraciones de sistemas virtuales son totalmente independientes del hardware ya que dentro de la virtualización se encuentran todos los controladores de dispositivos y aplicaciones virtualizadas necesarios para el funcionamiento de las máquinas virtuales incluyendo controladores de video, interfaces NIC[3] y controladores de NIC virtuales haciendo que no se tenga que reconfigurar las redes ni ningún otro aspecto al mover una máquina virtual físicamente desde un servidor a otro proporcionando así la propiedad de independencia de hardware a las máquinas virtuales.

[3] Tarjeta de interfaz de red. Permite la interfaz física de comunicación entre los dispositivos y los medios de red. Se encarga generar las señales que representen los datos a transmitir por los medios de comunicación.

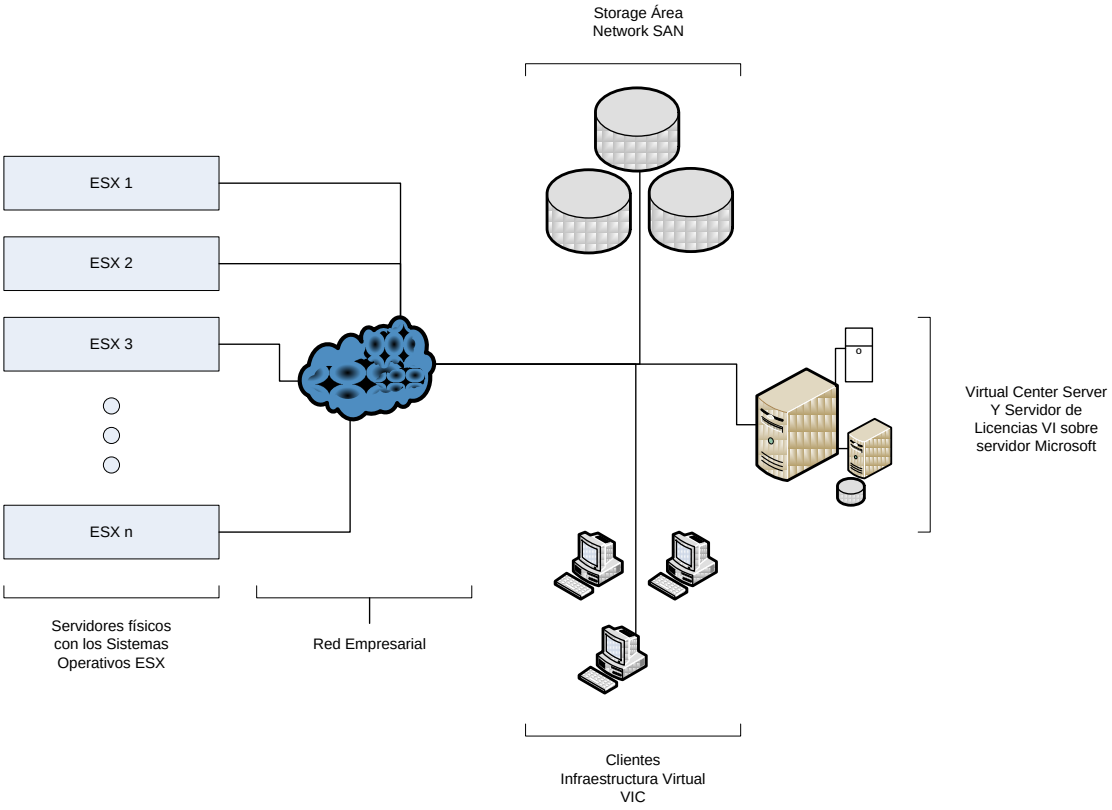
2.1.4 Descripción general VMware Infrastructure

VMware Infrastructure es un producto de virtualización de la firma VMware desarrollado para entornos empresariales la cual tiene como principal objetivo el aprovechamiento óptimo de los recursos hardware en la infraestructura de una organización. Este producto realiza la virtualización de la infraestructura de tecnologías de información empresarial de tal forma que esta infraestructura sea fácil de administrar, ocupe el menor espacio físico en la empresa posible, y cubra otras necesidades en el manejo de la información, garantizando su disponibilidad y su eficiente funcionamiento.

Este producto también cuenta con muchas otras ventajas como la centralización de la administración de la infraestructura de tecnologías de información y comunicación (TIC), el monitoreo centralizado de esta infraestructura, y cuenta además con otras herramientas para el manejo de la información empresarial como lo son la alta disponibilidad, la realización de backups y administración de actualizaciones, todo esto dependiendo del licenciamiento del producto que se haya adquirido por parte de la empresa. Con la implantación de VMware INFRASTRUCTURE y gracias a todas estas características que posee este software, se genera en la organización una infraestructura fácilmente manejable y eficiente con mayor capacidad de respuesta y a un menor costo que de la forma como se manejaba esta infraestructura anteriormente.

Este producto es un excelente ejemplo de la gran utilidad de la virtualización hoy en día y como se puede utilizar este concepto de virtualización aplicándolo en recursos de infraestructura empresariales con un alto grado de flexibilidad y adaptabilidad.

Figura 2. Representación de VMware Infrastructure



Fuente. Autor

2.1.5. Elementos que conforman la infraestructura virtual VMware VI en su versión Enterprise y su función

2.1.5.1 Sistema Operativo ESX Server

VMware ESX server es un sistema operativo servidor en modo texto que sirve como base para la implementación de la virtualización de la infraestructura tecnológica VMware Infrastructure, este sistema operativo es una capa de virtualización solida y ampliamente probada para entornos de producción como los que necesitan las grandes empresas que proporciona un servicio distribuido avanzado organizando los recursos de procesador, memoria, almacenamiento y red en varias máquinas virtuales que se almacenan dentro de un mismo servidor de amplia capacidad y pueden ser ejecutadas conjuntamente.

ESX es un sistema operativo basado en un núcleo Linux y modificado exclusivamente por la firma VMware con el fin de ofrecer la mayor fiabilidad para el uso de VMware Infrastructure, siendo tolerable a fallos y cumpliendo todos los requisitos que exige una

infraestructura de TIC[4] y comunicaciones de grandes, medianas y pequeñas empresas ofreciendo el máximo rendimiento, escalabilidad y solidez necesarios para estos entornos empresariales, además de que este SO ha sido probado bajo las necesidades de centros de datos de varias de las compañías más grandes del mundo.

2.1.5.2 Gestión de almacenamiento con Virtual Center

VMware Virtual Center es una capa de VMware Infraestructure encargada de la gestión del centro de datos, brindando la capacidad de centralización, automatización operativa, aprovechamiento de recursos y alta disponibilidad en la infraestructura que se va a organizar.

Virtual Center permite a los administradores de la infraestructura empresarial un ambiente muy completo para la gestión de esta con características de comodidad, fiabilidad, automatización, seguridad y control total de cada uno de los elementos que conforman la infraestructura virtual. Virtual Center permite:

- ✓ Organizar los recursos físicos disponibles en la empresa con prioridades de utilización predefinidas y agilizar los procesos que requieren de constante e intensiva utilización de recursos mediante la herramienta DRS incluida en el sistema operativo ESX. DRS asigna recursos inteligentemente según las configuraciones hechas por el administrador de la infraestructura VMware balanceando continuamente la asignación de recursos y asegurándose de que cada servidor virtual cuente con los recursos apropiados en cada punto de tiempo y además ayuda a prevenir que un servidor físico se sobrecargue de trabajo mientras que otros se encuentran subutilizados distribuyendo las tareas por igual entre nodos. La propiedad DRS da autonomía a la infraestructura virtual y permite incluir fácilmente cuando sea requerido más recursos representados en servidores físicos que pueden añadirse a un pool de recursos para que las máquinas virtuales dispongan de ellos y agregando así al sistema capacidad de procesamiento, almacenamiento, etc.

- ✓ Realizar una migración de maquinas virtuales sin ninguna clase de problemas entre servidores físicos dentro de la infraestructura virtual incluso si están encendidas (migración en caliente), así como un mantenimiento ininterrumpido mediante la herramienta VMotion incluida dentro de las características de VMware Infraestructure empresarial.

[4] Tecnologías de información y comunicaciones. Se refiere al conjunto de tecnologías software, hardware y de redes utilizados en los sistemas de información.

- ✓ Colaborar en el propósito de continuidad de negocio con ayuda de la herramienta de que dispone la infraestructura virtual VMware llamada VMware HA, que se trata de una herramienta que hace factible la continuidad de procesos dentro de la infraestructura virtual en caso de alguna falla de hardware dentro de un servidor físico o alguna falla de un sistema operativo en una máquina. Esta herramienta reacciona a alguna falla presentada en el hardware asignando otros recursos que se encuentren disponibles dentro de la infraestructura virtual y permitiendo la continuidad de los procesos casi que inmediatamente. Si la falla es de sistema operativo VMware HA reiniciara las máquinas virtuales y procederá a hacer migración de estas a otros servidores físicos en caso de ser necesario gracias a que su sistema de archivos VMFS lo permite.

Funcionalidades de Virtual Center:

- ✓ Hace gestión de las máquinas virtuales.

- ✓ Hace monitoreo constante de la disponibilidad de los sistemas y su rendimiento.

- ✓ Realiza notificaciones automáticas y alertas de correo según la configuración del administrador de la infraestructura virtual.

- ✓ Se encarga de la seguridad en el entorno mediante un control de acceso.

2.1.5.3 Servicios de sistema de archivos y multiprocesamiento simétrico

VMware Infrastructure es posible gracias a los servicios con que cuenta los cuales fueron desarrollados exclusivamente con el fin de que soporten los entornos de producción a los cuales están destinados, es decir, entornos de producción empresariales. Ejemplos de estos servicios son VMFS (Virtual Machine File System) y VSMP (Virtual Symmetric MultiProcessing).

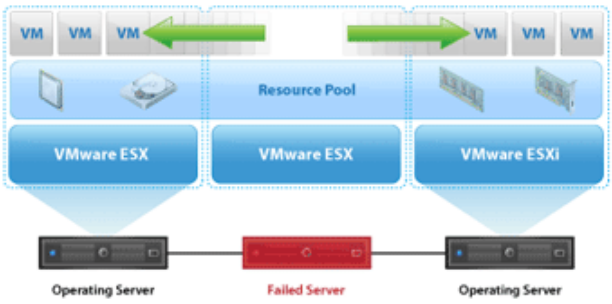
VMFS es un sistema de archivos propio de VMware diseñado para los equipos destinados a ser servidores ESX dentro de la infraestructura virtual VMware. Este sistema de archivos proporciona muchas ventajas sobre la infraestructura virtual alto rendimiento y es necesario para poder utilizar las herramientas de Vmotion, DRS y HA que ofrece la virtualización de infraestructura VMware.

VSMP brinda el servicio de poner varios procesadores al servicio de una máquina virtual. El multiprocesamiento simétrico se trata de mapear procesadores físicos o lógicos a una máquina virtual haciendo posible la asignación de múltiples procesadores a una sola máquina virtual y con el fin de que varias aplicaciones que compartan memoria y trabajen sobre el mismo sistema operativo puedan también compartir capacidad de procesamiento siendo ejecutados en dos o más procesadores. Para que el multiprocesamiento simétrico pueda ser posible es necesario como ya se dijo que las aplicaciones trabajen sobre el mismo sistema operativo ya que al ser de esta forma se carga únicamente una copia del sistema operativo para todos los procesadores y con este único SO cargado se pueden ejecutar los múltiples procesos en los múltiples procesadores.

2.1.5.4 Servicio de alta Disponibilidad (HA)

VMware HA (High Availability) es uno de los servicios más importantes de la infraestructura virtual ya que proporciona ventajas para la continuidad del negocio en caso de presentarse una falla a nivel de hardware o sistema operativo. En caso de presentarse alguna falla en alguno de estos dos elementos el servicio de HA se encarga de analizar la falla presentada y actuando de acuerdo a este análisis de la manera más adecuada posible, por ejemplo, si la falla es de sistema operativo este servicio puede proceder a reiniciar las máquinas virtuales o incluso migrarlas a otro sistema operativo sin ninguna clase de intervención de alguien del personal administrador de la infraestructura, además de hacerlo con una respuesta rápida al problema ya que las máquinas virtuales y los SO ESX se encuentran en constante monitoreo en busca de algún fallo. Si la falla se presenta en el hardware de uno de los servidores físicos incluidos dentro de la infraestructura virtual HA lo detecta automáticamente y procede inmediatamente a hacer una migración de las máquinas virtuales a otro servidor que se encuentre funcionando correctamente ya que la infraestructura virtual se encarga de garantizar que en todo momento se cuente con los recursos necesarios para poder reiniciar todas las máquinas virtuales de un servidor físico que falle sobre recursos adicionales en el sistema.

Figura 3. VMware High Availability



Fuente. VMWare

2.1.5.5 Distribución de recursos En la infraestructura virtual

Con la herramienta DRS (Distribution resourses Schedule) de VMware se administra inteligentemente los recursos físicos a disposición de la infraestructura virtual y siguiendo las necesidades empresariales gracias a las características de su distribución y sus opciones de configuración. DRS se encarga de tomar recursos físicos y organizarlos en recursos lógicos de acuerdo a la configuración realizada por el administrador de la infraestructura virtual. Estos recursos lógicos son llamados pool de recursos y están disponibles de forma compartida a servicio de las máquinas virtuales que se incluyan dentro de este pool de recursos. Este sistema se encarga de balancear las cargas de procesamiento y memoria inteligentemente permitiendo el eficiente uso de los servidores virtuales y utilizando el hardware de la mejor manera que sea posible. El sistema también toma información del comportamiento de cada una de las máquinas virtuales analizando su utilización de recursos promedio para realizar cambios en la asignación de recursos que puedan mejorar la eficacia del sistema y garantizar el nivel de servicio requerido.

VMware DRS trae consigo la herramienta DPM (Distributed Power Managment) que se encarga de administrar la operación o no operación de los servidores reduciendo el consumo de energía innecesario de los servidores físicos que no se están utilizando dentro de la infraestructura virtual. La utilidad DPM realiza el apagado de los servidores físicos que no sean necesarios para cumplir con los requisitos de hardware por las aplicaciones en un determinado tiempo, y también se encarga de encender estos servidores a medida que las aplicaciones vayan necesitando de más recursos disponibles.

2.1.5.6 Migración de máquinas virtuales con la tecnología VMotion

VMotion es una tecnología clave que permite la migración de las máquinas virtuales de la infraestructura virtual desde un servidor físico a otro incluso realiza migración en caliente es decir con las máquinas virtuales en plena operación y además lo hace con una completa transparencia para el sistema. Esta posibilidad hace que la infraestructura sea flexible y que el aprovechamiento de recursos sea mucho mayor, permitiendo que si una máquina virtual se encuentra escaza de recursos pueda ser migrada a un servidor dentro del pool de recursos que cuente con estos recursos disponibles. Esta tecnología hace posible los servicios que ofrece la infraestructura virtual de VMware de alta disponibilidad (HA) y distribución de recursos (DRS).

Esta tecnología ofrece la posibilidad de su configuración para realizar acciones automáticamente así como cuando tiene configuradas las utilidades HA y DRS en los pools de recursos, o cuando se presente alguna clase de falla en el sistema virtualizado. También podemos utilizar la herramienta VI Client o Virtual Center para

con ayuda de VMotion poder realizar migraciones de máquinas virtuales de un servidor físico a otro con fines de realización de mantenimiento, cambios de servidores, cambios de tecnologías, etc.

Otra de las ventajas de la migración de máquinas virtuales con VMotion es que las migraciones se pueden realizar incluso con los sistemas operativos y cualquier cantidad de aplicaciones que se encuentren funcionando en este ya que la máquina virtual no sufrirá ningún tipo de problema y seguirá trabajando como si no se moviera del servidor donde se encuentra.

2.1.5.7 Actualización de ESXs y máquinas virtuales con Update manager

La infraestructura virtual cuenta con la herramienta para actualizaciones automáticas Update Manager que actualiza tanto sistemas operativos ESX como de algunas maquinas virtuales Microsoft y RHEL (Red Hat Enterprise Linux). Esta herramienta escanea los ESX y las máquinas virtuales e instala parches a los sistemas Operativos después de realizar un snapshot (copia del estado del sistema) con el fin de que si se presenta un fallo después de la instalación de un parche puede devolverse el sistema al estado anterior. Otra propiedad de esta herramienta cuenta con la posibilidad de parchear las máquinas virtuales incluso cuando estas están paradas.

2.2 SOFTWARE LIBRE

2.2.1 Origen del concepto de libertad en el software

La libertad de software es un concepto que se fijo en los años 80 pero ya se practicaba desde los años 60 cuando el gran desarrollo de la informática se debió a que los programadores compartían sus avances para poder mejorar rápidamente los proyectos software. Durante los años setenta en laboratorios de inteligencia artificial en el Instituto de Tecnología de Massachusetts MIT existía una comunidad en donde no había ninguna restricción para compartir software, dentro de esta comunidad y en algún momento se hizo común el término software libre sin saberse quien fue el primero en utilizarlo ni en qué momento lo hizo, pero Richard Stallman que perteneció a este grupo fue quien años después en 1984 afianzaría este concepto e iniciaría el movimiento de software libre con el lanzamiento del manifiesto GNU.

2.2.2 Definición de Software libre

El término software libre fue definido por Richard Stallman y hace referencia a las libertades que debe otorgar un software que se quiera definir como libre.

- ✓ Libertad 0. Para ejecutar el programa para cualquier propósito.

- ✓ Libertad 1. Para estudiar el funcionamiento de los programas, cambiarlo y adaptarlo como se desee. El acceso al código fuente es una precondición para esto.

- ✓ Libertad 2. De redistribuir las copias, de modo que usted pueda colaborar con sus vecinos.

- ✓ Libertad 3. De distribuir copias que usted modifique a otros. Haciendo esto usted le da la oportunidad a la comunidad de beneficiarse de los cambios realizados por usted. El acceso al código fuente es una precondición para esto.

Un software se puede denominar libre si su licencia de distribución y uso no van en contra o imposibilitan alguna de las libertades descritas de alguna manera. En la actualidad existen varios tipos de licenciamientos de software que ofrecen la posibilidad de tener estas libertades aunque se diferencian en las restricciones que les hace el autor de la licencia sin violar las libertades básicas, por ejemplo, algunas licencias permiten la redistribución de software libre modificado pero con la condición de que la modificación incluya un nombre distinto del original en los binarios del código o acompañar los códigos fuente originales con parches que incluyan las modificaciones realizadas por cualquiera en vez de modifica directamente los códigos fuente originales.

Otro aspecto a tener en cuenta es que la palabra de origen inglés free utilizada en la definición en este idioma de software libe (free software) tiene dos posibles significados en el idioma español, el primero se refiere a la gratuidad de algo y el otro se refiere a la libertad de algo. Esto tiene como consecuencia que algunas veces quienes no conocen el concepto de software libre lo asocien con software gratis y aunque no es posible el obtener muchas ganancias con la distribución de software libre esto no es cierto, por ejemplo, alguien podría comercializar una copia que haya modificado el mismo de cualquier tipo de software libre pero quien lo compra tiene la posibilidad que otorga la tercera libertad del software de redistribuirlo a su antojo sin ningún tipo de restricción. Entonces en conclusión software libre (free software) se refiere a las libertades que tiene cualquier persona que adquiera un producto software con licencia libre, de usarlo, modificarlo y redistribuirlo a su antojo, y no a que el software se adquiera en cualquier ocasión de forma gratuita.

2.2.3 Otros términos referidos a las libertades legales de utilización del software

Existen varios conceptos que se refieren a los aspectos legales de utilización que el autor del software otorga a los usuarios, estos en ocasiones pueden confundirse si no se conoce exactamente cuál es su significado real.

- ✓ Open source

  El código abierto (Open source) Este es otro concepto que comparte la orientación del software libre de distribuir los códigos para poder mejorar eficazmente los productos pero es muy distinto en cuanto a la filosofía de esta ya que con este tipo de licenciamientos se podrían aprovechar algunos aspectos con el objetivo de hacer una comercialización de estos productos. La Filosofía del software de código abierto es diferente y va en contra a la ideología que propuso Richard Stallman de compartir el software junto con las libertades completas de uso, modificación y redistribución.

- ✓ Freeware

  Es software que se adquiere de forma gratuita y comúnmente es utilizado para promocionar otros programas o utilidades.

- ✓ Software de dominio público

  Se refiere a un software para el cual el autor cedió legalmente todos los derechos de utilización a cualquier persona que lo desee, sin ninguna condición adicional, lo cual tiene que quedar declarado explícitamente dentro de las estipulaciones del programa para que sea considerado de este tipo. Cualquier persona puede utilizar este software sin necesidad de ningún tipo de licenciamiento ni tampoco ninguna condición adicional ya que si se condiciona de alguna manera dejaría de ser software de dominio público.

- ✓ Copyleft

  El copyleft es un tipo de licenciamiento de software libre que obliga a que todos los productos derivados de este software como modificaciones y mejoras de este, sigan siendo software libre.

- ✓ Software propietario

  Es un software que se rige bajo las condiciones y restricciones que impone el autor en cuanto a utilización, modificación y redistribución del software. La mayoría de software con licencias de tipo propietario no da a conocer al público

su código fuente, prohíbe la modificación y la redistribución del software y solo habilita su uso en unos cuantos computadores.

2.2.4 Ventajas que puede ofrecer el software libre

El software libre trae consigo muchísimas ventajas tanto para el común de las personas como para las empresas que requieren software adaptable y a bajos costos o ningún costo en cuanto a la parte económica. Este software libre ofrece posibilidades por ejemplo a las empresas que requieren de algunas aplicaciones que puedan ser útiles y puedan ser implementadas con el fin mejorar los procesos de la empresa para hacer las labores de los trabajadores de la empresa más fáciles, o también ayudando a crear nuevos procesos con ayuda de estas herramientas software facilitando y haciendo posible el cumplimiento de los objetivos empresariales de una manera eficiente. Hay que tener en cuenta que el software libre no es viable y es una opción poco adecuada cuando los requerimientos de elaboración del software son muy altos, como lo son en las empresas que necesitan determinados software como sistemas operativos, herramientas de monitoreo u otras aplicaciones que cumplan con unos requisitos de seguridad y fiabilidad muy altos por el tipo de información que esta empresa maneja , de las empresas que necesitan de software altamente probado para ambientes de producción que requieren del funcionamiento continuo del software sin esperar ningún tipo de fallas ya que esto para estas empresas puede resultar en pérdidas económicas extremadamente, o de otras empresas que necesitan diferentes capacidades estrictas en el funcionamiento del software que optan por el software de tipo propietario que en determinadas circunstancias puede ofrecerles mucha más seguridad debido a la elaboración del software, soporte prestado por la firma desarrolladora o cualquier otra característica que tienen la mayoría de este tipo de software y así ajustarse más a sus necesidades. Por este motivo en muchas de las grandes empresas de la actualidad existe personal dedicado exclusivamente a la investigación de software para dar un asesoramiento a la empresa acerca de cuáles tipos de software se ajustan más a cada proceso y cuales herramientas más se podrían incluir para el mejoramiento de estos procesos de manera que la empresa tenga las mayores ventajas económicas y funcionales, ya sea con la utilización de software libre, propietario o cualquier otro tipo que se encuentre disponible.

2.2.5 Licencias más utilizadas en Software Libre

2.2.5.1 Licencias BSD

Las licencias BSD llamadas también licencias permisivas son aquellas que no imponen casi ninguna condición en la distribución y utilización del software, por lo tanto quien adquiere este software tiene la posibilidad de redistribuirlo con licencia privativa y utilizarlo para cualquier tipo de proyecto. Este tipo de software garantiza todas las libertades del software libre pero se despreocupa por hacer conservar estas

libertades a quienes modifican el programa y lo redistribuyen permitiendo el uso del código fuente en software privativo. Este tipo de licencias son también conocidas como licencias BSD debido a que se basan en la licencia usada por la Berkeley Software Distribution, un sistema operativo derivado de Unix que ha aportado grandes avances a los sistemas operativos y ha tenido varias derivaciones también que conservan este tipo de licencia.

Las licencias permisivas son tradicionalmente conocidas como de tipo BSD, ya que todas ellas están basadas en la licencia original escrita en la Universidad de California y que se usó en la Berkeley Software Distribution, una variante de Unix. Aunque no tanto como la GPL, las licencias permisivas son también muy populares y hay mucho software libre bajo ellas.

Este tipo de licenciamiento también es altamente utilizado habiendo varios software que se rigen por esta licencia o licencias con las mismas características y efectos, son ejemplo de ellas Apache, MIT (originalmente X11), OpenBSD, WinDump y otras.

- ✓ Ejemplo de licencia BSD:

Copyright (c) <year>, <copyright holder>
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions are met:
* * Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* * Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* * Neither the name of the <organization> nor the
* names of its contributors may be used to endorse or promote products
* derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS \AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2.2.5.2 Licencias GPL

Este es el tipo de licencia más utilizada en el software libre asegurando que el código fuente de este tipo de software no sea utilizado posteriormente en software privativo o software con otro tipo de licencias, es decir, asegura que el software y sus modificaciones siempre se encuentren bajo los parámetros de licenciamiento originales y siempre se garanticen todas las libertades del software. La licencia GPL se

encuentra dentro del rango de las licencias robustas o también llamadas licencias copyleft, las cuales garantizan de mejor manera las libertades del software haciendo conservar estas libertades a los que redistribuyen el software con modificaciones. El origen de esta licencia fue la licencia GPL creada durante el proyecto GNU en los inicios de la aparición del concepto de software libre.

La licencia GPL consta de una extensa serie de términos y condiciones que tienen que ser cumplida por quienes utilicen, modifiquen o redistribuyan este software y tiene algunos cambios en sus diferentes derivaciones y versiones (GPLv1, GPLv2, GPLv3, LGPLv3, LGPLv2.1, AGPLv3), que aumentan o disminuyen las posibilidades de manejo del software. También la documentación del software libre cuenta con una serie de reglas y restricciones que deben ser cumplidas por los que modifiquen estos software como las que exigen las licencias de documentación libres FDLv1.3, FDLv1.2, FDLv1.1.

2.3 MANTENIMIENTO A LA INFRAESTRUCTURA

2.3.1 Anatomía de un computador

Para poder entender donde posiblemente se están originando las fallas que presenta un computador primero se debe conocer cuáles son sus componentes y cuál es la utilidad de cada uno de estos, así se puede saber que está funcionando mal y de cuáles son las posibles soluciones a la falla, ya sea a nivel físico o de aplicación.

2.3.1.1 Hardware

Para resolver problemas de hardware adecuadamente en necesario primero que todo comprender como está conformado un computador físicamente y los elementos básicos que conforman y posibilitan el funcionamiento de los computadores, estos son:

- ✓ Placa base

  Es la placa de mayor tamaño en un computador. Es una tarjeta de circuito impreso que soporta todos los elementos que posibilitan el funcionamiento de la máquina. Esta placa incluye el chipset del microprocesador, la memoria caché, la BIOS, tiene incluidos los slots para la memoria RAM, ranuras de expansión como las PCI, SIMM, DIMM, ISA y AGP, la controladora IDE y la IO, algunas conexiones como la de la disquetera, el conector eléctrico, interface del teclado, mouse, USB, etc. Ya que la placa base es la principal parte del computador se debe tener en cuenta que tipos de estas placas son las que necesita la organización dependiendo de para que se quieren utilizar y los recursos con que se dispone, porque ya es sabido que con el rápido cambio de tecnología aparecen nuevas

placas con diferentes tipos de slots, ranuras, chipsets, componentes integrados, etc., que soportan diferentes tipos de tecnologías cada vez más avanzadas, por ejemplo memoria de alta velocidad, procesadores de varios núcleos y demás componentes que necesitan contar con placas que soporten su tecnología y velocidad de funcionamiento para así hacer un uso óptimo de los recursos que se tienen.

- ✓ Microprocesador

Es donde se llevan a cabo todas las operaciones que requieren el sistema operativo y todas las demás aplicaciones que tiene el computador. Está compuesto por la unidad aritmético-lógica encargada de operaciones de suma, resta, multiplicación y división (aritméticas) y operaciones como if, and, xor (lógicas), la unidad de control que se encarga de administrar todos los elementos para que todos los procesos en micro código, como movimiento de registros, se lleven a cabo de manera correcta asegurando que su funcionamiento sea adecuado y ordenado, el bus interno que es el puente de comunicación entre los elementos y los registros donde se guardan las instrucciones que posteriormente pueden pasar al procesador.

- ✓ Memoria RAM

Es un elemento fundamental en el computador. En la memoria RAM se guardan las instrucciones que los programas necesitan ejecutar y donde se guardan resultados de operaciones que se han requerido. Entre más grande es la capacidad de la memoria y mayor es su velocidad de transferencia, esta puede almacenar mas registros de ejecución y los programas operarán más rápidamente. La tecnología de las memorias RAM ha ido mejorando en el tiempo y actualmente las memorias más utilizadas son las memorias DDR2 y DDR3 (módulos DIMM de 240 contactos). Estas memorias se componen de circuitos integrados soldados sobre un circuito impreso.

- ✓ Tarjeta gráfica

Funciona como intérprete de datos provenientes del procesador para convertirlos en datos que comprensibles y representables por un dispositivo de salida de video. Algunas de estas tarjetas de video tienen funcionalidades añadidas como sintonización de televisión, reconocimiento de lápiz óptico, captura de video y otras.

- ✓ Puertos IDE, SATA y SCSI

Controla los dispositivos según su interfaz de transferencia de datos.

Las interfaces IDE también conocidos como puertos ATA se encargan de la transferencia de datos en dispositivos de almacenamiento, o dispositivos de lectura y escritura de datos CD/DVD. Algunas placas base tienen disponibles puertos de este tipo para conectar dispositivos.

Las interfaces SATA son una mejora de la tecnología de los puertos ATA y cuentan con ventajas sobre estos en velocidades y aprovechamiento de espacio cuando hay varios discos, también tienen una mayor amplitud posible en el cable de transmisión de datos. Esta clase de puertos son los más aceptados y utilizados actualmente por su buen desempeño y económica adquisición. La mayoría de placas base en la actualidad cuentan con estos puertos para conexión dispositivos de almacenamiento y algunos otros.

Las interfaces SCSI conocidos también en el lenguaje español como escosi se encargan también de la transferencia de datos entre dispositivos, superando en velocidad a las interfaces IDE y SATA. Estas interfaces son adecuadas en empresas con computadores de alto rendimiento como lo es el caso de ATH donde la mayoría de servidores las utilizan debido a su excelente desempeño aunque sea menos económica que las otras opciones.

- ✓ Otros puertos

Los puertos son interfaces que sirven para la transferencia de datos. Dicha interfaz puede ser física, o puede ser por software (virtual). Algunos son:

- Puertos Serie y Paralelo: Los puertos serie son utilizados usualmente para dispositivos mouse, módem, impresoras, joysticks y otros. Su nombre se debe a la forma como se hace la transferencia de datos desde los dispositivos de este tipo la cual es en forma de fila (en serie) uno detrás de otro. Los puertos en paralelo son utilizados para la conexión de dispositivos como impresoras, escáneres, unidades de almacenamiento externas, tarjetas de sonido, cámaras web y otros. La transferencia de datos en este tipo de dispositivos se hace por diferentes canales a la vez y de ahí su nombre (paralelo).

- Puertos PCI (Peripheral Component Interconnect): Son interfaces especialmente diseñadas para conexión de dispositivos tarjetas de

sonido, vídeo, red, inalámbricas, controladoras RAID, etc. Casi todas las placas base en la actualidad cuentan con varios de estos slots PCI para conexión de cualquiera de los dispositivos que se requiera agregar a la placa, por este medio de conexión a través de inserción de tarjetas.

- Puerto USB: Es uno de los puertos más útiles en la actualidad ya que permite la conexión de casi todos los tipos de dispositivos como discos de almacenamiento de diferentes capacidades, cámaras digitales, celulares, teclados, mouse, tarjetas de red, etc., externamente de una forma muy fácil y cómoda, y totalmente plug and play. Todos los computadores en la actualidad traen consigo varios puertos de este tipo gracias a su popularidad.

En varios casos es utilizada en la empresa la herramienta EVEREST, la cual puede realizar un extenso y detallado análisis del sistema, mostrando prácticamente todos los aspectos referentes a hardware, sistema Operativo, software y configuración de red (mayor énfasis en hardware) de los computadores. Es una excelente opción cuando se necesita revisar los componentes de un computador sin desarmarlo.

2.3.1.2 Software

Software se refiere a los componentes lógicos digitales en forma de bits que se instalan sobre la parte física de un computador (hardware), y utilizan estos elementos físicos para cumplir determinadas funciones específicas para las cuales fue creado. En otras palabras el software son comandos desarrollados en cualquier tipo de lenguaje que interactúan con el hardware y se apoya en este para cumplir con funciones específicas. Dependiendo su función el software se puede clasificar en varios grupos básicos:

- ✓ Software de sistema

Tiene el objetivo de facilitar la comunicación entre el usuario y la máquina e independizar al usuario de los procesos básicos e internos del computador para la ejecución de programas y este en cambio solo se preocupe por la inclusión de datos para la ejecución de tareas y posterior revisión de resultados, haciendo que la interfaz de de manejo del sistema se haga de una forma sencilla y se aprenda rápidamente, y el computador con todos sus elementos y dispositivos discos funcionen de manera transparente para el interesado en realizar cualquier tarea a través de la máquina. También es software de sistema el que se utiliza para realizar monitoreo del funcionamiento del computador, el software de realización de mantenimiento del computador.

- Sistemas operativos
- Controladores
- Software de monitoreo del sistema
- Software de mantenimiento del sistema

✓ Software de programación

Son herramientas que utiliza el programador en el proceso de desarrollo de cualquier tipo de software.

- Editores de texto
- Compiladores
- Intérpretes de lenguajes
- Depuradores
- Entornos IDE

✓ Software de aplicación

Tienen el objetivo de prestar un servicio al usuario para realización de alguna tarea o actividad.

- Aplicaciones ofimáticas.
- Software empresarial (Contabilidad, Auditoria, inventario, …)
- Software de telecomunicaciones (protocolos, administrador de routers, …)
- Software de entretenimiento (juegos, aplicaciones sociales, …)
- Software especializados (software de Diseño asistido, software de cálculo numérico, Software de astronomía, software de medicina)
- Software de seguridad (Antivirus, sniffers, firewalls, herramientas para encriptar datos, analizadores de logs, …)

El software también se puede describir basándose en su método de distribución. Entre estos se encuentran el software propietario, software libre, software open source, software de dominio público y otros.

2.3.2 La BIOS, el CMOS y el SetUp

Todas las placas base incluyen un chip BIOS de memoria ROM propio de estas que es cargado automáticamente al activar el botón de inicio del equipo, y es el encargado de realizar tareas como revisión de recursos hardware, reconocimiento y pruebas de dispositivos conectados, carga del Sistema Operativo instalado en memoria RAM y otros. En la BIOS también son configurables varias opciones del sistema como video, orden de arranque de discos (booteo), aspectos de la seguridad del sistema y otros, con el fin de que el administrador del equipo pueda controlar estos aspectos del funcionamiento del computador.

En las placas también se encuentra la CMOS (Complementary Metal Oxide Semiconductor) que es una memoria de bajo consumo de energía utilizada para guardar algunos valores del estado del sistema como discos duros del sistema, fecha y hora del sistema, y mantenerlos almacenados mientras el equipo se encuentra apagado. Esta memoria requiere de un bajo pero constante consumo energético y por este motivo se alimenta de la energía de una pila adaptada especialmente para este fin en la placa base.

La interfaz gráfica que permite la visualización y configuración de los parámetros de la BIOS y la CMOS se denomina SetUp. Esta interfaz es accesible de formas diferentes dependiendo de la placa base que tenga el computador, pero las formas más comunes de acceso al SetUp son presionando la tecla F1, DEL o Supr al encender el computador.

Algunos aspectos configurables con el SetUp son:

- Tarjetas gráficas y de sonido (habilitar o deshabilitar)
- Discos duros, dispositivos Plug & Play, periféricos, unidades ópticas y flexibles.
- Tamaño de la memoria.
- Secuencia de arranque del sistema.
- Configuración puertos PCI

- Seguridad y estado del sistema.
- Administración de energía.

2.3.3 Herramientas del Sistema Operativo Windows

2.3.3.1 La MMC (Microsoft Management Console)

La MMC es un proceso del sistema en Windows que permite ejecutar las herramientas de administración con que cuentan los sistemas operativos Windows desde su versión NT (NT/2000/XP/VISTA). El sistema trae por defecto en su instalación varias consolas de administración de servicios almacenadas cada una con diferentes opciones de utilidades de administración del Sistema en archivos con extensión *.msc a las cuales se puede acceder mediante la opción ejecutar en el inicio del sistema. Algunos ejemplos útiles para la realización de mantenimiento con estas consolas de servicios son:

- **devmgmt.msc** administrador de dispositivos
- **services.msc** servicios del sistema
- **gpedit.msc** editor de políticas de grupo (solo en XP Professional)
- **perfmon.msc** Monitor del rendimiento del sistema
- **eventvwr.msc** Visor de Sucesos
- **dfrg.msc** Desfragmentar disco duro

2.3.3.2 Otras herramientas del sistema

También es posible acceder mediante comandos y a través de ejecutar en el inicio de Windows a las opciones del panel de control de Windows los cuales son archivos del tipo *.cpl, algunos ejemplos son:

- **nusrmgr.cpl** Administración de cuentas de usuario
- **odbccp32.cpl** Administrador de base de datos ODBC
- **ncpa.cpl** Conexiones de Red

Los sistemas Windows también cuentan con otras utilidades para realización de tareas, actividades o algunas de configuración del sistema que son accesibles por medio de comandos en el menú ejecutar de inicio del sistema y son archivos

ejecutables del tipo *.exe. Algunas de estas pueden ser de mucha utilidad en algunos casos, como por ejemplo:

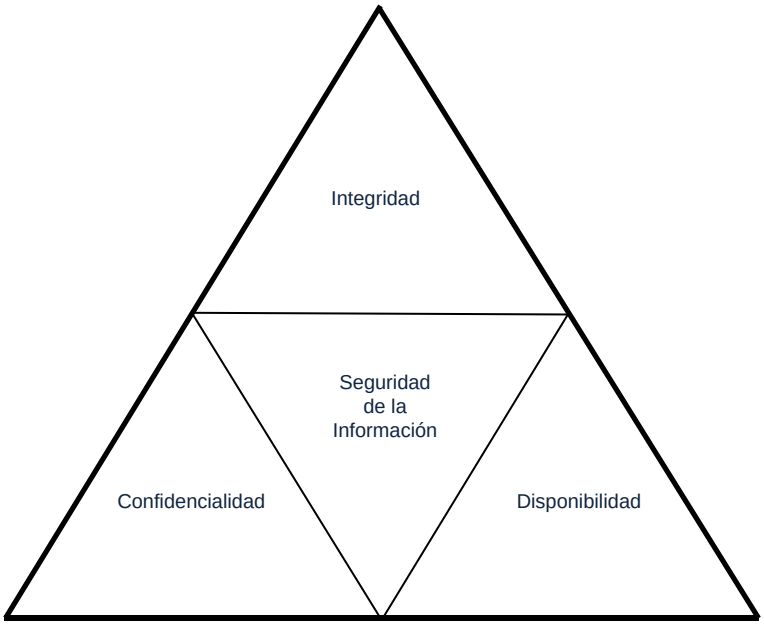
- **chkdsk** utilidad de chequeo del disco(s)
- **diskpart** Administración de particiones del disco
- **regedit** Editor de registro de Windows
- **msconfig** Utilidad de configuración del sistema
- **msinfo32** Información del Sistema
- **cleanmgr** Limpiar espacio en disco
- **bootcfg** Modificar archivo boot.ini

2.4 SEGURIDAD INFORMÁTICA

2.4.1 Definición de Seguridad Informática

Se puede definir seguridad informática como la implementación de acciones necesarias para lograr proteger la información digital contenida en un sistema o una red informática de ataques por personas no autorizadas o eventos desafortunados que puedan afectar la confidencialidad, integridad o disponibilidad de esta información en cualquier forma. La norma ISO/IEC 17799 con titulo de código de buenas prácticas para la gestión de la seguridad de la información define la seguridad de la información como la preservación de estos tres aspectos que son comúnmente conocidos por sus acrónimos en el idioma inglés “CIA” de las palabras Confidentiality, Integrity, Availability.

Figura 4. Seguridad de la información según la norma ISO 17799



Fuente. Enciclopedia de la seguridad Informática[5]

La seguridad de la información como disciplina se enfoca en el desarrollo de herramientas, políticas y procedimientos que se acoplen a un sistema existente para proteger un sistema de ataques o eventos no planeados que puedan afectarlo. El estudio de la seguridad informática requiere de amplios conocimientos en muchos aspectos, empezando por la criptografía y otras herramientas para la protección de los datos, pasando por el correcto manejo y uso del hardware, métodos organizacionales y de auditoría, y la legislación vigente.

La mayoría de sistemas de seguridad de las grandes empresas exigen el cumplimiento de requerimientos críticos que deben cumplirse estrictamente y de manera confiable para que estos se puedan usar e implementar, ya que si no lo son, su falla pueda tener graves consecuencias como por ejemplo la pérdida de vidas humanas (sistemas de control de seguridad nuclear o armas químicas), poner en peligro grandes ecosistemas (controles en la extracción de crudo marítimo), ocasionar graves pérdidas a infraestructuras financieras (cajeros automáticos y sistemas en bancos), afectar la viabilidad de sectores comerciales (sistemas de encriptación de la televisión pagada), o facilitar actos ilícitos (registros notariales o judiciales).

Los requisitos de seguridad cambian notablemente de un sistema a otro. Algunas de las necesidades típicas en la mayoría de sistemas son autenticación de usuarios, integridad en el registro de transacciones o contabilizaciones y confidencialidad de

[5] **Gómez V, A**, Enciclopedia de la Seguridad Informática. Primera Edición. Alfaomega Grupo Editor, S.A. de C.V., México. 2007

datos, pero hay que tener cuidado en evaluar muy bien todos los aspectos que deben protegerse en un determinado sistema ya que si se desprotegen aspectos importantes, o se protegen pero de forma inadecuada el sistema será vulnerable a ataques y fallas.

2.4.2 Ejemplo de implementación e importancia de la seguridad informática en entidades Bancarias y de cajeros automáticos

El centro del funcionamiento de una entidad bancaria o de servicios de cajeros automáticos es normalmente un sistema de almacenamiento de información donde se guardan los archivos de identificación de cuentas, clientes, y archivos de registro de transacciones diarias. La amenaza principal de este sistema es el propio personal del banco ya que estos pueden tener más fácil acceso a información vital en los procesos de seguridad de esta información. La principal defensa ante estas situaciones son las políticas y procedimientos empresariales para el almacenamiento y protección de la información que han evolucionado en muchos aspectos durante siglos, por ejemplo, técnicas y herramientas contables que aseguren el claro registro de operaciones donde cada débito contra una cuenta debe ser emparejado por otro igual y opuesto crédito contra otra cuenta y solo permitan acceso de lectura y escritura a personal autorizado, controles en transacciones de altos montos de dinero donde se necesita del visto bueno y la autorización de altos mandos, sistemas de monitoreo que buscan realización transacciones inusuales o sospechosas de clientes para su evaluación y seguimiento, y también la administración de los permisos a los sistemas de información empresarial a usuarios que requiere periodos vacacionales, no trabaja más en la empresa o simplemente ya no necesita de determinados permisos para el ejercicio de sus labores.

La cara pública de los bancos son los cajeros automáticos. La autenticación de transacciones basadas en la tarjeta personal de un cliente y su número de identificación personal de tal manera que se pueda defenderse contra ataques tanto internos como externos es más difícil de lo que aparenta. Muy frecuentemente en este tipo de empresas se encuentran con los casos de “retiros fantasmas”, que se presentan cuando los delincuentes (o el personal de la entidad) han encontrado y explotado las vulnerabilidades del sistema. Los cajeros automáticos también son conocidos por ser los primeros que en gran escala utilizaron y comercializaron el uso de la criptografía, y también ayudaron a establecer estándares en este campo de la seguridad informática.

En los sistemas informáticos de estas empresas existe un alto número de mensajería de gran valor. Estos mensajes son utilizados para movilizar grandes sumas de dinero entre bancos y entidades localmente e internacionalmente, para comercio de servicios, para emisión de cartas de crédito y garantías y muchas otras operaciones. Para prevenir posibles ataques que puedan comprometer esta información usualmente se

utiliza una defensa, la cual es una mezcla entre procedimientos de administración segura de documentos, control de acceso y criptografía.

La mayoría de entidades de la rama bancaria también utilizan grandes cajas fuertes de seguridad, protegidas con sistemas digitales en las cuales las alarmas contra robo están en constante comunicación con los centros de control de seguridad. En estas la criptografía también es utilizada para prevenir que los delincuentes manipulen las comunicaciones de tal forma que inhabiliten las alarmas y aparente que "todo está bien" cuando estas son vulneradas.

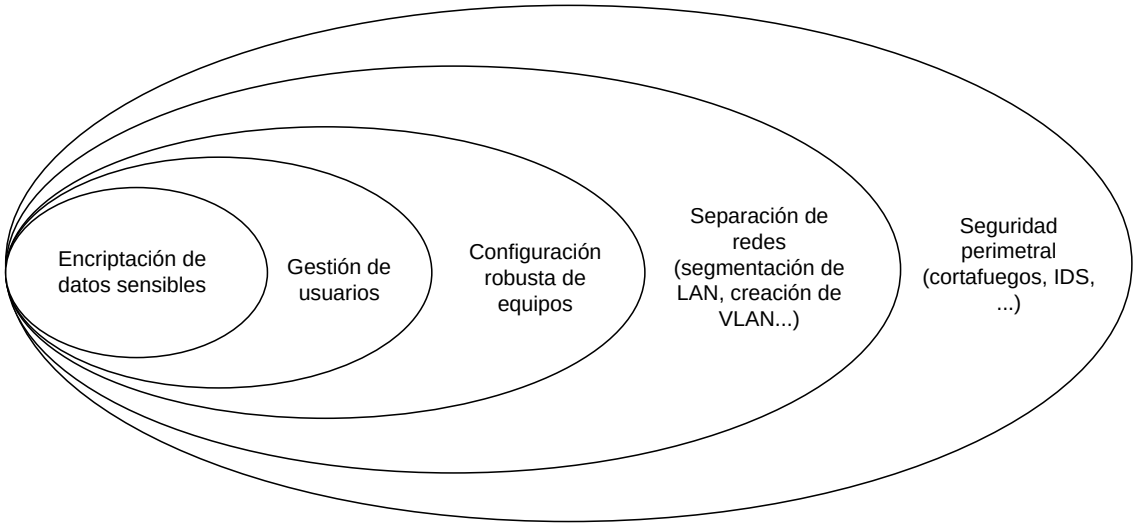
Sobre los últimos años, todas las entidades bancarias y similares han adquirido presencia en el internet, con sitios web y facilidades para los clientes de administrar sus cuentas en línea. Esto también permite a los usuarios con tarjetas debito o crédito usarlas para hacer compras en línea, y por este medio se adquiere el resultado de las transacciones comerciales. Para proteger este negocio, estas entidades usan las tecnologías estándar para la seguridad en la internet, incluyendo la encriptación SSL/TLS construida dentro de los navegadores web, y firewalls para prevenir a los hackers de los servidores web hacer túneles para acceder los sistemas principales de almacenamiento de documentos y manipularlos detrás de estos.

Más adelante se examinarán algunas aplicaciones para la seguridad en estos casos. La seguridad informática en los bancos es importante pos muchas razones. Hasta hace poco, los bancos eran los que principalmente dominaban el mercado de los productos de la seguridad informática, por esto es que tienen una desproporcionada influencia en los estándares de seguridad. Incluso cuando una tecnología no es manejada por estándares internacionales, puede de cualquier forma estar frecuente y fuertemente utilizada en varios sectores de la economía y el comercio.

2.4.3 Principio de defensa en profundidad aplicado a la seguridad de la información

Este principio es una forma de diseño de una estructura de seguridad por medio de capas dentro de la infraestructura tecnológica organizacional. Si una organización utiliza este tipo de estructura de seguridad de la información, esta va a contar con varios niveles de seguridad diferentes donde todos tendrían que ser vulnerados antes de que un atacante pueda acceder a la información. Este tipo de diseño retrasa el acceso a la información por parte de un atacante, dando tiempo de tomar las medidas necesarias para proteger la información. Es conveniente implementar dentro del diseño de defensa en profundidad, una primera línea de defensa con medidas de seguridad perimetral (vigilancia privada, firewalls, proxies, dispositivos de monitoreo, auditorías, etc.) que harían aún más difícil el acceso no autorizado a la información o la intrusión de una persona no autorizada que intente tomar control del sistema de información.

Figura 5. Representación del principio de defensa en profundidad aplicado a la seguridad de la información



Fuente. Enciclopedia de la seguridad Informática[6]

Mediante la aplicación de este principio se pueden controlar fácilmente intentos de intrusión de atacantes inexpertos que intenten penetrar el sistema, ya que si un atacante no tiene grandes conocimientos en métodos de intrusión de sistemas fácilmente se verá imposibilitado para penetrar el sistema después de las primeras capas de protección de la información, y se rehusara a seguir analizando y atacando el sistema.

Aunque la seguridad perimetral es muy importante no todo debe depender de ésta, y no se deben descuidar los diferentes métodos de protección del sistema y todas las posibles medidas de prevención que se puedan tomar para asegurar el sistema, tales como, configuración robusta de servidores, actualización de parches de seguridad en sistemas operativos y aplicaciones, desactivación de servicios innecesarios del sistema, cambio de contraseñas y cuentas de usuario por defecto de los equipos.

2.4.4 Objetivos de la seguridad informática y planos de actuación

Algunos de los objetivos principales que busca la seguridad de la información son:

- ✓ Minimizar de la mejor manera posible los riesgos que tiene la información, bloquear amenazas y gestionar para evitar problemas posibles.

[6] **Gómez V, A**, Enciclopedia de la Seguridad Informática. Primera Edición. Alfaomega Grupo Editor, S.A. de C.V., México. 2007.

- ✓ Velar por que los recursos de tecnologías de información de la empresa se utilicen por personas autorizadas de manera correcta y apegada a los objetivos empresariales.

- ✓ Tener planes de contingencia adecuados para poder actuar de manera correcta ante la presentación de cualquier evento desafortunado, y así poder continuar de manera rápida con las operaciones normales de la infraestructura tecnológica y disminuir las pérdidas lo más que sea posible.

- ✓ Adaptarse a la legislación vigente del territorio cumpliendo con todas las normas y estándares exigidos y protegiendo de la mejor manera la información y la infraestructura empresarial.

Para poder cumplir los objetivos descritos se debe gestionar en cuatro planos de actuación importantes:

- ✓ Plano Técnico: Tiene en cuenta el desarrollo y gestión de los métodos y técnicas de protección de los recursos tecnológicos y la información que esta contiene, y contempla tareas como:

    - o Selección de tecnologías adecuadas y su correcta implementación y seguimiento con el fin de evitar cualquier vulnerabilidad en el sistema.

    - o Análisis de métodos y herramientas que ayuden a proteger la información.

    - o Desarrollo o utilización de tecnologías de información estandarizadas cumpliendo con todas las normas y protocolos de seguridad.

- ✓ Plano Legal: Se preocupa por cumplir las normas legales vigentes en el territorio de su competencia para contar con todos los estándares de seguridad implantados por las autoridades competentes y buscando la protección de la información en todos los aspectos, contempla tareas como.

    - o Cumplimiento de controles de seguridad y calidad exigidos.

    - o Seguir al pie de la letra estándares y protocolos de seguridad exigidos.

- Establecer mecanismos exigidos con fines de mejoras en aspectos de seguridad de la información

✓ Plano humano: Se encarga de proteger los sistemas de información empresariales de posibles ataques por parte de los recursos humanos de la organización, y contempla tareas como:

- Capacitación de usuarios para el uso de la infraestructura tecnológica de su competencia.
- Elaboración de reglas y penalizaciones internas por acciones que afecten la seguridad de la información.
- Realización constante de auditorías.
- Control de accesos y permisos para la utilización de los sistemas.

✓ Plano Administrativo: Se enfoca en el análisis y la planeación de las autoridades en seguridad de la empresa que son las encargadas de evaluar el estado actual de seguridad de la información en la infraestructura tecnológica y de crear e implantar políticas y procedimientos adecuados que cumplan los objetivos de seguridad empresariales

- Realización de normas de utilización de la infraestructura tecnológica empresarial para los empleados.
- Creación e implantación de políticas y procedimientos.
- Realización de planes de contingencia y atención a riesgos.

2.4.5 Gestión de la seguridad de la información

Un sistema de gestión de la seguridad de la información (SGSI) es un proyecto realizado que comprende todas las medidas de un sistema general de gestión empresarial que tienen que ver con la seguridad informática, como lo son las políticas, procedimientos, estructuración y recursos necesarios para implementar los sistemas de seguridad de la información.

La guía ISO/IEC 27003:2010 es un documento guía que las empresas que requieran

tener sistemas estandarizados deben tomar como referencia para la implementación adecuada de un SGSI, de acuerdo a los parámetros de la norma internacional estándar para este tipo de sistemas que se describe en la ISO/IEC 27001.

2.4.6 Legislación informática en Colombia

2.4.6.1 Ley de la protección de la información y de los datos (Ley 1273)

Esta ley es la primera en su clase que se enfoca en la judicialización y penalización de las personas que afectan la seguridad de la información en varios aspectos. El contenido de esta ley se encuentra dentro del Anexo 1 del presente documento.

Podemos encontrar las diversas leyes, proyectos de ley e implementaciones realizadas en el código penal de Colombia y concernientes a la informática a través de la historia en la web de informática jurídica[7], de donde se tomo la anterior información.

- ✓ Asobancaria y ley 1273 de 2009

"Para la Asociación Bancaria y de Entidades Financieras (Asobancaria) es necesario que la legislación, la normatividad y las instituciones en general se adecuen rápidamente a los constantes cambios tecnológicos.

Los banqueros argumentan que la Ley 1273 de 2009, sobre delitos informáticos, constituye un gran avance en materia de seguridad informática, ya que mediante los nuevos tipos penales se facilitan las labores de judicialización y condena de los ciberdelincuentes.

Pero a la vez llama la atención porque todos estos avances se tornan insuficientes si los ciudadanos no asumen el compromiso de dar un manejo responsable y cuidadoso a la información y a los instrumentos utilizados para la realización de transacciones electrónicas.

Según el gremio, las entidades bancarias han venido realizando esfuerzos para mitigar los fraudes bancarios realizados por medios informáticos.

"Los bancos han desarrollado, constantemente, acciones de protección de los datos que manejan; definen protocolos y hacen verificaciones permanentes de la seguridad

[7] Información actualizada referente a la legislación jurídica para aspectos relacionados con la informática http://www.informatica-juridica.com/legislacion/colombia.asp

de sus sistemas de información; y realizan monitoreo sobre los links de su sitio web para que estos no sean modificados ni se suplanten sus certificados digitales", sostiene.

Y es que el riesgo de este tipo de fraudes no depende exclusivamente de la seguridad sobre sus propios sistemas, sino también de la vulnerabilidad que se presenta por prácticas inseguras de los clientes al realizar las transacciones."[8]

2.4.6.2 Leyes de Colombia no regulan el correo no deseado

"Aunque muchos países del mundo están combatiendo la proliferación de correos no deseados en Colombia no está muy claro que entidad debe regular o reglamentar esta actividad. Las leyes actuales no están preparadas para afrontar un fenómeno que afecta la economía, tiempo, rendimiento y vida diaria de miles de colombianos. A diario llegan a las cuentas de correo electrónico en todo el país una serie de mensajes con destinatario desconocido o de otros países donde se ofrecen todo tipo de productos, servicios e informaciones. Venta de pastelitos, cursos para convertirse en un escolta profesional, torneos de golf nacionales e internacionales, invitaciones a fiestas y jolgorios, difusión de eventos como congresos, charlas de superación personal y cuanta actividad existe en el mundo está llegando a las cuentas de correo, saturando la capacidad de estas soluciones y poniendo en riesgo la seguridad e información personal. Esta situación podría ser resultado de la actividad propia de las redes pero en términos económicos trae una afectación para el país que hasta el momento no ha sido cuantificada y que se produce por la utilización del ancho de banda y uso de la infraestructura del país. Por si fuera poco la revisión de este tipo de correo genera pérdida de tiempo y ocasiona el gasto de millones de pesos en aplicativos que ofrecen seguridad para no saturarse de Spam, como es conocido el correo no deseado.

Shirley Vera, gerente de canal oficial de Trend Micro en Colombia, una de las compañías multinacionales de seguridad informática más grandes del mundo, afirmo que se calcula que el correo electrónico no deseado en el país está por encima del 58 por ciento lo que ha significado un crecimiento de más del 80 por ciento comparado con el 2003. Hace cinco anos, se estimaba que el spam estaba cercano al 32 por ciento del tráfico total, hoy esa cifra es muy superior y la tendencia es que seguirá aumentando, afirmo la vocera de la compañía. Por su parte Symantec, otra de las compañías globales de seguridad, en el último informe sobre Spam da a conocer que de 10 correos enviados en el mundo ocho son Spam. Este es el comportamiento mundial y es un indicador de lo que está sucediendo en todas partes del mundo, hace un año estábamos en un 60 por ciento, afirmo a LA REPUBLICA, Daniel Eduardo Rojas Murcia, marketing manager para North Latin América de Symantec.

[8] Artículo tomado de: **Base de datos Proquest**. Universidad Industrial de Santander, UIS.

Precisamente esta delicada situación ha puesto en alerta a las autoridades de varios países donde ya están funcionando leyes concretas que combaten directamente a los spammers. En Estados Unidos esta actividad es considerada delito y penalizada con multas y cárcel según The Can Spam Act una ley federal que ya ha puesto tras la rejas a ciudadanos dedicados a esta actividad. En Latinoamérica en Perú hay una sanción administrativa y queda el interrogante acerca de que se está haciendo en Colombia desde el punto de vista de que la actividad viene creciendo.

No está muy claro en Colombia cual debe ser la entidad que se dedique a la regulación y control de esta actividad. No existe claramente una definición que obligue a alguna institución estatal a combatir o imponer multas ocasionadas por los perjuicios que ocasionen colombianos por el envió de esta información que utiliza la infraestructura del país.

Desde el punto de vista legal se podría pensar que la Superintendencia de Industria y Comercio tiene competencia en este tema, así mismo una de las entidades que podría regular esta actividad es la Comisión de Regulación de Telecomunicaciones pero hasta el momento no hay nada claro. Carlos Álvarez, vocero oficial en Colombia de la organización latinoamericana Alfa Redi que investiga, discute y formula propuestas de acción en temas de políticas y regulación de la Sociedad de la Información y experto abogado en este tema menciona que solamente hay una mención del tema de Spamming en las leyes colombianas. Para el experto el decreto reglamentario 1524 de la ley 769 de pornografía infantil es la única mención a nivel legal de esta actividad con el agravante de que solo define que es spamming y obliga a los prestadores de servicio a acceso a Internet la obligación de instalar en los servidores aplicaciones que eviten el trafico de Spam a través de sus redes. No se sanciona como tal a una spammer. Solamente impone obligaciones a los prestadores, afirmo.

En el país el tema tendría tres orbitas de análisis. La primera de ellas es el Habeas Data que es un derecho constitucional que le permite a cualquier ciudadano del territorio nacional exigir al administrador de cualquier base de datos cambiar o borrar toda la información personal que esté registrada. El habeas data aplica porque se crean bases de datos donde se recopila información que puede llegar hacer de carácter personal, señala el experto. El otro tema que está involucrado es el de las normas de protección al consumidor en lo que tiene que ver con publicidad engañosa ya que muchos de estos correos prometen, por ejemplo, mayor potencia sexual o evitar la caída del cabello y finalmente se ofrecen mercancías de mala calidad."[9]

[9] Artículo tomado de: **Base de datos Proquest**. Universidad Industrial de Santander, UIS.

2.4.7 Vulnerabilidades de los Sistemas Informáticos

2.4.7.1 Causas de las vulnerabilidades de los sistemas informáticos

A continuación se enumeran las causas más comunes de la presentación de vulnerabilidades informáticas:

- ✓ Débiles diseños de protocolos de redes

  La utilización de protocolos incorrectos en procesos críticos de seguridad es un grave problema ya que esto podría afectar los tres aspectos a proteger de la seguridad de la información. Un ejemplo es la utilización de protocolos utilizados en servicios de redes diseñados sin mecanismos de respuesta a situaciones anómalas que puedan provocar la caída del servicio de red y así este sería un ataque de denegación de servicios.

  Otro error de diseño es utilizar protocolos que no utilicen encriptación (traspaso de archivos en texto plano) para el envío de información sensible a través de una red de datos, ejemplos de estos protocolos son el de conexión remota básico (Telnet), el de transferencia de archivos (FTP) o el de correo electrónico en su versión más básica (SMTP).

- ✓ Errores de programación

  Otra gran cantidad de problemas de vulnerabilidades en los sistemas se encuentra en el desarrollo de software cuando se cometen errores de programación que pueden ser aprovechados para atacar un sistema informático.

  Estos errores son inevitables ya que el desarrollo de software lo hacen personas que como cualquier otra pueden cometer errores y desconocerlos al final del desarrollo de la aplicación. Para contrarrestar este problema se utilizan comúnmente parches de seguridad y actualizaciones que corrigen errores descubiertos, pero en ocasiones hasta estos mismos parches contienen otros errores que se pueden traducir en más vulnerabilidades, y por este motivo hay que constantemente estar actualizando el sistema e instalando todos los parches de seguridad que vayan apareciendo. Para el caso de los sistemas operativos de Microsoft es recomendable hacer instalaciones de estos en la versión de lenguaje inglés ya que los parches para estas versiones aparecen en primer lugar, antes que las versiones de otros idiomas.

También es recomendable conocer la rapidez con que una firma de software propietaria de cualquier herramienta la cual se esté pensando implementar en la empresa, responde a la detección de errores de programación en sus productos antes de aprobar la implementación del software. Examinando este aspecto se debe buscar la opción más atractiva entre las posibilidades de soluciones en el mercado útiles para las tareas que se necesiten, ya que una herramienta de software a la cual su firma representante no responda con rapidez a los errores detectados, es una herramienta que agrega vulnerabilidades al sistema de información empresarial representados en días de riesgo que duran mientras se corrigen los errores detectados en el software.

Otra causa frecuente de vulnerabilidad son los conocidos “Buffer overflow” o desbordamiento del búfer, que es una falla presentada en programación cuando se diseñan programas sin los controles necesarios para evitar que un usuario pueda introducir un valor en el buffer de mayor tamaño al que se ha reservado para este. El buffer es un espacio en memoria reservado para guardar datos que se utilizarán en alguna ejecución de algún programa para que no se presenten demoras de ejecución, son ejemplo de estos las aplicaciones que admiten la introducción de datos por parte del usuario donde se guardan datos que posteriormente utilizará el programa cuando este se ejecute. Algunas funciones como la strcpy del lenguaje C no tienen control sobre estos desbordamientos, y estos errores pueden ser aprovechados por personas malintencionadas con el fin de ejecutar un código arbitrario en una aplicación con suficientes derechos sobre el sistema, pudiendo así vulnerar la seguridad del sistema y tomar control de este evadiendo todas las medidas de seguridad implantadas.

El realizar este tipo de ataques es considerablemente complicado ya que requiere de tener exhaustivo conocimiento de la arquitectura del programa y del procesador del equipo donde se ejecuta el programa con la vulnerabilidad.

Para evitar este tipo de vulnerabilidad deberían existir controles de validación de datos que se almacenen en el buffer de memoria cuando se diseñen y desarrollen programas, garantizando que no se supere el valor reservado para los campos y evitado así los desbordamientos.

Los datos de un programa que se ejecuta son almacenados temporalmente en la pila de la memoria. Los datos ubicados después del búfer de memoria contienen una dirección de retorno denominado puntero de instrucción, que le permite al programa continuar su tiempo de ejecución. Si se presenta desbordamiento del búfer, la dirección de retorno se sobrescribe y el programa leerá una dirección de memoria que no corresponde a la continuación de ejecución del programa generando una violación de segmento en la aplicación.

Cualquier persona con suficientes conocimientos sobre esta vulnerabilidad y el sistema a atacar, puede asegurarse de que la dirección de memoria sobrescrita corresponda a una dirección existente en memoria, por ejemplo, una dirección que apunte dentro del mismo búfer de la vulnerabilidad, y así, las instrucciones que se ingresaron en este búfer pueden ser ejecutadas con los privilegios de la aplicación.

De esta forma, es posible que los sistemas sean atacados al incluir instrucciones en el búfer que por ejemplo puedan ejecutar un intérprete de comandos (shell), permitiendo así que el atacante no tome control sobre el sistema.

Hay que tener en cuenta que el lenguaje C, que es muy utilizado para el desarrollo de aplicaciones en Internet, no realiza validación de campos para prevenir que las variables introducidas en estos no superen la memoria reservada.

- ✓ Configuración inadecuada de los Sistemas de información

La mala configuración de los sistemas conlleva a la generación de vulnerabilidades que pueden ser fácilmente explotadas, como es el caso de dejar un sistema con su configuración por defecto (sin cambiar la configuración inicial después de la instalación), que permite que fácilmente un atacante pueda “adivinar” la configuración del sistema y aprovecharse de esto para vulnerarlo.

Algunas de las causas comunes de presentación de vulnerabilidades en los sistemas de información son las siguientes:

- No cambiar las cuentas de usuario por defecto en el sistema operativo instalado en los equipos.
- Ejecutar servicios innecesarios en el sistema o ejecutar servicios con permisos sobre el sistema que exceden los necesarios para su correcta función.
- No mantener al día la instalación de actualizaciones y parches del sistema o de las aplicaciones en este.
- Desactivación o inutilización por parte del usuario de opciones de seguridad del sistema.

- Configuración de routers con protocolos de enrutamiento poco seguros (como el RIP), que no garantizan la integridad de los mensajes de control con los cuales se intercambian información sobre rutas de envío de paquetes. Es aconsejable utilizar protocolos de enrutamiento más avanzados y seguros, como el OSPF o el BGP, que incorporan funciones de autenticación y control de la integridad de los mensajes.

- Contar con excesivas relaciones de confianza entre redes y servidores, que facilitan el acceso a servidores sin requerir de autenticación, como las de los servidores de confianza en sistemas Windows.

✓ Falta o deficiencia en las políticas de seguridad empresariales

Algunas de las deficiencias que se presentan en las políticas que deben ser implementadas en empresas con requerimientos de seguridad de la información para eliminar vulnerabilidades en los sistemas se listan a continuación:

- Configuración de contraseñas poco robustas y mala utilización de estas: contraseñas que no exigen requisitos mínimos de seguridad (longitud, caracteres requeridos, frecuencia de cambio,…), no concientización de los usuarios sobre el uso y protección de sus contraseñas de usuario (comunicar contraseñas, contraseñas grupales, anotación de contraseñas en lugares visibles al público,…), etc.

- Deficiente control de los intentos de acceso al sistema: No bloqueo de cuentas cuando se producen determinados fallos de autenticación; no registro de intentos fallidos reiterados de autenticación con una misma cuenta; falta de seguimiento y control (alarmas, monitoreo,…) del tiempo y horas habituales de conexión de una sesión de usuario para detectar situaciones anómalas, etc.

- Poco estricto control de acceso a los recursos: usuarios del sistema con permisos de acceso superiores a los necesarios para sus labores.

- Escaso control sobre los equipos portátiles o soportes informáticos: (memorias USB, discos duros, cintas de backup,…).

- Escaso control de impresiones con información sensible: ausencia de vigilancia o seguridad en impresoras o lugares que contengan documentación archivada.

- Falta de control sobre tareas realizados por personal ajeno a la empresa, como en el caso del personal outsourcing, personal de servicios,….

- Despreocupación por el adecuado almacenamiento de las copias de seguridad, o por los procedimientos implantados para su generación y revisión periódica.

- Deficiente o inexistente limitación del acceso físico a los equipos más sensibles, dispositivos de red y cableado: Centro de cómputo, cámaras, archivadores, etc.

- Instalación de programas poco fiables por parte de usuarios sin contar con la respectiva autorización de los responsables de la seguridad de la información en la empresa.

- Despreocupación por la instalación de actualizaciones y parches de software en servidores y otros equipos críticos.

- Poco control sobre el uso de herramientas antivirus en la infraestructura y la actualización de sus bases de datos.

- Desactivación o no activación de logs en servidores, dispositivos de red sin activar, o activados con información insuficiente.

- No control de herramientas y métodos para encriptar datos en el sistema.

- Transmisión de archivos sensibles y mensajes de correo sin encriptar ni autenticar, sobre todo a través de redes públicas o basadas en enlaces inalámbricos.

✓ Falta de concientización de los usuarios y personal responsable de la seguridad de la información mediante formación en la reglamentación y temas de seguridad.

Los errores de falta de concientización de los recursos humanos se describen a continuación:

- En ocasiones no se hace la capacitación correcta a los usuarios para mostrar la forma en que se puede colaborar y las reglas que se deben seguir para mejorar la seguridad de la información empresarial y así evitar las consecuencias laborales o legales que generan el incumplimiento de estas conductas.

- La capacitación debe mostrar al usuario cómo funcionan las herramientas y soluciones tecnológicas de seguridad implantadas en la empresa como antivirus, IDS, firewalls,…, y así se tome conciencia de su importancia y sea respetado por los usuarios, ya que se conoce que la mayoría de problemas de seguridad son provocados por personal dentro de la empresa.

- Esta labor en mayor parte es responsabilidad de la parte administrativa de la empresa, ya que estos son los que deben tener el compromiso de crear proyectos de formación y concientización de usuarios sobre el tema a través de personas especializadas.

✓ Existencia de "puertas traseras" en los sistemas informáticos

- Las puertas traseras o backdoors son vías de acceso por medio del código de un de cualquier software que permiten tener acceso y tomar control de este pasando por alto todos los mecanismos de seguridad para su acceso normal.

- Las puertas traseras pueden ser causadas por descuidos en el desarrollo del software al no eliminar servicios necesarios mientras se desarrollaba el software que son innecesarios el producto final, también pueden ser ocasionadas intencionalmente por el desarrollador del software para poder tener acceso a un sistema saltándose los mecanismos de seguridad o pueden ser creados con herramientas malware por personas malintencionadas que quieran vulnerar el sistema.

2.4.8 Códigos maliciosos

Un código malicioso o malware es un programa o parte de uno que está diseñado para quebrantar cualquiera de los aspectos de la seguridad de la información sin autorización de los encargados de este tema. Los códigos maliciosos pueden realizarse con diferentes motivos como lo son las bromas, intenciones de robo, destrucción o alteración de la información, utilización de recursos sin autorización, saturación de recursos, bloqueo de sistemas, etc.

La mayoría de estos malware se pueden propagar por si mismos o auto reproducirse y por este motivo pueden extenderse por las redes para sobrevivir e infectar sistemas de información completos si no se cuenta con las medidas de seguridad adecuadas que

permitan bloquear la intrusión y propagación del virus o al menos permitan tomar acciones necesarias para eliminarlo después de que ha invadido algún sistema.

Un malware informático puede ser desarrollado en cualquier lenguaje de programación ya sea Visual Basic, C, lenguajes de aplicaciones ofimáticas como los macros de office, Java o lenguaje ensamblador. Los malware más reconocidos y que se diferencian por su tipo de ataque, los recursos que utilizan o su intención son:

- ✓ Virus de sector de arranque. (Atacan archivos de arranque del sistema)
- ✓ Virus de archivos ejecutables. (Atacan archivos ejecutables)
- ✓ Caballos de Troya. (Vienen escondidos dentro de otro software y se ejecutan con este)
- ✓ Bombas de Tiempo. (Cuando infectan un equipo esperan a un determinado evento programado para ejecutarse)
- ✓ Gusanos. (se auto reproducen y transportan por redes)
- ✓ Ataques DoS. (Atacan la disponibilidad de recursos de un sistema).
- ✓ Spyware. (Realizan espionaje de información en los sistemas).
- ✓ Keylogers. (Capturas datos introducidos por teclado como contraseñas, cuentas, etc.).
- ✓ Botnets. (Realizan sistemas atacando de forma distribuida en redes).
- ✓ Rootkits. (se ocultan y oculta información de procesos, archivos y otros que estén afectando a los equipos para que no sean descubiertos fácilmente).
- ✓ Jokes. (Hacen bromas no autorizadas a los usuarios del equipo infectado).

Algunos de los virus tienen la propiedad de auto ejecutarse al inicio del sistema operativo mediante la creación de un registro en el sistema, para verificar en caso de sospecha de un virus que infecte un sistema operativo Windows y se ejecute al iniciar se deben revisar el registro de Windows mediante el comando regedit en inicio>>ejecutar y en las siguientes extensiones.

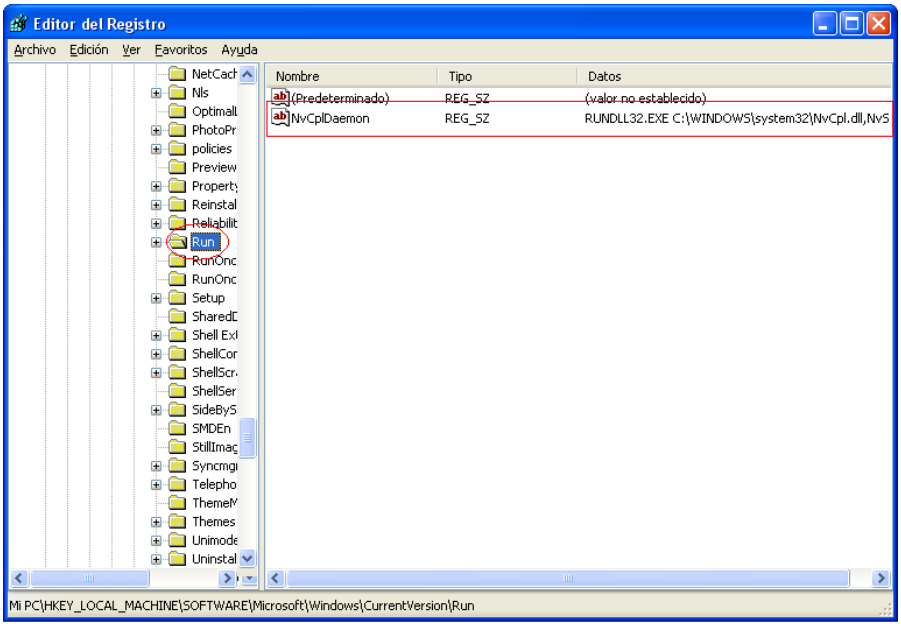
- ✓ \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- ✓ \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\\Windows\CurrenVersion\Run Once

- ✓ \HKEY_LOCAL_MACHINE\SOFTWARE\l\/licrosoft\Windows\CurrentVersion\Run OnceEX

HKEY_LOCAL_MACHINE puede cambiar por HKEY_CURRENT_USER

Figura 6. Archivos registrados en el inicio del Sistema Operativo Windows



Fuente. Autor

2.4.9 Daños ocasionados por los virus informáticos

2.4.9.1 Síntomas comunes en un sistema infectado con Malware

Con el fin de detectar posibles infecciones que se encuentren afectando el sistema operativo y aplicaciones se muestran los siguientes síntomas comunes en estos casos.

- ✓ Desaparición, modificación o corrupción de archivos.
- ✓ Respuesta lenta inusual o bloqueo aplicaciones o del sistema.
- ✓ Fallas en aplicaciones o inestabilidad del sistema.
- ✓ Aparición de procesos y servicios desconocidos y que se encuentren activos en el sistema (administrador de tareas “Ctrl + Alt + Supr”).
- ✓ Cambios en las plantillas del procesador de texto, hoja de cálculo, etc.
- ✓ Apertura inusual de puertos (“netstat –a” en el Shell de Windows: cmd).
- ✓ Envíos automáticos de mensajes a otros usuarios.
- ✓ Incremento del tráfico en la red.
- ✓ Aparición de elementos inesperados en la pantalla: imágenes, mensajes extraños, cambios en los iconos, etc.

2.4.9.2 Acciones comunes del Malware en la ejecución de rutinas

Entre los daños correspondientes a las rutinas de ataque a sistemas que son más utilizadas por los Malware se pueden resaltar los siguientes:

- ✓ Inhabilitación de programas de seguridad (antivirus, firewalls, servicios de administración del sistema, filtros antispam, IDS…) del equipo, dificultando la corrección del problema y facilitando posteriores infecciones de otros virus o el control remoto del equipo por parte de un usuario no autorizado.

- ✓ Robo de información a través de cualquier medio de transporte de datos como e-mail, sesiones FTP, etc.

- ✓ Destrucción o modificación de archivos en discos duros locales y de red a los que tiene acceso el equipo infectado. Esta acción podría afectar a todos los tipos de archivos o sólo a los de algunos tipos de archivo con una extensión determinada (por ejemplo documentos *.doc).

- ✓ Cambio de servidores DNS.

- ✓ Formateo de discos duros.

- ✓ Ataques para descifrar contraseñas de usuarios.

- ✓ Creación de puertas traseras abiertas en los Sistemas infectados para posible posterior toma de control de forma remota en equipos infectados.

- ✓ Utilizar los equipos infectados para llevar a cabo ataques contra otros computadores conectados en red

3. PROYECTO JUNTO CON EL ÁREA SOPORTE TÉCNICO PARA LA IMPLEMENTACIÓN DE LA VIRTUALIZACIÓN DE INFRAESTRUCTURA – VMWARE INFRASTRUCTURE

INTRODUCCIÓN

Parte importante del ámbito empresarial son los servidores, los cuales son esenciales para mantener disponibles tareas y procesos de los cuales la mayoría son imprescindibles para el buen funcionamiento de la organización. Los servidores más importantes que maneja la empresa ATH son los servidores transaccionales donde se registran todos los datos que representan movimientos de dinero entre cajeros, estado de los cajeros y estado de las cuentas de los bancos para los cuales prestan estos servicios. Algunos otros de los servidores que se manejan son el servidor de correo (interno y externo), el servidor de antivirus, el servidor de cámaras, el servidor de actualización de Windows (WSUS), servidores proxy, servidores de software, servidores de dominio, servidores de almacenamiento de datos.

En la empresa muy recientemente se empezó a implementar la virtualización de la infraestructura de TIC, mediante el uso de distintas herramientas acopladas que tienen la capacidad de hacer esta virtualización tanto de red como de servidores llamada Vmware infrastructure. Estas herramientas implantadas conjuntamente facilitan y mejoran de una manera enorme la administración de servidores, almacenamiento de datos, y uso de recursos informáticos con que cuenta la organización, y además prestan muchos otros servicios como alta disponibilidad, respuesta a fallos, distribución de recursos, portabilidad de servidores.

Actualmente se está realizando el proyecto de virtualización de los servidores transaccionales con el objetivo de mejorar los procesos y los planes de continuidad de negocio de la empresa.

Esta infraestructura genera muchísimas ventajas para el ámbito empresarial y hace que la administración y seguimiento de los procesos en los servidores empresariales funcionen de manera eficiente y sean fáciles de manejar.

3.1 VENTAJAS QUE OFRECE EL PROYECTO DE VIRTUALIZACIÓN DE LA INFRAESTRUCTURA VMWARE A LA EMPRESA

Con la implementación de la tecnología de virtualización VMware se da a la empresa

un gran ahorro tanto en costos operativos como costos de propiedad y contribuye en el mejoramiento de las operaciones empresariales con un aumento de la eficiencia en la operación de la infraestructura creada y también con el mejoramiento de los planes de continuidad del negocio aportando nuevas acciones posibles en caso de algún evento desafortunado que afecte uno o varios servidores físicos. Las ventajas que trae VMware Infrastructure a los aspectos organizacionales de ATH son:

- ✓ Reduce los requisitos de hardware aumentando la eficiencia en el uso de este en un alto porcentaje.

- ✓ Reduce el espacio necesario para los servidores en el centro de cómputo y reduce el consumo de energía eléctrica.

- ✓ Facilita al personal operar, monitorear y administrar la infraestructura, mediante la simplificación y la automatización de estos procesos que se centralizan y se hacen mucho más sencillos de realizar.

- ✓ Mejora la disponibilidad de los servicios, la utilización de recursos y el proceso de mantenimiento dentro de la infraestructura empresarial con las diferentes medidas que proporciona la virtualización y las herramientas disponibles.

- ✓ Mejora las políticas empresariales de continuidad del negocio permitiendo recuperación en caso de fallos inesperados y realización de mantenimiento con las máquinas en caliente.

- ✓ Permite realizar la ampliación de la infraestructura física de una manera sencilla solo agregando nuevos servidores físicos a la infraestructura ya conformada cuando las aplicaciones y procesos aumentan y requieren de más recursos físicos.

- ✓ Es independiente del hardware lo que hace posible la migración de la infraestructura virtual a otro hardware para la actualización o cualquier otro motivo.

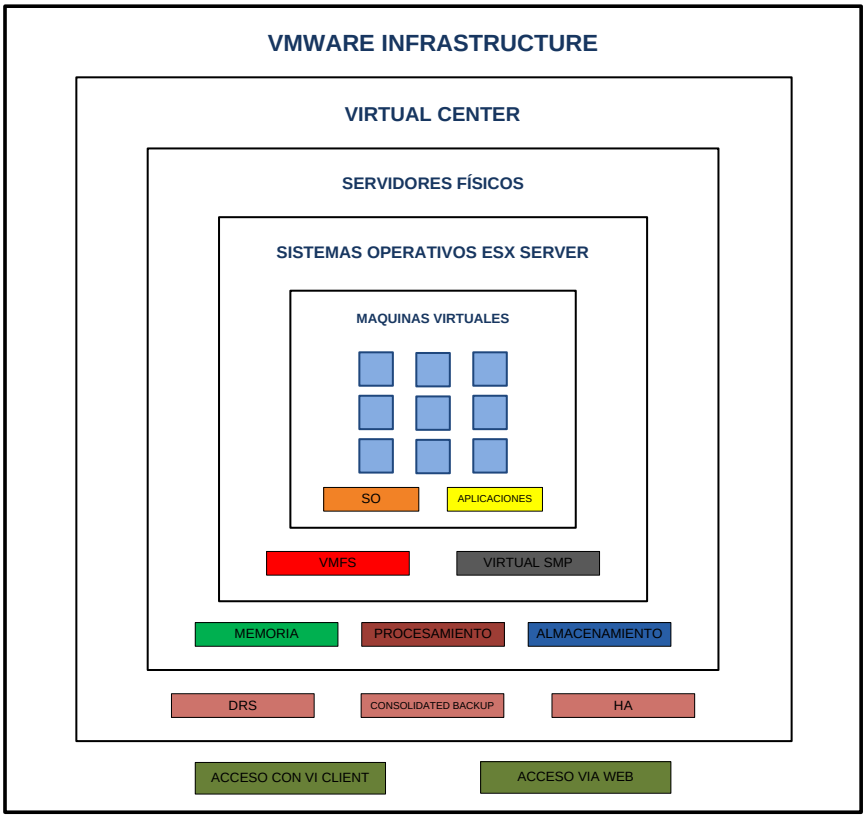
- ✓ Hace monitoreo inteligente de forma frecuente y adecua los elementos de la infraestructura de forma flexible para establecer la mejor funcionalidad posible de acuerdo a las preferencias configuradas por el administrador.

- ✓ Facilita la creación de nuevos servidores que sigan una plantilla común y la realización de backups de las máquinas virtuales.

3.2 IMPLEMENTACIÓN DE VMWARE INFRASTRUCTURE 3 EN ATH

La empresa ATH cuenta con varias áreas de trabajo de las cuales algunas realizan tareas de administración de servidores e infraestructura, como son el área de telecomunicaciones, el área de centro de cómputo, el área de seguridad Informática, el área de soporte Técnico, el área de soporte a la Infraestructura y otras. En el caso del área de soporte Técnico recién está implementada, y aún se trabaja en ello, la tecnología de Vmware Infrastructure para varios servidores. Actualmente se trabaja con el área de centro de cómputo con el objetivo de virtualizar la infraestructura de los servidores transaccionales de la empresa. Se va a hacer la explicación del proceso de virtualización de los servidores transaccionales del área de centro de cómputo en un Clúster[10] "Cluster ATH" y la organización de su infraestructura.

Figura 7. Capas de VMware Infrastructure



Fuente. Autor

[10] Acoplamiento de los recursos de varios servidores físicos que funcionan como si fueran uno solo con fines de mejorar los procesos de computación.

3.2.1 Recursos Hardware necesarios

La mayoría de recursos de hardware como servidores, clústers, infraestructura de networking, y demás elementos importantes utilizados de la Empresa ATH para realizar procesos y manejar información de esta misma y del Grupo Aval, entre ellos los necesarios para la virtualización de infraestructura Vmware, se encuentran ubicados en el centro de cómputo (también conocido como centro de procesamiento de datos) de la empresa.

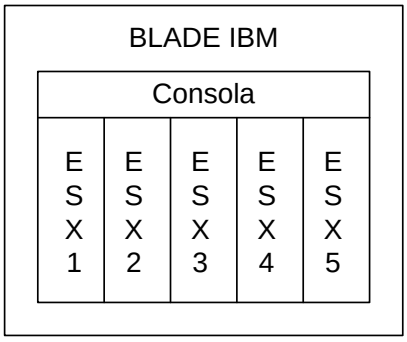
En el centro de cómputo se tienen los siguientes recursos hardware que se adquirieron para este proyecto y son necesarios para la implementación de Vmware Infrastructure y el alojamiento de los servidores transaccionales virtuales de los cuales se han incluido 34 servidores hasta el momento:

- ✓ 1 Blade[11] IBM

  - ✓ Cinco cuchillas[12] Blade (servidores físicos) que conformaran el clúster, donde en cada una se instalaran los S.O. ESXs, cada cuchilla cuenta con:

    - 120 GB de Disco Duro
    - 2 procesadores Quad Core (8 núcleos) de 2.66 GHz
    - 16 GB de RAM
    - 2 NICs (Interfaz de tarjeta de red)

Figura 8. Representación Blade IBM y cuchillas Hardware con los Sistemas Operativos ESX



Fuente. Autor

[11] Servidores Físicos de gran capacidad acoplados especialmente para el aprovechamiento de espacios en los centros de cómputo empresariales.

[12] Hace referencia a cada servidor físico dentro del Blade IBM el cual tiene determinados recursos Hardware entre los que están procesadores, memoria y disco duro.

A cada cuchilla como se puede ver en la figura anterior se le instala el Sistema Operativo ESX, este es un S.O en modo texto, el cual tiene kernel de S.O Linux (Red Hat) y va a tener alojados en promedio 7 servidores en 7 máquinas virtuales cada una con:

- ✓ S.O Windows NT
- ✓ 1 GB de RAM
- ✓ 15 GB de Disco duro
- ✓ 1 procesador de 2.6 GHz

El almacenamiento de las maquinas virtuales se hace en un arreglo de Discos SAN (Storage Área Network), cada SAN tiene definidas 5 LUNs (Logical Unit Number) con 105 GB de capacidad cada una para un total de 525 GB en la SAN.

3.2.2 Instalación de ESX Server

Primero que todo fue necesario instalar los sistemas operativos en modo texto que posteriormente sirvieron como base para el posterior aprovisionamiento de las máquinas virtuales. Este paso se realizo por igual para las 5 cuchillas del blade IBM del centro de cómputo.

Para Instalar el S.O ESX Server se contó con el medio de instalación CD-ROM y se siguieron los siguientes pasos:

- ✓ Bootear el CD de instalación.
- ✓ Empezar la instalación. Al iniciar se presentan 2 opciones (modo gráfico y modo texto), se realiza en modo gráfico.
- ✓ Se hace la configuración del teclado y mouse, se acepta la licencia de instalación.
- ✓ Se hace el formato de la unidad de disco local. Hay que tener cuidado porque el software no revisa estos discos y borra todo los datos de este, por esto, hay que verificar que se va a formatear el disco local y no algún arreglo SAN.

- ✓ Se hace la configuración de la red: Se elige la NIC virtual que se va a utilizar para la consola (vswif0), se ingresa la IP de la consola, el Gateway, el DNS, y el FQDN del ESX. Los datos en ATH fueron:

    - IP: 192.168.11.7
    - Gateway: 10.130.0.15
    - DNS: 10.130.0.15
    - FQDN: athvmesx1p.ath.net

- ✓ Se selecciona la hora local (Time Zone Selection)

- ✓ Se teclea la contraseña de administrador (root).

- ✓ Se verifica toda la información, se acepta y se reinicia el servidor.

3.2.3 Instalación del Virtual Infrastructure Client (VI Client)

El VI Client es la interfaz principal de VMware Infrastructure donde se puede manipular, administrar y monitorear todo el sistema, es el cliente de administración remota del Servidor Virtual Center y los Hosts (ESX), con este se puede hacer conexión al Virtual Center Server o a cada uno de ESX Servers individualmente. La interfaz muestra distintos tipos de opciones dependiendo de a qué tipo de servidor se haga conexión y este también provee de una consola de acceso a las máquinas virtuales.

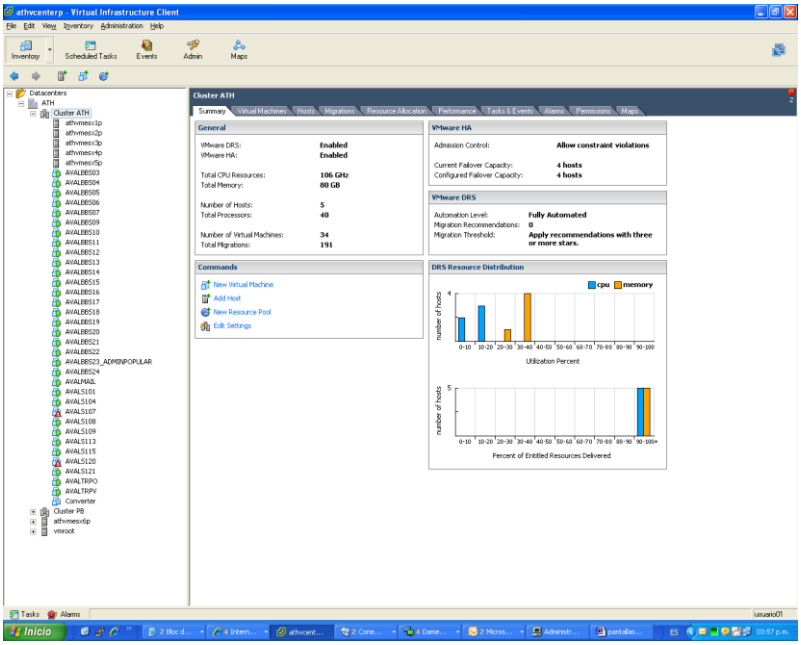
Después de instalar los servidores ESX se instaló el Virtual Infrastructure Client que es la parte más importante en ésta infraestructura en cuanto a administración, configuración y seguimiento de todos los elementos del sistema virtual. La instalación es bastante sencilla, ésta se instaló como una aplicación sobre el sistema operativo de los equipos donde se requirió tener esta herramienta administrativa y teniendo en cuenta que se pudiera conectar con los ESX o con el Virtual Center.

Con el Virtual Infrastructure Client es posible acceder a los ESX instalados en la red mediante el protocolo Web http y hacer configuraciones (networking, insertar licencia, añadir usuarios y permisos, añadir maquinas virtuales, etc.).

3.2.3.1 Infraestructura VMware en ATH desde el VI Client

A continuación podemos ver como es la administración y monitoreo de la infraestructura a través de la utilización de la herramienta VI Client. Se ven algunas pantallas de las opciones administrativas (control, configuración y monitoreo) configuradas según el servidor al que se está conectado y las necesidades organizacionales que se tengan. También se podrá observar gráficamente como está organizada la infraestructura virtual y como es vista ésta desde la aplicación VI.

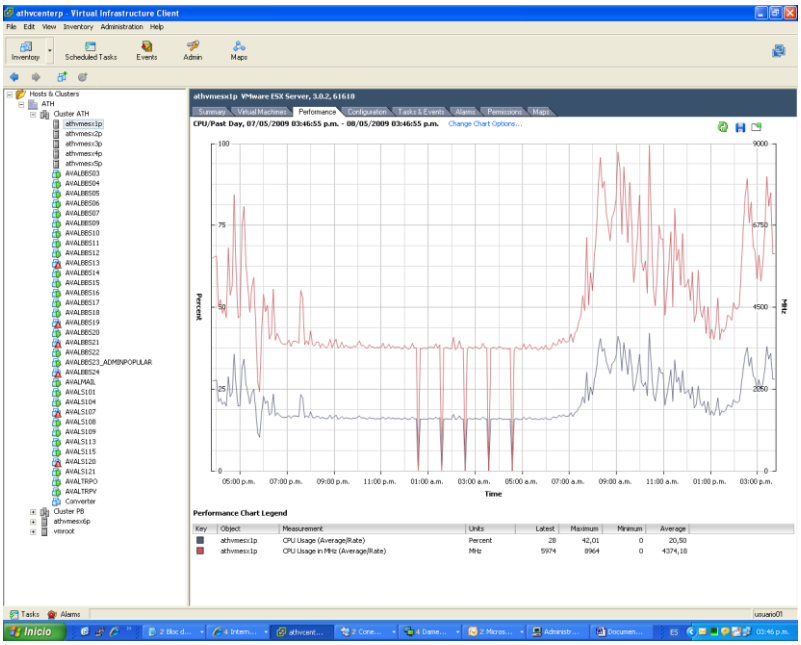
Figura 9. Ventana WEB para monitoreo y Administración del Clúster ATH



Fuente. Autor

En la parte izquierda de la gráfica se ve como está conformado el Clúster ATH con sus Hosts ESX y sus máquinas virtuales. En la parte derecha se encuentra el resumen de las características del clúster (Summary) y las demás pestañas de administración y monitoreo. Si se necesita ver las opciones de administración y monitoreo de los ESX o las máquinas virtuales individualmente, se debe dar clic en el ESX o máquina virtual en la parte izquierda de la página y así se verán las opciones en el panel derecho de la página.

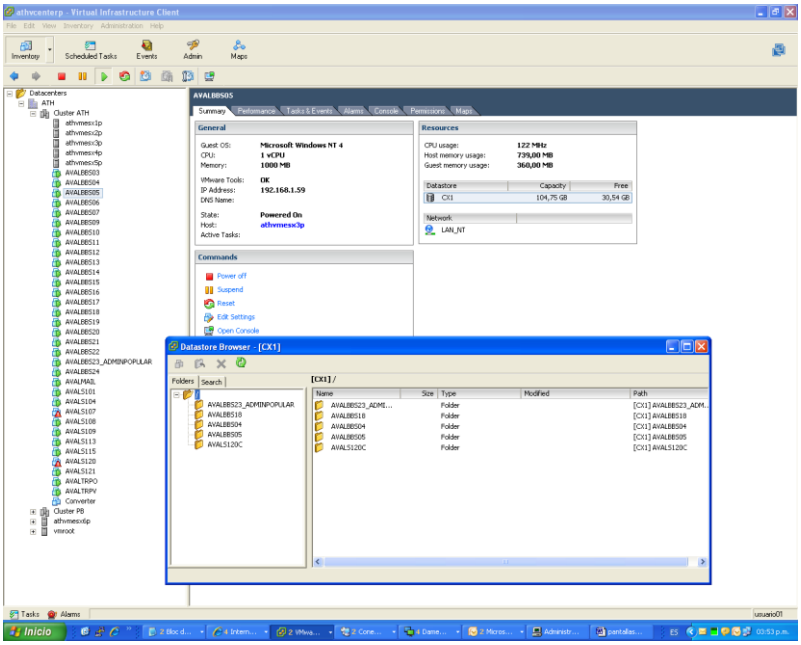
Figura 10. Ventana WEB para monitoreo y Administración del ESX athvmesx1p



Fuente. Autor

En esta gráfica se puede ver el monitoreo del desempeño de la CPU en términos de MHz y de porcentaje en el transcurso del tiempo para el servidor ESX athvmesx1p.

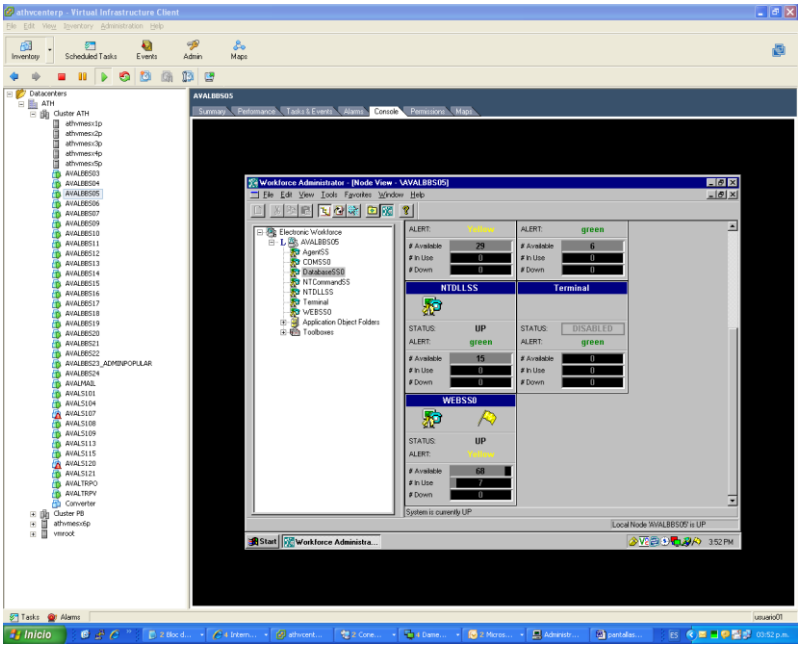
Figura 11. Contenido de una LUN



Fuente. Autor

En ésta grafica se puede ver que dentro de las opciones de la máquina virtual es posible acceder (en resources – Datastore – CX1) a la información de la LUN donde la máquina virtual se encuentra almacenada, y vemos cual es el contenido completo de ésta LUN que en este caso tiene 5 maquinas virtuales (los folders).

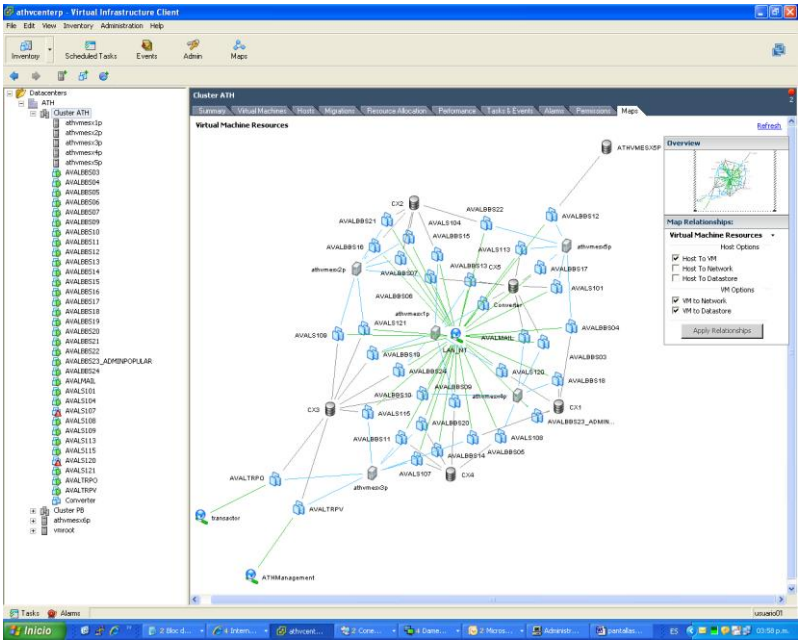
Figura 12. Acceso remoto a una máquina Virtual dentro de la Infraestructura Vmware mediante el Virtual Infrastructure Client



Fuente. Autor

En ésta gráfica se ve como es el acceso remotamente mediante la consola del VI Client al control de una máquina virtual dentro de la infraestructura.

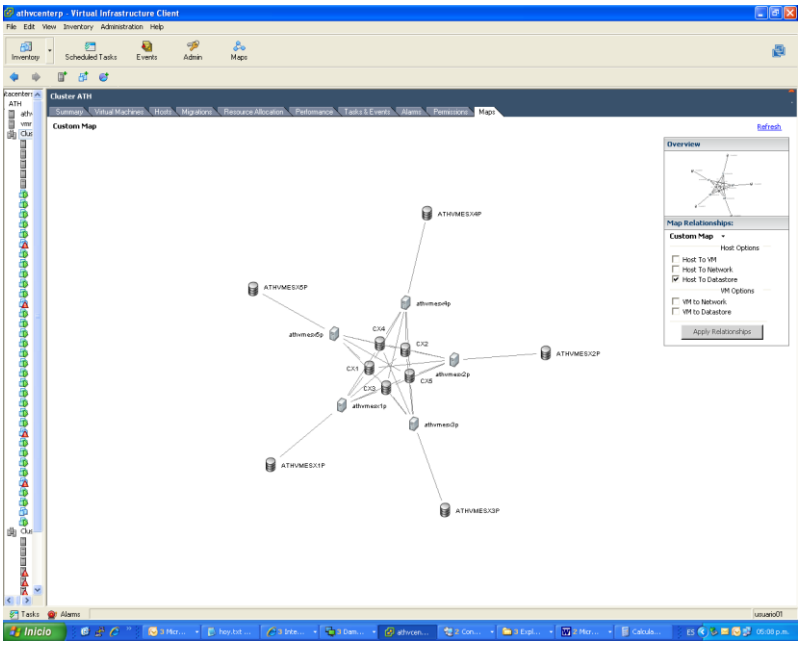
Figura 13. Conexión de red de todos los elementos del Clúster ATH visto desde el Virtual Infrastructure Client



Fuente. Autor

En esta gráfica se puede ver cómo está configurada la infraestructura virtual VMware Infrastructure para este clúster (Clúster ATH). Se puede ver claramente como todas las máquinas virtuales tienen conexión a todas las LUN para que en caso de una falla o cualquier otro motivo que ocurra en la infraestructura, ésta se encargue de utilizar todas las herramientas que tiene (VMware HA, VMotion, VMware DRS,…) para garantizar la disponibilidad y eficiencia de los servidores virtuales. La infraestructura está conectada en una red LAN y además tiene conexión con la red transaccional y una red de administración.

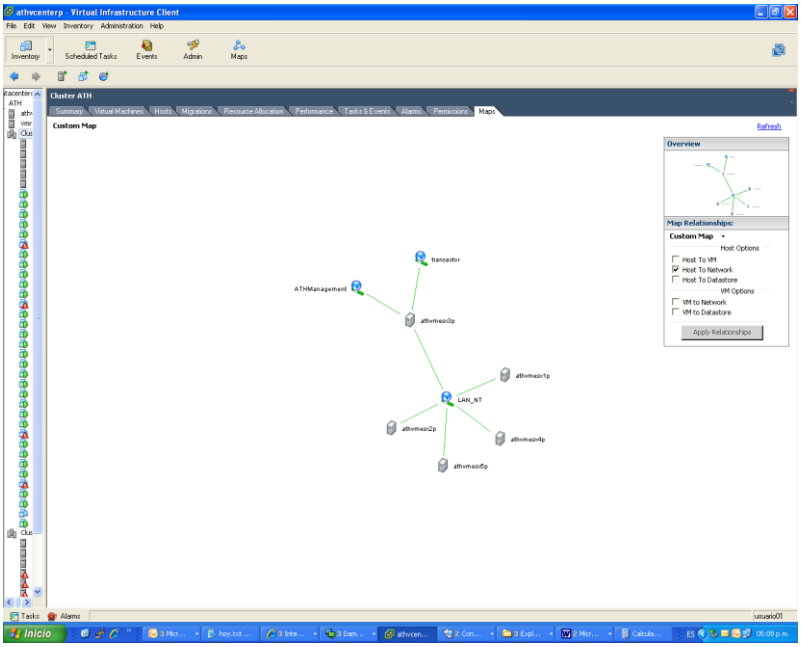
Figura 14. Conexión entre Hosts y LUNs visto desde el Virtual Infrastructure Client



Fuente. Autor

En ésta gráfica se observa la conexión entre los Hosts y las LUN (Datastore) en la infraestructura virtual.

Figura 15. Conexión de la Infraestructura Virtual con las redes Empresariales



Fuente. Autor

En ésta gráfica se ve como es la conexión de los Hosts ESX y las redes empresariales.

3.2.4 Configuración del protocolo de sincronización de tiempo en red NTP para los Servidores ESX

Es importante que los host servidores ESX corran con el tiempo correctamente de modo que los datos de funcionamiento puedan ser recogidos y transferidos correctamente.

El Network Time Protocol (NTP) es un protocolo estándar de Internet usado para sincronizar los tiempos de relojes a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP (Datagramas) como su capa de transporte, usando el puerto 123 y está diseñado para resistir los efectos de la latencia variable.

Para hacer la configuración del NTP se puede ir por muchos caminos. Uno de estos, el cual se utiliza en ATH se describe a continuación:

- ✓ Se abre una sesión de consola de comandos segura (secure shell session) hacia el Servidor ESX. Se usa el aplicativo Putty, el cual es libre y reconocido ampliamente.

- ✓ Se ingresa la IP del servidor ESX y se selecciona la opción de protocolo SSH.

- ✓ Se abre la sesión y se hace login con una cuenta diferente a la de administrador.

- ✓ Después de hacer el login con la cuenta diferente a la de administrador se digita el comando: su **–,** para cambiar a la cuenta de administrador. (Estos dos últimos pasos se tienen que hacer para poder ingresar al servidor con privilegios administrativos de forma indirecta, ya que por defecto no es posible el acceso directamente a la cuenta root por motivos de seguridad, pero esta configuración se puede cambiar con otros comandos y la modificación de algunos archivos para que se pueda hacer login directamente con la cuenta root)

- ✓ Se saca backup del archivo de configuración NTP, /etc/ntp.conf:

  cp /etc/ntp.conf /etc/ORIG.ntp.conf

- ✓ Se usa uno de los editores de texto del sistema operativo (nano o vi) para modificar el archivo /etc/ntp.conf;

  nano –w /etc/ntp.conf

- ✓ Se encuentra la entrada restrict default ignore en el archivo para modificarla así:

  Restrict default kod nomodify notrap noquery nopeer

- ✓ Se baja a la seccion # --- OUR TIMESERVERS -----, y se buscan las lineas:

  # restrict mytrustedtimeserverip mask 255.255.255.255 nomodify notrap noqwery

  # server mytrustedtimeserverip

  Se remueven los símbolos # de las dos lineas y se reemplaza el término mytrustedtimeserverip por la IP o el hostname del servidor NTP que se tenga. El resto se deja todo igual.

- ✓ Se deja el resto del archivo como está, guardar y salir.

- ✓ Se crea un backup del archivo, /etc/ntp/step-tickers:

  cp /etc/ntp/step-tickers /etc/ntp/ORIG.step-tickers

- ✓ Se abre el archive con el editor nano y se añade la dirección del servidor NTP.

  nano –w /etc/ntp/step-tickers

<Dirección_IP_o_hostname_del_servidor_de_tiempo_NTP**>,** por ejemplo: <192.168.103.229>

- ✓ Guardar y salir.

- ✓ Se habilita el servicio ntpClient sobre la consola de servicio:

```
Esxcfg -firewall -e ntpClient
```

- ✓ Se reinicia el demonio vmware –hostd para que los cambios que se hicieron con esxcfg-firewall surtan efecto en el VI Client.

```
# service mgmt -vmware restart
```

3.2.5 Networking

El servidor ESX permite crear redes virtuales internas para el manejo de la consola, maquinas virtuales, etc. Esta configuración interna de las redes virtuales se hace teniendo en cuenta unos parámetros preestablecidos:

Primero se revisa la información de las NICs virtuales en el ESX usando el comando (con la ayuda de PuTTY y con privilegios administrativos):

```
esxcfg nics -l
```

Se examina la información que se despliega con el comando anterior y se siguen las siguientes instrucciones:

- ✓ Se usa la vmnic con menor número de dirección PCI para el servicio de consola (este ya esta creada ya que la realiza automáticamente en el proceso de instalación del ESX Server).

- ✓ La red para las maquinas virtuales usa vmnic con el segundo menor número de dirección PCI.

- ✓ La red de VMotion, usa la vmnic con el más alto número de dirección PCI.

Ejemplo:

Tabla 3. Parámetros para la configuración de las Redes Virtuales

Tipo servicio	PCI address	Nombre del Virtual Switch
Consola de Servicio	02:00:00	vswitch0
Maquinas Virtuales	02:00:01	vswitch1
Kernel VM	07:06:00	vswitch3

Fuente. Autor

El resto de la configuración de red se realiza a través del VI Client en la pestaña configuración, en networking, creando los Switches virtuales y configurando las NICs virtuales.

3.2.6 Creación de un Datastore tipo VMFS

Al instalar los servidores ESX, estos vienen equipados con soporte para adaptadores HBA (host bus adapter) de canal de fibra. También al instalar se asignan varias LUN, dos de las cuales son llamadas LUN privadas. Estas LUN privadas son las LUNs que se van a utilizar para el almacenamiento de datos (las máquinas virtuales) junto con las LUNs de los otros servidores ESX, conformando así una SAN (Storage Área Network) y posibilitando todos los beneficios que trae la infraestructura Vmware. La conformación de las LUN puede ser posteriormente modificada.

Estas unidades lógicas están basadas y diseñadas para implementarlas en una unidad SAN, y mediante la utilización de VI Client es posible realizar la configuración de las LUNs, donde se pueden extender y convertir al formato VMFS (Virtual Machine File System) convirtiéndose en una datastore que inicialmente solo será visible para este ESX, también desde VI Client se puede asignarles y cambiarles el nombre o remover y volver a crear las datastores en formato VMFS creadas si es necesario.

El formato VMFS es un formato de archivos creado especialmente para el uso de VMware Infrastructure, pero también es posible si se necesita usar el formato NFS

(Network File System) que es otro protocolo para sistema de archivo distribuido en redes.

3.2.7 Creación del Virtual Center

El servidor virtual center es otro de los componentes de Vmware Infrastructure que se usa para integrar todos los SO ESX.

Para la instalación de Virtual center es necesario primero la creación de una base de datos ODBC en el computador servidor de VC y para uso de este mismo, después de la creación de esta ODBC se hace la instalación del servidor de licencias de Vmware y por último si se desea se puede instalar el VI Client en esta máquina.

Después de instalado el Virtual Center y con la ayuda del VI Client ya se pueden añadir host ESXs a la infraestructura con el ánimo de tener una integración de toda la infraestructura que va a ser fácil de administrar y controlar, y tendrá todas las ventajas que ofrece esta tecnología de virtualización. Para acceder al Virtual Center mediante el uso de VI Client se hace login de la misma forma que para acceder a un ESX individual pero en vez de digitar la IP del ESX se digita la IP del Virtual Center en el login.

Al acceder al virtual center se tienen muchas posibilidades de configuración y control tales como visualización y modificación del inventario de la infraestructura, administrar los ESX y los clúster que creemos a partir de estos, crear maquinas virtuales en cualquier datacenter, instalar Sistemas Operativos en las máquinas Virtuales, y muchas otras.

3.3 CONFIGURACIÓN DE VIRTUAL INFRASTRUCTURE SEGÚN REQUERIMIENTOS EMPRESARIALES

Después de implementar toda esta infraestructura se debe proceder a la configuración de todas las herramientas con que esta cuenta y guiándose por las necesidades y requerimientos que tenga la empresa. La herramientas con que Vmware Infrastructure son muchas y bien configuradas pueden hacer que los procesos de los servidores sean bastante fáciles de llevar y además tengan una magnífica seguridad en cuanto a integridad, confidencialidad y disponibilidad.

Algunos de los servicios que ofrece son:

- ✓ Clonación de maquinas virtuales con templete provisioning.

- ✓ Crear máquinas virtuales que funcionen como NAT router.

- ✓ Permitir a las maquinas virtuales acceder a materia prima (hardware) de una LUN disco.

- ✓ Crear VLANs.

- ✓ Agregar, quitar y administrar permisos para acceder a las máquinas virtuales.

- ✓ Crear pools de recursos para administrar y controlar los recursos hardware de la infraestructura mediante políticas según las necesidades de los servidores.

- ✓ Migrar maquinas virtuales entre hosts con VMotion de acuerdo a nuestro criterio o necesidades en la organización estructural.

- ✓ Hacer distribución inteligente y automática de recursos entre las máquinas virtuales con Vmware DRS ajustando los pool de recursos según prioridades, uso y disponibilidad de estos.

- ✓ Monitorear el funcionamiento de las máquinas virtuales y sus recursos (procesador, memoria,…) mediante distintas herramientas y opciones (graficas, estadísticas…).

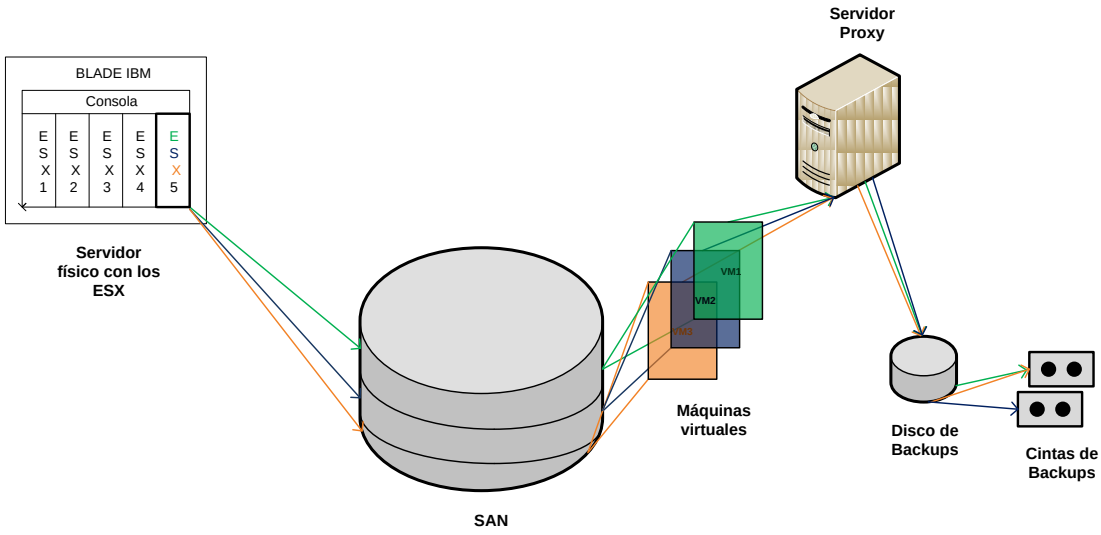
- ✓ Crear alarmas para las máquinas virtuales alerten cualquier suceso que se considere importante (sobrecargas de procesamiento, inactividades, etc) con opciones de respuesta como envío de e – mails o reiniciación de las máquinas.

- ✓ Aumentar la disponibilidad de los servidores utilizando VMotion que se encarga de migrar automáticamente y en caliente (máquinas virtuales encendidas) si se requiere las máquinas virtuales a otro host por cualquier motivo de falla que lleve a no disponer de los recursos hardware de su propio host siguiendo con los procesos de estas máquinas utilizando los recursos disponibles de la infraestructura.

3.4 REALIZACIÓN DE BACKUPS EN LA INFRAESTRUCTURA VIRTUAL DE ATH

La infraestructura virtualizada con VMware ofrece la posibilidad de la realización de backups de las máquinas virtuales con su servicio VMware Consolidated Backup, pero este en si no es un software dedicado a la realización de backups y debe estar apoyado con herramientas que realmente estén diseñadas y perfeccionadas para este propósito. Esta utilidad de Backups permite ser configurada y compenetrada con el software profesional de backups con el fin de realizar los backups de acuerdo con las necesidades de frecuencia, servidores críticos, nivel de redundancia y otros que exija la empresa. Actualmente esta herramienta puede ser utilizada para realizar los backups a través de la red empresarial o a través de servidores proxy con ayuda de otras herramientas para realización de backups. Es posible y adaptar el modo de realización de estas tareas de muchas formas incluyendo realizaciones de backups a una unidad LUN completa o simplemente realizar backups a determinados archivos que contienen cada una de las maquinas virtuales (archivos *.vmdk). En ATH se tiene implementada la infraestructura de backups de la forma que se muestra a continuación y con la ayuda de la herramienta profesional para la realización de backups llamada HP Data Protector.

Figura 16. Realización de Backups en la Infraestructura Virtual



Fuente. Autor

4. EXPLORACIÓN E IMPLEMENTACIÓN SOFTWARE LIBRE: OCS INVENTORY NG.

4.1 IMPLEMENTACIÓN DEL SOFTWARE LIBRE OCS INVERNTORY AGENT

El proceso de investigación de software libre en ATH se puede presentar ya sea por sugerencia de alguien del personal de la empresa (trabajadores o directivos) o por que el equipo de investigación ha encontrado alguna herramienta bajo licencia de software libre que se presume podía implementarse en la empresa, siempre con el objetivo de mejorar los procesos empresariales sin afectar otros procesos.

La herramienta de realización de inventarios y distribución e implementación de paquetes OCS Inventory es una herramienta web que funciona bajo la licencia de software libre GPL v2. Al iniciar la práctica empresarial en la empresa ATH se estaba trabajando ya en la investigación de esta herramienta y las posibles ventajas que podía ofrecer al área de soporte a la infraestructura en sus procesos de monitoreo y revisión de software como los de inventario de hardware. En el transcurso de la práctica empresarial se trabajo junto con los integrantes del área de soporte a la infraestructura en la investigación de este software para su posterior implementación en todos los equipos del establecimiento principal de la empresa en la ciudad de Bogotá.

OCS Inventory está diseñado con el objetivo de facilitar de gran forma al administrador de una red de equipos en la realización del inventario de todos los elementos software y hardware actualizado de estos, y además de esto permite la distribución de paquetes con protocolo SSH en los computadores que tengan el agente instalado el cliente (OCSNG AGENT). Para lo anterior se debe instalar un servidor (OCSNG SERVER), el cual permite administrar los datos y controlar a los agentes, utilizando la comunicación entre el cliente y el servidor que está basada en protocolos HTTP/HTTPS y los lenguajes de programación PHP y XML. Otra ventaja de esta herramienta es que permite ser desplegada en las plataformas Windows y Linux.

Para la instalación del servidor de OCS Inventory se debe cumplir con el requisito de instalación de la utilidad independiente de plataforma XAMPP ya que este software solo funciona sobre esta utilidad. La instalación de esta herramienta nos permitirá:

- ✓ Tener instalado un servidor web Apache en el equipo donde se instalará el servidor OCS Inventory.

- ✓ Contar con el servidor y manejador de base de datos MYSQL que permitirá almacenar la información de los inventarios.

- ✓ Instalar el intérprete para páginas web dinámicas PHP.

- ✓ Instalar el intérprete en modo shell para programación estructurada, orientada a objetos y funcional PERL.

4.1.1 Instalación del OCS Inventory NG Server versión 1.0.2 para Windows

El servidor se instaló únicamente en un equipo y servirá para que el administrador realice cualquier servicio que esta herramienta ofrece y presta el servicio de inventariado e implementación segura de paquetes a los equipos que tengan instalado el agente (cliente) con la configuración apuntando a este servidor.

El servidor de OCS Inventory se instaló en un servidor físico ubicado en el área de soporte a la infraestructura el cual también es utilizado como servidor de archivos por los integrantes de esta misma área. Este servidor físico está conectado a la red de trabajadores interna de la empresa y por esto es accesible desde cualquier otro computador dentro de esta misma red. El servidor de inventario OCS es accesible vía web y hay comunicación con él desde cualquier equipo de la empresa conectado a la red mediante el protocolo http, por lo tanto los administradores de esta utilidad pueden acceder a ella desde cualquier equipo conectado al servidor en red y revisar el inventario o hacer distribución de paquetes en los equipos con los agentes instalados.

Para empezar a implementar la utilidad primero se descargaron los instaladores de servidor y de cliente, los cuales se encuentran disponibles gratuitamente en la página oficial de OCS Inventory de internet[13]. Después de ingresar a la opción de descargas dentro de la página se eligió primero la versión a instalar (versión 1.02) y se procedió a descargar los archivos para plataforma Windows en los links de descarga los cuales son: OCSNG_WINDOWS_SERVER-1.02.1.zip (Servidor OCS) y OCSNG_WINDOWS_AGENT_1.02.zip (Cliente OCS).

Al tener el archivo comprimido que contiene el archivo instalador del servidor OCS en el disco duro del servidor físico se descomprimió con la herramienta 7-Zip y se obtuvo el archivo OcsWin32ServerSetup.exe.

Al ejecutar este archivo se presentaron algunos mensajes indicando que en el equipo no se encontraba instalada la utilidad web XAMPP e indicando que esta debía ser instalada antes de proceder a realizar la instalación del OCS Inventory server ya que esta herramienta no puede ser implementada en un servidor web diferente de este.

Después de los mensajes de advertencia se procedió con la instalación del servidor

[13] Pagina Oficial de la Aplicación OCS INVENTORY NG. http://www.ocsinventory-ng.org/.

web XAMPP. Algunos pasos importantes en la instalación del Servidor web se mencionan a continuación.

- ✓ Se escogió el directorio por defecto de instalación C:\xampp.
- ✓ Se seleccionaron los componentes a instalar (XAMPP y OCS Inventory ng Server)
- ✓ Se inició el XAMPP control panel cuando se mostró el mensaje de advertencia para iniciar el panel al final de la instalación del XAMPP.
- ✓ Se termino realizando la instalación del OCS Inventory NG server.

Al finalizar la instalación el asistente dio la opción de revisar el estado de la seguridad del servidor. Esta se reviso con el fin de verificar su estado. Después de la instalación se debieron realizar algunos pasos de configuración que se describen a continuación:

En la página web desplegada automáticamente al finalizar la instalación del server (http://localhost/ocsreports/install.php) se realizó la configuración de los parámetros de seguridad del manejador de base de datos MySql de la siguiente forma:

- ✓ MySql login: root
- ✓ MySql password: (se deja vacio)
- ✓ MySql HostName: localhost

Después de realizar esta configuración se mostro una ventana web donde se ve como la base de datos realiza algunas acciones, crear la base de datos "ocsweb" y el usuario MySQL con la contraseña, asignar al usuario los permisos sobre la base de datos como seleccionar, insertar, eliminar, etc. El servidor OCS utiliza este usuario para conectarse a la base de datos. En esta misma ventana se realizó la configuración del TAG que es una opción que ofrece el aplicativo para poder agrupar los computadores con clientes mediante un criterio especial. El TAG utilizado fue "AREA DE LA EMPRESA" para clasificar los computadores según el área de trabajo donde se encuentra el equipo.

Con esto se finalizo la instalación del OCS Server y se mostro una notificación que advirtió:

NOTICE: You will not be able to build any deployment package with size greater than 200M. You must raise both post_max_size and upload_max_filesize in your php.ini to increase this limit.

Esta notificación se refiere a la opción de distribución de paquetes que incluye esta herramienta advirtiendo que no es posible implementar paquetes de tamaño superior a 200 Mega Bytes y diciendo que se puede editar esta opción en el archivo php.ini del servidor XAMPP que se encuentra dentro de la carpeta php modificando las variables post_max_size y upload_max_filesize.

Con el servidor instalado ya se pudo hacer login en la página principal del OCS server en la dirección http://localhost/ocsreports/index.php con el usuario "admin" y el password "admin" y en este momento ya está preparado el servidor de inventario e implementación de paquetes OCS para prestar sus servicios.

4.1.2 Instalación del OCS Inventory NG Agent versión 1.0.2 para Windows

El agente de OCS Inventory se instaló en todos los equipos de trabajo de la sede principal de ATH para los cuales se requería mantener un inventario actualizado de hardware y software. Para cada equipo se repitió la instalación y configuración del agente paso a paso como se describe a continuación:

El archivo OCSNG_WINDOWS_AGENT_1.02 que se descargo anteriormente fue guardado en el servidor de archivos para poder accederlo desde cualquier equipo conectado a la red empresarial.

Desde cada uno de los equipos de trabajo en donde se requería instalar el cliente OCS Inventory se procedió a descomprimirlo y ejecutarlo.

Durante el proceso de instalación de los agentes el software requirió la inserción de los datos y elecciones de configuración para lo cual se procedió a configurar los agentes de la siguiente manera:

Tabla 4. Datos para la configuración del Cliente OCS en la empresa

REQUERIMIENTO	**VALOR**	**CHECKEADO**
Server Address	10.130.0.89	
Server Port	80	
No IE Proxy		SI
Enable log file		SI
Inmediatly launch inventory (=/NOW)		SI
No Ocs_Contact shortcut (=/NoOcs_ContactLnk)		NO
Misellaneous	SIN VALOR	

Fuente. Autor

Campos:

- ✓ SERVER ADDRESS: Dirección del equipo donde se instaló el servidor OCS Inventory.

- ✓ SERVER PORT: Puerto para la comunicación con el servidor.

- ✓ NO IE PROXY: Comunicación sin proxy.

- ✓ ENABLE LOG FILE: Habilitar archivo de logs.

- ✓ INMEDIATLY LAUNCH INVENTORY (=/NOW): Enviar inventario al servidor al finalizar la instalación.

- ✓ NO OCS_CONTACT SHORTCUT (=/NoOcs_ContactLnk): Deshabilitar el acceso directo a la opción Ocs Contact.

Después de configurar estos datos comenzó la instalación del agente. Mientras se está instalando el software hace el requerimiento del TAG que clasifica al equipo. En el TAG se incluyo la clasificación de cada equipo de trabajo según su área, por ejemplo, Recursos Humanos.

4.2 ADMINISTRACIÓN DE OCS INVENTORY

Después de la instalación del servidor y el cliente OCS Inventory fue posible acceder vía web y utilizar las opciones que ofrece esta herramienta. Algunas de las opciones que fueron utilizadas por el área fueron:

4.2.1 Listas de computadores

- ✓ Todos los computadores:

  Esta opción realiza una lista con todos los computadores que han hecho contacto con el servidor y han enviado su inventario. La información que muestra por defecto esta opción para cada computador inventariado es:

  - o TAG

- Fecha del último inventario
- Nombre del computador
- Nombre del usuario activo cuando se realizó el inventario
- Sistema operativo instalado en el computador
- Capacidad de memoria RAM del computador (MB)
- Capacidad de CPU del computador (MHz)

Estas opciones son editables ya que tienen la opción de remover e insertar columnas que muestren información diferente (Dirección IP, Dominio, etc.) dependiendo de los requerimientos del administrador de la herramienta.

✓ Etiqueta (TAG):

Esta opción muestra la información de las etiquetas que se han incluido en el inventario y la cantidad de equipos que existen inventariados con cada etiqueta. La información que se muestra con esta opción es:

- TAG
- Número de computadores con ese mismo TAG

✓ Grupos:

En esta opción se crean grupos de computadores siguiendo algún criterio de selección. La información que se muestra una vez creado el grupo es la siguiente:

- Nombre del grupo
- Descripción del grupo
- Fecha de creación
- Número de computadores en el grupo

✓ Programas:

Esta es una opción de mucha utilidad en la empresa ya que ofrece la posibilidad de revisar el software inventariado en los computadores por

distintos criterios, por ejemplo, por letra del alfabeto inicial, por nombre del software o por cantidad de equipos que tengan determinada cantidad de software. Esta utilidad es muy útil a la hora de monitorear software con licencia privativa, con el fin de no superar las licencias instaladas de las adquiridas para evitar posibles sanciones y tampoco desaprovechar licencias adquiridas que no se estén utilizando. Esta utilidad muestra 2 campos de información que son:

- Nombre del Software
- Cantidad de este Software instalado en los equipos inventariados

✓ Varios criterios:

Con esta opción es posible clasificar los computadores inventariados bajo uno o más criterios seleccionados por el administrador que realiza la consulta. Algunos de los criterios de selección son:

- Dirección IP
- Dirección MAC
- Dominio
- Memoria
- Nombre del computador
- Sistema Operativo
- Fecha del último inventario

4.2.2 Descripción detallada de equipos

En ocasiones fue necesario realizar la revisión del estado de computadores particularmente a causa de problemas o requerimientos como revisión de paquetes y actualizaciones de seguridad del sistema operativo, revisión de licenciamiento de un equipo, tarjetas de red del equipo y otra información necesaria para las labores de soporte a la infraestructura y mantenimiento. Para esto se utilizó esta herramienta y la opción de revisión detallada del inventario de un equipo. Esta opción es posible al seleccionar un equipo en particular dentro de la estructura de inventario OCS inventory describiendo detalladamente al equipo seleccionado y mostrando información sobre:

✓ Software del equipo

- ✓ Aspectos de configuración del equipo (Dominio, memoria virtual, etc.)
- ✓ Procesadores
- ✓ Memoria
- ✓ Almacenamiento
- ✓ Tarjetas de video
- ✓ Dispositivos de red
- ✓ Dispositivos de entrada
- ✓ Otros

Esta utilidad también dio la posibilidad de ver en la misma página web el inventario completo (sin criterio de selección) e imprimirlo si era necesario.

4.2.3 Modificación de la etiqueta TAG

Puede presentarse la necesidad de modificar la etiqueta de conformación de grupos en la empresa como por ejemplo no dividirlos en áreas sino en pisos. Si se quiere crear o modificar la etiqueta TAG, se selecciona la opción archivo de modificación de la etiqueta se introduce el nuevo TAG y se selecciona la opción envoyer (enviar).

4.3. DISTRIBUCIÓN DE SOFTWARE Y EJECUCIÓN DE COMANDOS SOBRE LOS COMPUTADORES CLIENTES

4.3.1 Requerimientos que fueron necesarios para la utilización de distribución de software

1. Se debió configurar las opciones del servidor local en la opción configuration de la siguiente forma en cada una de las pestañas:

- ✓ En SERVIDOR

  Habilitar la opción LOGLEVEL para el registro de eventos.
  Dar un valor a la casilla SESSION_VALIDITY_TIME (validez de una sesión en segundos). p.e. 100, y actualizar este valor.

- ✓ En DISTRIBUCIÓN SOFTWARE

  Habilitar la opción DOWNLOAD y DEPLOY.
  Dar un valor a la casilla DOWNLOAD_PERIOD_LATENCY(tiempo de espera entre dos periodos de distribución) p.e. 30, y actualizar este valor.

- ✓ En REGISTRO

  Habilitar la opción REGISTRY (funcionalidad de extraer claves del registro), y actualizar este valor.

- ✓ En INTERFAZ

  En la casilla DOWNLOAD_PACK_DIR: Elegir la opción por default que debe ser (C:/xampp/htdocs/DOWNLOAD).

  En la casilla IPDISCOVER_IPD_DIR: Elegir la opción por default que debe ser (C:/xampp/htdocs/oscreport/IPD).

2. Tener activado el protocolo SSL, ya que cuando se descarga la información que se va a implementar se realiza un proceso crítico para la seguridad de la información, entonces este protocolo se usa con el objetivo de que si alguien logra usurpar al servidor de distribución no sea posible lanzar cualquier comandos, archivos o instalaciones no autorizadas. Por este motivo el servidor de distribución de OCS utiliza SSL.

3. Instalar en cada cliente un certificado digital para autenticarse con el servidor. Este certificado se debe guardar en un archivo llamado “cacert.pem” en el directorio donde están los archivos del cliente OCS, usualmente C:\Archivos de programa\OCS Inventory Agent, en Windows.

El certificado de autenticación utilizado en la implementación de ATH de esta utilidad de inventario fue un certificado autofirmado creado con una utilidad de creación de certificados que ofrece la herramienta XAMPP llamada makecert.bat. Si más adelante fuera necesario se podría reemplazar este certificado autofirmado por un certificado de alguna infraestructura de llave pública que posea la empresa.

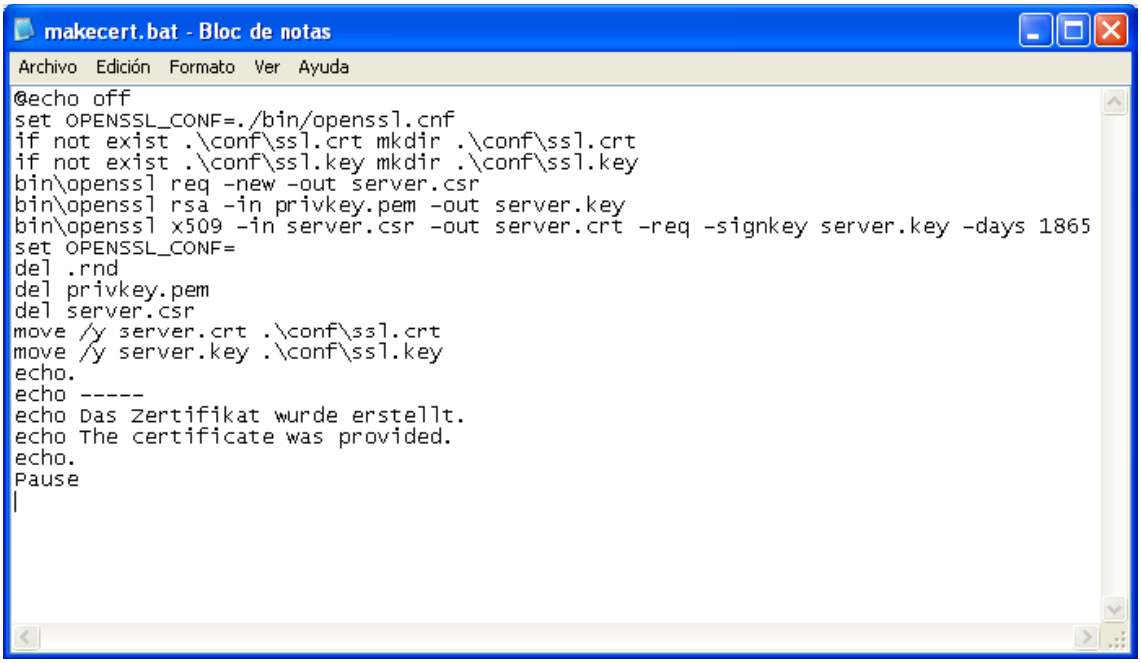
4.3.2 Certificación SSL

La certificación SSL utiliza algoritmos de cifrado para encriptar información que se transmite en una red de datos entre un servidor y un cliente. Esto quiere decir que el aspecto de la confidencialidad de la información está a salvo y la información está protegida de ser obtenida por personal no autorizado mientras esta viaja por la red. Este certificado puede ser utilizado por varios servicios web y para el caso de la implementación de OCS Inventory en ATH es utilizado por el protocolo FTP para el copiado seguro de archivos. Esta certificación está basada en un algoritmo de clave (Pública / Privada) que utiliza una clave de entre 40 y 128 bits de longitud. A medida de que la tecnología avanza estas claves poco a poco se hacen más fáciles de descifrar por esto la contramedida para este problema es aumentar el número de bits de longitud de la clave en el tiempo. Para este caso en ATH se utilizó un certificado autofirmado creado con la utilidad makecert que está disponible en la herramienta XAMPP.

4.3.2.1 Creación de un certificado autofirmado

En el servidor XAMPP se encuentra disponible un archivo de ejecución por lotes llamado “makecert.bat” para generar certificados autofirmados. Este script está localizado en el directorio de instalación del servidor XAMPP (generalmente C:\) en “\xampp\apache” y es de la siguiente forma:

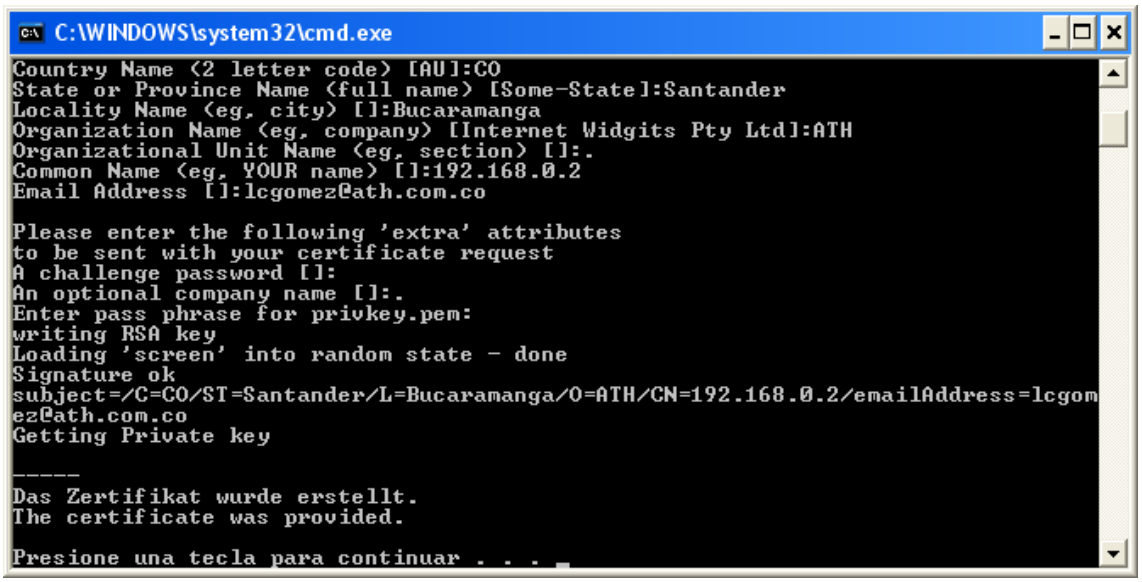
Figura 17. Script para generar archivos auto firmados, incluido en el servidor XAMPP dentro del archivo "makecert.bat"



Fuente. Autor

Este script se utilizó para generar el certificado utilizado en OCS Inventory. Este Script genera por defecto un certificado autofirmado usable por 365 días, pero en el script este parámetro es modificable por cualquier cantidad de días (nótese en la imagen que se modifico a 1865 días) "- days 1865" que son aproximadamente 5 años. Cuando se ejecuta el archivo makecert.bat, este genera la llave privada y luego pregunta por el password (de al menos 4 caracteres). Se digitó el password y se confirmó.

Figura 18. Generación del certificado auto firmado



Fuente. Autor

Después de esto se digitaron otros datos necesarios para la creación del certificado y se finaliza la creación.

Por último se tuvo que guardar en certificado server que quedo generado en el directorio xampp\apache\conf\ssl.crt\ con el nombre server.crt, en cada computador cliente en el directorio del Agente con el nombre de "cacert.pem".

4.3.3 Utilización del Servidor de Distribución

Con la opción de distribución de software se pudo hacer uso de una herramienta muy importante que ofrece OCS. Esta herramienta nos permitió Lanzar archivos ejecutables de manera remota desde el servidor OCS hacia cualquier conjunto de maquinas con el agente instalado que requirieran la instalación de determinado software, nos permitió almacenar también directorios y archivos en cualquier grupo de máquinas con el agente o ejecutar remotamente comandos SHELL también a las máquinas que fue necesario.

4.3.3.1 Funcionamiento del servidor de distribución

Un paquete tiene cuatro componentes

- ✓ Una prioridad: Esta va de 0 a 10 siendo 0 la más alta, es decir primero se implementaran las acciones de los paquetes con número de prioridad 0, después los de 1 y así sucesivamente. Hay que tener cuidado cuando se utiliza la prioridad 0 ya que si hay algún problema al implementar este paquete provocará que el resto de paquetes no sean implementados hasta que éste lo esté.

- ✓ Una acción: La acción puede ser copiar, ejecutar o lanzar. Copiar para almacenar archivos remotamente, ejecutar para enviar comandos de SHELL remotamente y lanzar para ejecutar programas.

- ✓ Un archivo con extensión .zip: Es el archivo donde comprimimos todos los archivos necesarios para la ejecución del paquete.

- ✓ Comandos opcionales para el lanzamiento de los ejecutables.

Dentro de la opción distribución de software se encuentran las sub opciones crear, activar y reglas de afectación que se explican a continuación.

4.3.3.2 Creación de un paquete de distribución

Dentro de las opciones de distribución de software la opción crear se utilizó para crear un paquete, ya fuera con el objetivo de ejecutar la instalación de un software, copiar archivos o ejecutar comandos.

Al elegir esta opción apareció una ventana web donde se pudo escoger entre las opciones de distribución copiar, lanzar o ejecutar. A continuación vemos los ejemplos de creación de paquetes con estas tres opciones.

- ✓ Ejemplo Copiar:

Configuración en la creación de paquete de copia de archivos:

- ✓ Nombre: copiar carpeta mis documentos

- ✓ Sistema Operativo: Windows
- ✓ Protocolo: HTTP
- ✓ Prioridad: 3
- ✓ Archivo (a copiar en computadores clientes): C:\Documents and Settings\Administrador\Escritorio\mis documentos.zip → es el archivo donde comprimimos todos los archivos y directorios que queremos copiar en los agentes.
- ✓ Ruta: C:\My files

Después de la configuración del paquete éste se dividió en fragmentos dependiendo de la capacidad y velocidad de la red por ejemplo en partes de 500 KB. Después de esto el paquete quedaba creado y estaba listo para ser activado.
Resultado:

Con paquetes creados como los de este ejemplo se crearon paquetes que cuando eran afectados guardaban todos los archivos y directorios dentro de la carpeta comprimida en .zip (en el ejemplo -> mis documentos.zip) en los agentes que se hizo la afectación con este paquete dentro del directorio especificado (en el ejemplo C:\My Files). En este ejemplo no existe notificación al usuario del procedimiento ya que no se configuró esa opción.

- ✓ Ejemplo lanzar

Configuración en la creación de paquete de ejecución de programas:

- ✓ Nombre: ejecutar 7zip
- ✓ Sistema Operativo: Windows
- ✓ Protocolo: HTTP
- ✓ Prioridad: 5
- ✓ Archivo (instalado en computadores clientes): C:\Documents and Settings\Administrador\Escritorio\7z465.zip →donde se encuentra el instalador
- ✓ Nombre de archivo: 7z465.exe /S /NP /DEBUG

Resultado:

Esta opción fue utilizada en los casos donde se necesitaba lanzar archivos ejecutables (en el ejemplo -> 7z465.exe que fue comprimido en un archivo llamado 7z465.zip) con

la opción de agregar opciones de ejecución adicionales como las que se muestran en el ejemplo, modo silencioso (/S), sin proxy (/NP) y modo debug o depurador habilitado (/DEBUG).

- ✓ Ejemplo ejecutar:

Configuración en la creación de paquete de ejecución de comandos:

- ✓ Nombre: configurar proxy
- ✓ Sistema Operativo: Windows
- ✓ Protocolo: HTTP
- ✓ Prioridad: 5
- ✓ Archivo (opcional, la orden "ejecutar" lo puede usar): ES OPCIONAL NO PONEMOS NADA
- ✓ Comando: Proxycfg.exe /p 192.168.1.1
- ✓ Avisar al usuario: SI
- ✓ Texto: Se cambiara el proxy
- ✓ Cuenta regresiva: 30 segundos
- ✓ El usuario puede abortar: NO
- ✓ El usuario puede esperar: NO

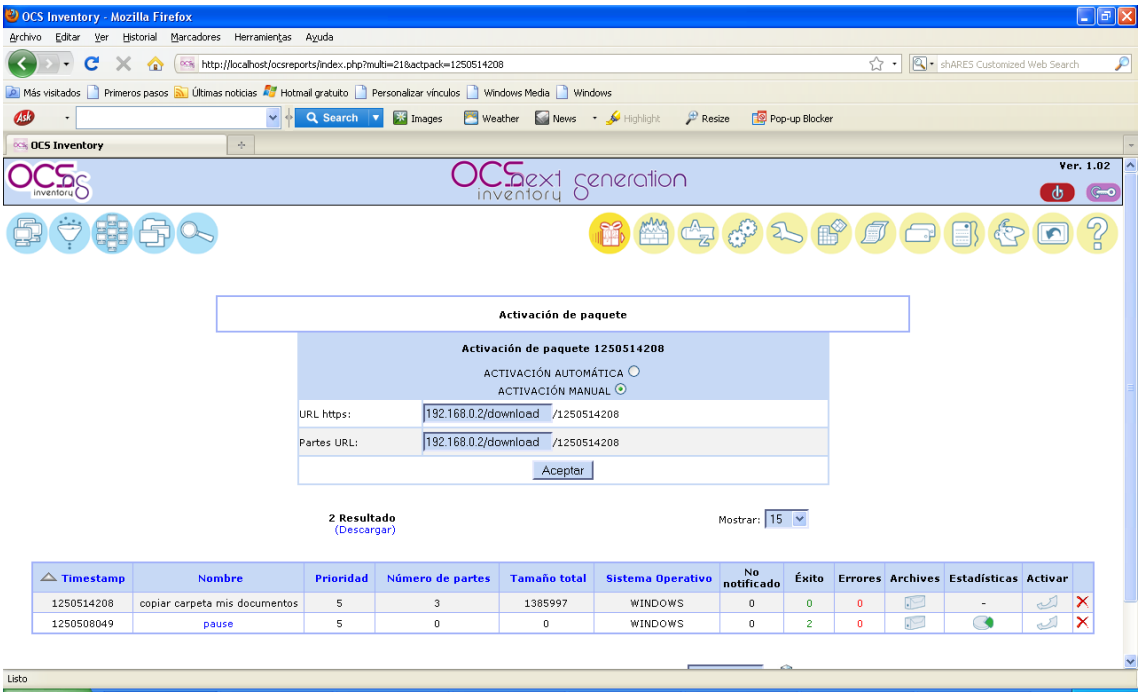
Resultado:

Con esta opción fue posible la ejecución de comandos para la realización de configuraciones o acciones en el sistema. En el ejemplo se realiza una configuración del proxy con la dirección 192.168.1.1 en los equipos cliente, dando un aviso de 30 segundos al usuario “Se cambiara el proxy” sin permitirle al usuario cancelar o retrasar la instalación.

4.3.3.3 Activación de paquetes de distribución

Después de creado un paquete fue necesario activarlo para posteriormente poderlo utilizar (afectar) sobre los computadores clientes, para esto se debe dirigir a la opción de Distribución de software y dar clic sobre la opción activar donde aparecen tanto los paquetes activos como los que faltan por activar.

Figura 19. Activación de paquetes para su implementación en OCS Inventory



Fuente. Autor

En la ventana de activación se debió digitar la URL de descarga de paquetes en el servidor donde también se descargan las partes de los paquetes, esta es por defecto IP_DEL_SERVIDOR/download y es la misma en los dos campos. Después de incluir la información en los campos y enviarlos el paquete quedó activado.

Para finalizar el proceso de distribución de paquetes se realizó el proceso de afectación de paquetes activados según el caso a equipos en particular o a equipos de forma masiva.

4.3.3.4 Afectación de paquetes de distribución en equipos clientes

- ✓ Afectación de uno en uno

Para afectar de uno en uno se accedió desde el servidor al inventario del computador que se requiera afectar y dentro de la opción mostrar todo (mostrar todo el inventario) se eligió la opción adicionar paquete, luego se eligió el paquete activado que se requería afectar, se afectó y se confirmó la operación.

Después de esto fue necesario esperar a que el servidor hiciera contacto con los clientes y que realizara la implementación del paquete. Cuando un paquete se afecta pasa al estado afectado en los equipos y aparece en estado: ESPERANDO

NOTIFICACIÓN. Después de este estado pasa al estado NOTIFICADO y por último al estado SUCCESS.

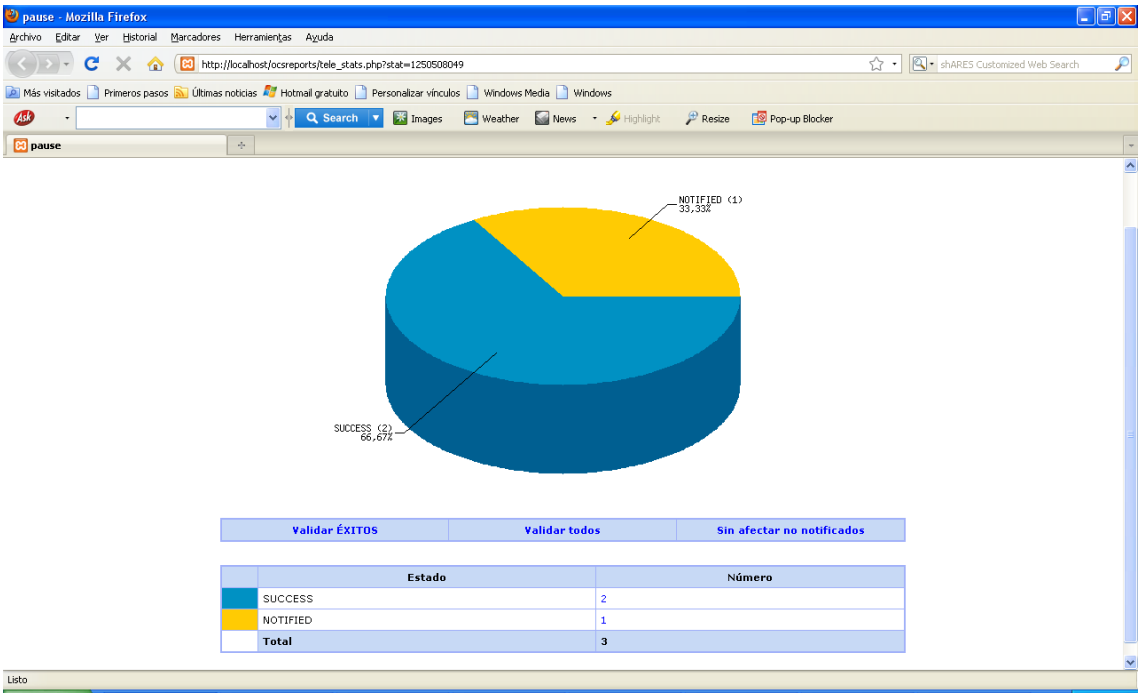
- ✓ Afectación masiva

Cuando se requirió hacer distribución de paquetes en varios computadores se utilizó la opción de creación de grupos estáticos e incluir en estos el grupo de computadores los cuales serían afectados. Después de seleccionar el grupo estático se eligió la opción adicionar paquete y luego afectar en el paquete requerido. Después de esto se realizaron los mismos pasos de la afectación de uno en uno.

4.3.4 Estadísticas de la distribución de paquetes

También se pudo hacer un seguimiento de los paquetes implementados para saber si habían hecho efecto y poder ver las estadísticas de afectación de estos. Para esto se utilizo la opción de estadísticas que se encuentra en la opción activar de la opción Distribución de software. El resultado de las estadísticas se mostro de la siguiente forma:

Figura 20. Estadísticas de la distribución de paquetes



Fuente. Autor

En el grafico se ve como se muestran las estadísticas por estado de los paquetes en cada máquina con la ayuda de una gráfica de pastel.

5. MANUAL DE MANTENIMIENTO Y SOPORTE A LA INFRAESTRUCTURA

INTRODUCCIÓN

Los computadores en la empresa A Toda Hora S.A como en casi todas las grandes y medianas empresas son un elemento fundamental ya que son útiles para la mayoría de tareas cotidianas en cualquier área de la empresa. En la actualidad casi no existe ninguna organización que no disponga de estos elementos que facilitan varias de las tareas dentro de la empresa, y estos como cualquier otro elemento tienen una vida útil que puede alargarse dependiendo del uso que se les dé y de las medidas de cuidado que se implementen para estos. Esta infraestructura tecnológica que presta diferentes servicios siempre son vulnerables a fallas que son inevitables en cuanto al hardware y el software, y cuando esto pasa siempre es importante contar con una solución eficaz y eficiente para poder continuar sin problemas con el trabajo que se está realizando haciendo uso de estos elementos, así como también implementar medidas para evitar la mayor cantidad de problemas posibles.

Los problemas en la infraestructura se pueden dividir en tres categorías:

- ✓ Problemas de hardware
- ✓ Problemas de Software
- ✓ Problemas de Redes

La experiencia y los conocimientos son muy importantes en este campo para poder actuar de la forma más adecuada en caso de algún improvisto, ya que entre más conocimiento se tenga y en forma más detallada acerca del funcionamiento de toda la infraestructura, la tecnología y el software utilizados en los sistemas es mucho más probable que se pueda escoger la mejor opción para resolver cualquier inconveniente. De cualquier modo aún si no se tiene experiencia y tampoco se cuenta con nadie que la tenga, es posible llegar a la solución de problemas que se presenten ya que en la internet, bases de datos, bibliotecas, revistas, etc., es posible encontrar foros, soluciones, manuales, trucos, libros, herramientas, o cualquier otra cosa que pueda servir como guía para poder solucionar los problemas realizando los pasos adecuados y basándose en los síntomas que presenta la infraestructura.

5.1 ÍNDICE GUÍA DE SOLUCIÓN DE PROBLEMAS DE MANTENIMIENTO DE INFRAESTRUCTURA

Tabla 5. Guía para la solución de problemas de mantenimiento y soporte a la Infraestructura

PROBLEMAS PRESENTADOS	HERRAMIENTAS Y ACCIONES A SEGUIR	DOCUMENTACIÓN
Bajo rendimiento del Sistema	perfmon.msc, taskmgr, herramientas de optimización.	Sección 5.3, 5.4.2
Alertas de error de disco	Chkdsk, diskmgmt.msc, herramientas de gestión de discos en live CD u otros	Sección 5.3
Problemas con discos	Diskpart, Diskmgmt.msc, herramientas de gestión de discos en live CD u otros	Sección 5.3
Problemas con registros de configuración del sistema	Regedit	Sección 5.3, 5.6.3.1
Se necesita diagnóstico, optimización, limpieza, configuración, monitoreo y otras tareas de administración y mantenimiento del sistema	Herramientas útiles	Sección 5.3, 5.5.2.7
Problemas con el hardware	Herramientas live CD	Sección 5.5.1.1
Problemas con controladores	devmgmt.msc, ntbtlog.txt	Sección 5.5.1.3
Problemas de inicio de Windows	CD Windows, boot.ini	Sección 5.5.2.2
Problemas con el apagado de Windows	msconfig.exe, CD de Windows, panel de control, herramienta restaurar sistema Windows	Sección 5.5.2.3
Problemas con configuraciones o instalaciones recientes que afectaron el S.O.	Herramienta restaurar sistema Windows	Sección 5.5.2.4
Daño o perdida de archivos del S.O. Windows XP	CD Windows XP (Reparar Sistema)	Sección 5.5.2.5
Daño grave del S.O	CD Windows XP (Formateo y reinstalación del sistema)	Sección 5.5.2.6
Problemas con sucesos de Windows	Eventvwr.msc	Sección 5.6.3.3

Problemas con la aplicación Outlook para correo electrónico de Microsoft	Outlook, panel de control	Sección 5.7.1
Problemas de acceso a la red mediante el explorador de Internet	Internet explorer	Sección 5.7.2

Fuente. Autor

5.2 FRECUENCIA DE LA REALIZACIÓN DEL MANTENIMIENTO

Dependiendo de las condiciones en que se encuentra la infraestructura y la exposición a factores externos así como también el uso que se le da y el comportamiento que presenta, se determina que tan seguido se debe hacer el mantenimiento preventivo de esta o cuando es necesario un mantenimiento correctivo. En las condiciones normales de una empresa el mantenimiento preventivo debe realizarse aproximadamente 1 vez al año para mantener la infraestructura en buenas condiciones técnicas de funcionamiento y se debe hacer mientras dure el ciclo de vida útil de la infraestructura ya que cuando termina el ciclo de vida útil esta ya se vuelve obsoleta y se debe realizar el cambio de esta en vez de su mantenimiento.

El mantenimiento correctivo se realiza cada vez que sea necesario, por ejemplo, cuando se presentan dificultades con aplicativos, cuando se sospecha o se tiene la seguridad de una infección de virus en el computador, cuando se presentan mensajes de fallas en el sistema operativo, cuando el computador no está funcionando de manera correcta o cuando este no funciona.

5.3 USO DE ALGUNAS HERRAMIENTAS DEL SISTEMA OPERATIVO WINDOWS XP

Para las diferentes tareas desarrolladas en la empresa, en varias ocasiones fueron de utilidad las herramientas que ofrecen los Sistemas Operativos Windows. A continuación se describen algunas de estas herramientas y los casos en los cuales fueron utilizadas para monitorear o administrar del sistema, con el fin de que este funcione de manera correcta y con la configuración de sus características acopladas a las necesidades empresariales.

- ✓ Perfmon.mcs

  Esta es una utilidad de monitoreo de rendimiento del sistema. Los elementos

principales a los cuales se realiza monitoreo con esta herramienta son: Memoria RAM, CPU y discos (lógicos y físicos).

Esta herramienta puede ser útil cuando se detecta que el equipo está consumiendo más recursos del sistema de los que debería. En este caso se procede a revisar cual es el proceso que está consumiendo recursos innecesarios para proceder a desactivarlo.

Por ejemplo en la práctica empresarial se presentó un caso donde que el computador estaba trabajando más lento de lo que normalmente trabajaba. Se procedió a hacer revisión del equipo, se ejecutó la herramienta Perfmon.msc donde se pudo ver que se estaban consumiendo demasiados recursos CPU, ya que no se estaban ejecutando aplicaciones que pudieran necesitar de este recurso y el consumo de este era de aproximadamente el 60%.

Después de esto mediante la herramienta de administración de tareas de Windows (taskmgr) se encontró que el proceso de la herramienta de navegación Firefox estaba activo y consumía más recursos CPU de los que debería consumir normalmente, luego era la que estaba generando el problema de lentitud del equipo.

Ya conociendo la fuente del problema se revisó el aplicativo Firefox y se encontró que dentro de las extensiones agregadas de este se encontraba una extensión (Messenger plus live toolbar) la cual consumía demasiados recursos innecesariamente y era la que provocaba en inconveniente de respuesta lenta del equipo cuando se ejecutaban otras aplicaciones.

Se procedió a desinstalar este agregado y a revisar de nuevo el rendimiento del sistema y se notó que efectivamente se estaban usando menos recursos de CPU por parte de la aplicación Firefox.

Como en este caso esta herramienta puede ser útil para monitorear el rendimiento de los recursos del sistema y proceder a aplicar las acciones necesarias si se presenta alguna anomalía.

- ✓ Chkdsk

Esta herramienta es usada en los casos que es necesario comprobar el estado de un disco duro, es decir, si hay errores en alguno o algunos de sus sectores, o en el sistema de archivos. A pesar de que hay muchas otras herramientas

para este tipo de comprobación esta es una que viene por defecto con la instalación del sistema operativo Windows y es una buena opción en cualquier caso.

Un ejemplo de utilización de esta herramienta del sistema durante la práctica empresarial fue en un caso del área de centro de servicios donde en un computador aparecía un mensaje advirtiendo que el disco podía tener errores y que era recomendable realizar un backup para evitar posible pérdida de datos.

Al ser reportado este error, se procedió a hacer la realización de un backup de los archivos importantes del usuario del equipo y a la revisión del estado del disco. Para esto se utilizó la herramienta chkdsk en primera instancia, donde se pudo corroborar que el disco tenía varios sectores defectuosos. Con una opción que ofrece esta misma herramienta (Examinar e intentar reparar sectores defectuosos) se intento reparar los sectores del disco pero no fue posible. Después de esto se recurrió a herramientas de live Cd como Hiren's boot CD o MiniPE para utilizar herramientas que estos incluyen de gestión de discos e intentar repararlos.

Después de tratar de reparar el disco con varias herramientas no fue posible su arreglo. Se procedió a realizar el reporte e informarle al usuario que debería hacer una petición de cambio de disco duro al área de soporte a la infraestructura para incluirlo en la lista de inventario requerido para el siguiente mes.

- ✓ Diskpart y diskmgmt.msc

Esta herramienta se puede utilizar en caso de tener discos con espacios libres para crear particiones desde el sistema operativo Windows, hacer conversiones entre formato de disco diferentes, extender volúmenes y otras opciones de administración de los discos duros. Esta herramienta es una extensión que ofrece más utilidades de administración de disco de las que se pueden encontrar en la herramienta de administración de discos gráfica de Windows el cual es accesible con el comando diskmgmt.msc.

Mediante la interfaz gráfica diskmgmt.msc es posible realizar acciones como ver propiedades de los discos, cambiar opciones de seguridad para el acceso a estos, Eliminar unidades Lógicas, desfragmentar el disco, etc. Mediante la interfaz de comandos diskpart es posible ejecutar varios comandos de los cuales algunos se describen a continuación:

- LIST [DISK|VOLUME|PARTITION]: Este comando lista dependiendo del parámetro que se le ingresa los discos, volúmenes o particiones en el computador, por ejemplo LIST VOLUME listaría los volúmenes de unidades, discos externos, y unidades de CD/DVD conectadas en el computador.

- SELECT [DISK|VOLUME|PARTITION]: Lleva el foco hacia el disco, volumen o partición del parámetro para hacer que las siguientes instrucciones ejecutadas se enfoquen en este objeto.

- CLEAN: Borra la información de configuración y toda la información del disco.

- CREATE[VOLUME|PARTITION]: Crea un nuevo volumen o partición

- REMOVE: Se utiliza para quitar letras de la unidad o volumen. Por ejemplo para eliminar el volumen D se digita remove letter D. después de eliminar el volumen el sistema Operativo no lo reconocerá y se tendrá que agregar de nuevo para acceder a él desde el sistema operativo.

✓ Regedit:

Esta herramienta es útil cuando se necesita modificar configuraciones de cualquier parámetro del sistema operativo ya que en este registro se encuentran todas las entradas de configuración de hardware, software, usuarios, seguridad, y demás elementos del sistema operativo y sus aplicaciones instaladas. Hay que tener un estricto cuidado al manipular este registro ya que si por algún motivo se realiza un cambio erróneo dentro de este puede ocasionar graves problemas, desde el no funcionamiento de cualquier aplicación en particular, hasta un daño en alguna configuración que no permita arrancar el sistema operativo.

Para evitar problemas se puede prevenir que el sistema tenga una falla después de que es modificado este registro erróneamente, para esto es necesario hacer un backup de las entradas actuales del registro cuando tiene un correcto funcionamiento y posteriormente si se puede proceder a la modificación de este.

La realización de este backup es sencilla, solo se necesita ingresar al editor de registro digitando regedit en inicio>>ejecutar, acceder al menú archivo>>Exportar,

y escoger la ubicación de disco donde se desea almacenar las entradas actuales de registro. Para volver a importar estas entradas de registro se debe ejecutar el archivo que fue guardado en disco cuando se está trabajando con privilegios administrativos y estas entradas se cargaran automáticamente al registro sobrescribiendo las que tiene en el momento y dejando la configuración del sistema como estaba cuando se exportaron las entradas.

Un ejemplo de utilización de esta utilidad en la empresa de la práctica es en la ejecución de programas de inicio, que se puede modificar mediante esta herramienta. Por ejemplo si se quiere que el programa “execute.exe” se inicia al tiempo con el sistema operativo, es decir, cada vez que el sistema se reinicie se debe ingresar al editor de registros digitando regedit en inicio>>ejecutar, y posteriormente buscar dentro del árbol de registro la siguiente carpeta:

MIPC\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Hacer clic sobre la carpeta y en la parte derecha de la ventana del editor de registros se pueden ver los ejecutables y las ubicaciones de estos, que se están iniciando con el sistema. Para eliminar alguno de estos archivos de inicio hacer clic derecho sobre él y elegir la opción eliminar. También es posible modificar o cambiar el nombre de los archivos de inicio. Para ingresar un nuevo archivo ejecutable de inicio se hace clic derecho en la parte blanca del editor de registro y debajo de los archivos que ya están agregados, se elige la opción nuevo>>valor alfanumérico, se digita el nombre y se presiona Enter. Después de esto se le da clic derecho a este archivo y se elige la opción modificar, dentro de esta opción se agrega la ubicación del archivo que se requiere agregar al inicio, en este caso execute.exe, y se hace clic en aceptar. Con esto ya queda añadido el archivo execute.exe al inicio de Windows y se iniciara cada vez que se reinicie el sistema.

Existen muchas otras herramientas tanto del sistema como otras libres o comerciales, que son útiles a la hora de la realización del mantenimiento a los Sistemas Operativos Windows. A continuación se describen algunas de estas herramientas las cuales serán nombradas o explicadas a lo largo del manual:

Tabla 6. Algunas herramientas importantes y su Utilidad

Herramienta	Sistema Operativo	Utilidad
EVEREST	Windows 95 o superior	Diagnóstico de hardware y Software
System Mechanic	Windows 2000 o superior	Optimización de equipo
Ccleaner	Windows 98 o superior	Optimización de equipo
Malwarebytes	Windows 2000 o superior	Detección y eliminación de Malware
Spyware Doctor	Windows XP o superior	Detección y eliminación de spyware
AVG	Windows 2000 o superior	Detección y eliminación de virus
Herramientas de Windows (*.msc, *.cpl y utilidades)	Windows	Configuración, monitoreo, utilidades y reparación del sistema
Hiren's boot CD	No requiere	Live CD con múltiples herramientas para mantenimiento y soporte del sistema
MiniPE	No requiere	Live CD con múltiples herramientas para mantenimiento y soporte del sistema
CD Windows	CD de instalación del sistema	Reparación o reinstalación del sistema operativo.

Fuente. Autor

5.4 MANTENIMIENTO PREVENTIVO EN LA EMPRESA

5.4.1 Frecuencia del Mantenimiento Preventivo y comparación de vida útil de la Infraestructura con o sin Mantenimiento

El mantenimiento preventivo tiene el fin de conservar los elementos IT de la empresa de la mejor forma posible para que estos tengan una mayor vida útil y funcionen de manera correcta mientras son utilizados en la empresa. La mayor parte de fallas y reducción de vida útil de los equipos por no realizar mantenimiento preventivo se debe a la acumulación de polvo en el hardware que produce recalentamiento en el sistema y puede generar cortos circuitos ya que este tiene elementos conductores, a la mala utilización de los componentes del sistema, o a malware que ataca a estos componentes. La no realización del mantenimiento preventivo hace al sistema vulnerable a fallas que se tendrán que solucionar con mantenimiento correctivo.

Este tipo de mantenimiento en la empresa ATH se realiza 1 vez al año y cuenta de varios pasos que adecuan el sistema en procura de su correcto funcionamiento y con ánimos de prevenir de la mejor forma posible la aparición de fallas que interrumpan las actividades laborales de los trabajadores.

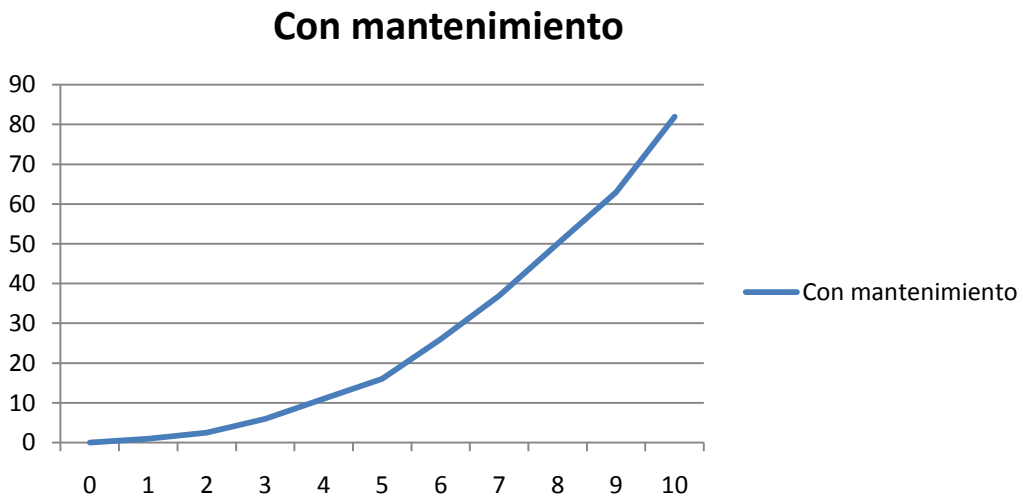
Teniendo en cuenta las condiciones ambientales en la empresa y los avances de la tecnología se puede ver un comportamiento del porcentaje de la inutilidad con respecto al tiempo de vida de los equipos similar al que se presenta a continuación, uno sin mantenimiento y otro con mantenimiento preventivo:

- ✓ Eje x: tiempo de vida útil que lleva el equipo
- ✓ Eje y: porcentaje de inutilidad del equipo

Figura 21. tiempo de vida de equipos vs inutilidad del equipo, SIN realización de mantenimiento

Fuente. Autor

Figura 22. Tiempo de vida de equipos vs inutilidad del equipo, CON realización de mantenimiento



Fuente. Autor

Podemos ver en las gráficas como con la realización de mantenimiento se reduce el riesgo de falla de los equipos y aumenta su vida útil.

5.4.2 Herramientas para el Mantenimiento Preventivo

Para cualquier labor de mantenimiento se debe utilizar la herramienta adecuada. En cuanto al mantenimiento preventivo, se pueden mencionar las siguientes que fueron utilizadas durante la práctica empresarial:

Para mantenimiento de sistema (software):

- Aplicativos para optimización que se van utilizaron: Ccleaner, System Mechanic.
- Información necesaria para cambio de passwords o usuarios.
- Aplicativos para revisión de equipo. Antivirus, antispyware, antimalware.

Para mantenimiento físico (hardware):

- Sopladora, aerosol limpia contactos, espuma limpiadora, silicona lubricante, trapo limpio, juego de destornilladores. Estos elementos se utilizan para quitar polvo y limpiar dispositivos electrónicos del computador.

5.4.3 Pasos para la realización del Mantenimiento Preventivo

1. Se debe preparar adecuadamente para el mantenimiento físico. Es recomendable usar tapabocas y uniforme de laboratorio.
2. Se retiran todos los conectores de la parte trasera del computador, y llevar la CPU a un lugar adecuado para hacer el mantenimiento.
3. Se destapa la CPU y se procede a hacer la limpieza con ayuda de la sopladora. hay que tener cuidado con los ventiladores ya que son muy sensibles y se pueden dañar fácilmente, para esto es recomendable limpiarlos con el soplador en revoluciones no tan altas y con la ayuda de un destornillador para evitar la rotación del ventilador. También se puede utilizar fácilmente la sopladora para la limpieza del teclado.
4. Se utiliza el limpia contactos para limpiar los dispositivos electrónicos (Board, tarjetas,…).

5. Se cierra la CPU y se procede a conectar los cables anteriormente desconectados.

6. Se limpian los dispositivos externos (monitores, teclado, caja,…) con el trapo y la espuma limpiadora y se lubrican con la silicona. IMPORTANTE: No limpiar pantallas LCD con espuma ni silicona ya que se pueden dañar, estos solo se deben limpiar con un trapo limpio.

7. Si se requiere se puede escanear el equipo con las herramientas antivirus y otras antimalware con que se cuente.

8. Se ejecutan las herramientas software de limpieza y optimización de equipo con que se cuenten para eliminar archivos innecesarios, reparar registro, desfragmentar disco, optimizar velocidad y funcionamiento, etc. Algunas de estas herramientas son: Ccleaner, System Mechanic, Tune Up, Clean my Registry, etc. Con estas herramientas también se desinstalan los aplicativos que no sean necesarios para el desarrollo de las actividades laborales y se eliminan los programas de inicio de Windows que no se necesiten para mejorar el rendimiento del equipo.

9. Se actualiza la información del mantenimiento (fecha, eventos, etc.). esto se puede realizar con algún software, en ATH se realiza con OCS Inventory.

10. Por último y por motivos de seguridad se hace cambio de la contraseña de administración local del equipo.

5.5 MANTENIMIENTO CORRECTIVO

5.5.1 Mantenimiento Correctivo de Hardware

Este mantenimiento se presenta cuando existe una falla física en el computador y su objetivo es reparar esta falla para continuar con el trabajo normal de la máquina. Es mantenimiento correctivo desde una pequeña soldadura para corregir un circuito hasta el cambio una tarjeta de memoria, de sonido, de video, o el cambio de un dispositivo periférico. Para realizar este tipo de mantenimiento es importante revisar primero varias posibilidades de solución para luego elegir la que se ajuste más a las necesidades económicas y de funcionamiento de los equipos en la empresa, por ejemplo, en varias ocasiones resulta mucho más económico cambiar algún dispositivo que falla por uno nuevo que el tratar de repararlo ya sea porque en la empresa hay limitaciones de tiempo y sobrecarga de trabajo, porque los elementos de reparación resultan ser más costosos y no se tienen en el inventario, o porque hay probabilidad de que con el arreglo no se repare totalmente el dispositivo.

5.5.1.1 Problemas comunes de hardware en la empresa y posible solución

- ✓ El computador no arranca (no prende): Es el error más común en el área de soporte. Repare el área de arranque (Boot) de disco duro o sistema de archivos (FAT, NTFS, etc.), verifique posible hardware defectuoso, batería de CMOS baja, actividad de un Virus o fallas de la fuente de alimentación. Puede utilizar herramientas de live CD como ayuda para chequear discos, reparar MBR, boot.ini, etc.

- ✓ Hay ruidos mecánicos extraños que vienen de adentro del computador: Revise los ventiladores y si esta es la fuente del ruido repárelos o cámbielos. Si la fuente del ruido es uno de los discos utilice una herramienta de chequeo de disco para verificar si existen sectores dañados (los sistemas operativos Windows XP cuentan con una herramienta de chequeo dando clic derecho en la unidad que se desea revisar, en propiedades, herramientas, o ejecutando el comando chkdsk desde inicio ejecutar, o si no existen muchas otras herramientas de este tipo como MHDD 4.6 o HDD Scan 3.2 que incluso pueden ejecutarse desde un Live CD), si hay problemas en el disco que no se pueden solucionar con herramientas software es preciso cambiar el disco ya que se podría presentar pérdida irrecuperable de datos, si no existe ningún problema no es necesario hacer nada ya que por el tiempo los discos tienden a volverse no silenciosos. Verificar si la causa del ruido se debe a una fuente de alimentación sobrecalentada o la CPU, si es así es necesario repararla o cambiarla porque esto ocasiona funcionamiento inestable o pérdida total del computador.

- ✓ No es posible leer CD o DVD: asegúrese de que la unidad esta correctamente conectada a los cables alimentadores dentro de la caja, si trata de leer un DVD verifique que su unidad sea lectora de CD/DVD, saque el disco, límpielo e insértelo de nuevo verificando que este del lado correcto y la puerta de la unidad está bien cerrada.

- ✓ No es posible apagar el computador con el interruptor de la caja: Este interruptor se conecta con la placa base en la mayoría de sistemas ATX y no con la fuente de alimentación como en los diseños anteriores. En los diseños modernos es recomendable apagar el equipo siempre con el sistema operativo, en el caso de Windows con inicio>>apagar el equipo, pero si no es posible se pulsa el botón de apagado por unos segundos hasta que se apague el equipo. Si esto no funciona verifique que el botón de apagado este haciendo contacto con el interruptor de la placa base guiándose con el manual de esta.

- ✓ No puede utilizar puertos frontales: Si los cables de extensión que conectan a estos con la placa base no están bien conectados los puertos no funcionarán. Compruebe que estos puertos estén habilitados en la BIOS.

- ✓ No funciona algún dispositivo periférico (monitor, teclado, mouse, etc.): los fallos más comunes de este tipo se presentan en la parte trasera del computador con los cables periféricos. Verifique que todos los cables del computador estén bien conectados, los cables serie, paralelos y VGA utilizan tornillos que se aprietan manualmente y si no están bien conectados podrían causar fallos intermitentes o completos en el hardware. Al desconectar los cables de los dispositivos diferentes a los USB o IEEE-1394 es necesario reiniciar el sistema operativo para que el equipo vuelva a identificar el hardware conectado. Cuando conecte los cables a los puertos de la parte trasera del computador evite que se enreden porque pueden provocar un mal funcionamiento de los dispositivos externos, como la impresora y el monitor. Los cables enredados también causan tensión a los puertos y podrían darse mal funciones o fallos de puerto. Verifique también si los controladores de los dispositivos están instalados, para esto en Windows XP puede dar clic derecho en mi PC, administrar, administrador de dispositivos y verificar los drivers que hacen falta por instalar.

- ✓ El monitor cambia de colores y se torna verde, rojo o azul: esto se presenta cuando no hay buena conexión entre el monitor y el puerto VGA. La mayoría de veces es por causa de mala conexión del cable del monitor en alguno de sus lados o simplemente que este cable está dañado. Verifique que el cable este bien conectado o intente cambiando el cable. Si nada de esto funciona puede ser que el problema sea un daño más grave en la tarjeta de video o el puerto de conexión del dispositivo y en ese caso sería conveniente cambiar la tarjeta.

- ✓ No funciona o funciona mal el mouse: Si el mouse es mecánico (de los que tienen una esfera en la parte inferior) es posible destaparlo fácilmente con la ayuda de un destornillador y limpiarlo, ya que estos con el tiempo acumulan polvo en el interior (en la esfera o en las ruedas generadoras de pulso por su movimiento) provocando malos funcionamientos de este.

- ✓ El modem no logra conectarse a internet o lo hace y a los minutos se desconecta:
  después de una tormenta eléctrica es posible que se queme el módem, no es confiable el diagnostico de Windows sobre los módems instalados, en este caso es recomendable que cambie el módem.

- ✓ Hay sobrecalentamiento: Los fallos de los ventiladores de la fuente de alimentación, de los procesadores, del chip “puente Norte” o los de la tarjeta de video pueden provocar sobrecalentamiento y pueden dañar los componentes. La solución a estos problemas es la mayoría de veces una limpieza a los ventiladores ya que debido al acumulamiento de polvo dentro de estos puede que la energía que utilizan no alcance para moverse y se traben.

- ✓ Fallas en ventiladores: Cuando alguno(s) del los ventiladores no funcionan es necesario repararlo o cambiarlo. Algunos ventiladores son fáciles de desarmar y reparar simplemente quitándoles el polvo y limpiándolos con aceite 3 en 1. Si no es posible repararlo se debe cambiar por uno de las mismas dimensiones y que trabaje con el mismo voltaje que el dañado, esto se realiza fácilmente con la ayuda de un cortafrío y cinta aislante.

- ✓ Tarjetas sueltas: Hay que verificar que todas las tarjetas (video, memorias,…) estén debidamente conectadas dentro del computador ya que de lo contrario se presentarían fallos indeseables de funcionamiento. Algunos concejos para prevenir esto son: Asegurarse de que el soporte de las tarjetas este a ras con la pared trasera de la caja, que el conector este bien metido en la ranura, que la tarjeta que insertamos efectivamente sea del slot que utilizamos.

- ✓ No se puede encender el computador: Un procesador o un modulo de memoria mal instalados pueden causar que el computador no encienda.

- ✓ Fallos en la batería: La batería mantiene los ajustes configurados en la BIOS, estos ajustes se almacenan en la memoria CMOS. Si la batería se agota (dura unos tres o cuatro años) se perderán estos ajustes. Si este es el caso cambie la batería.

- ✓ Fallo en el chip BIOS: El chip BIOS puede destruirse por una descarga electrostática (ESD) o por descargas de rayos, pero también pueden quedar obsoletos. Mientras que algunos sistemas utilizan chip BIOS conectado mediante zócalos en otros está soldado. En ambos casos existen actualizaciones para el software de la BIOS con nuevas funciones como soporte para procesadores y hardware recientes.

5.5.1.2 Prevención de descargas electrostáticas al realizar Mantenimiento correctivo de hardware

Hay que tener en cuenta ciertos cuidados cuando se destapa un computador para realizar cualquier mantenimiento hardware ya que existe el peligro de las descargas electrostáticas ESD que se presentan cuando dos elementos con diferente potencia eléctrica hacen contacto o se acercan demasiado el uno del otro. La mayoría de ocasiones estas descargas ESD son imperceptibles ya que para darse cuenta de una descarga de estas se necesitaría que se generara una chispa, y así la descarga fuera visible, pero para que aparezca una chispa tendría que presentarse una descarga de más de 800 voltios. Tan solo basta con una descarga de 100 voltios para dañar una placa de memoria, una CPU o cualquier otro elemento electrónico del computador. Para evitar este peligro existen pasos que se pueden seguir al abrir un computador:

- ✓ Utilizar limpiadores antiestáticos.

- ✓ Utilizar prendas de algodón u otras fibras naturales al trabajar en el computador para evitar generar electricidad estática.

- ✓ Utilizar dispositivos anti-ESD del mercado como pulseras, pinzas de cocodrilo o alfombrillas anti estáticas. Se deben conectar las pinzas al computador después de que se haya desenchufado. Así se igualara la potencia eléctrica del cuerpo con la del computador para evitar descargas electrostáticas.

- ✓ Tomar los componentes del computador por los soporte y tratar de evitar tocar los circuitos de las placas o los conectores energía y datos.

5.5.1.3 Solución de problemas con controladores y conflictos hardware

Al instalar cualquier dispositivo físico con el sistema como tarjetas, impresoras, etc. Es necesario instalar el software de controlador que es el encargado de realizar una interfaz de comunicación entre el dispositivo y el hardware para que estos interactúen y el dispositivo funcione correctamente con los recursos necesarios del sistema. Es posible que en ocasiones se presenten conflictos o problemas con los dispositivos y sus controladores.

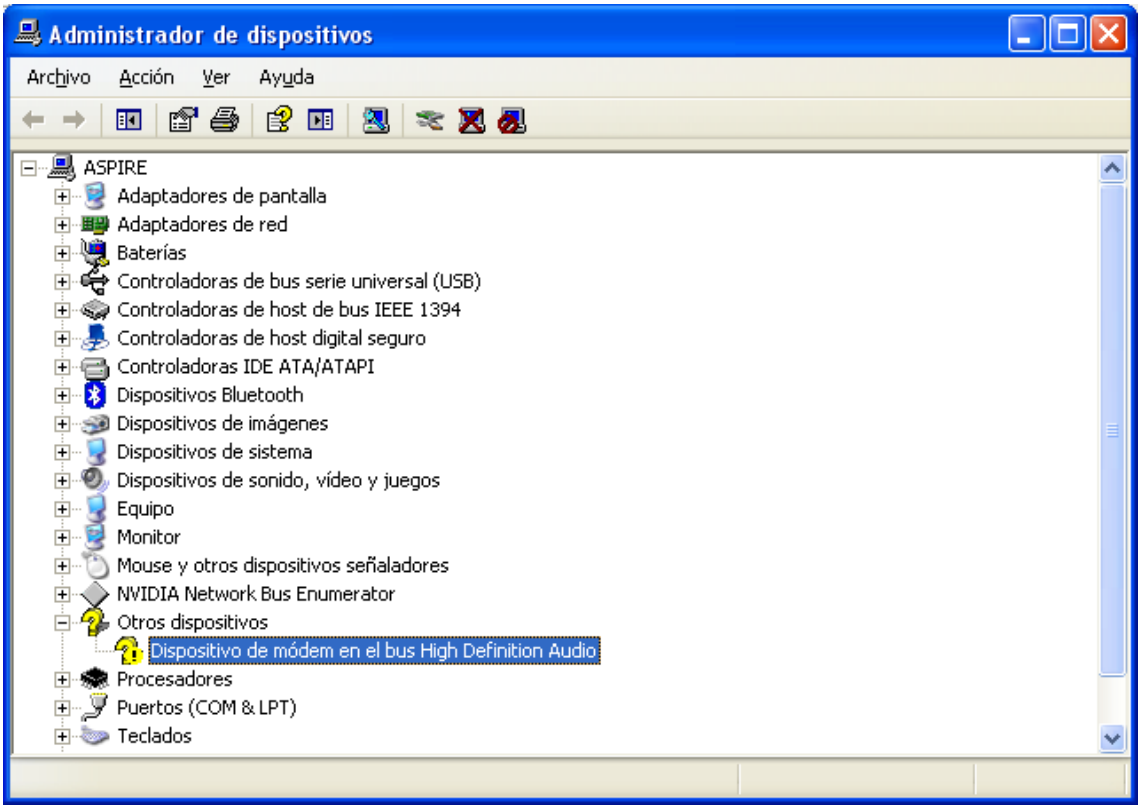
Una interrupción es una línea que une el periférico al procesador. Una interrupción es de hardware cuando es solicitada por uno de los componentes de físicos del computador. Por ejemplo, este es el caso al tocar una tecla y que el teclado llama la

atención del procesador sobre este hecho. No obstante, los 256 interruptores no pueden ser solicitados al mismo tiempo ya que se interrumpe el hardware y los diferentes periféricos siempre realizan interrupciones muy específicas. Por lo tanto, al instalar las tarjetas de expansión, debe asegurarse que, durante la configuración, el mismo interruptor no se utilice para dos periféricos diferentes. Si esto sucediera, ocurriría un "conflicto del hardware" y ningún periférico funcionaria. Verdaderamente, si dos periféricos utilizan el mismo interruptor, el sistema no sabrá cómo distinguirlos. Un conflicto del hardware no sucede únicamente cuando dos periféricos poseen el mismo tipo de hardware, también puede ocurrir un conflicto cuando dos periféricos poseen la misma dirección E/S o usan los mismos canales DMA.

La solución de conflictos de hardware y problemas con controladores se puede resolver de la siguiente forma:

Acceda a Panel de control>> Sistema>> Hardware >> Administrador de Dispositivos. También es posible ingresar al administrador de dispositivos digitando el comando devmgmt.msc en Inicio>>Ejecutar.

Figura 23. Administrador de Dispositivos



Fuente. Autor

Si algún dispositivo tiene problemas, se podrá ver a su lado un símbolo de interrogación junto con otro símbolo de menor tamaño, el cual indica si el dispositivo muestra algún problema:

- ✓ Un signo de exclamación (!) en negro indica que hay un problema con el dispositivo. Puede que incluso si el dispositivo advierte problemas este esté funcionando. Dando clic derecho en el dispositivo con problema en la opción propiedades se puede ver el código del problema para poder intentar resolverlo.

- ✓ Una letra "X" en rojo indica que el dispositivo está deshabilitado. Los dispositivos deshabilitados se encuentran conectados físicamente al equipo pero no pueden cumplir sus funciones y no pueden ser utilizados hasta que se vuelvan a habilitar en el sistema operativo.

- ✓ Una letra "i" en azul dentro de un campo blanco en un recurso de dispositivo de las propiedades del equipo indica que no se ha activado la característica Usar configuración automática para el dispositivo y que el recurso se seleccionó manualmente. Tenga en cuenta que esto no indica que el dispositivo tiene un problema o está deshabilitado.

Una causa por la cual no pueda estar funcionando un dispositivo es simplemente porque aún no se han instalado los drivers para éste. En tal caso veremos en el dispositivo el signo (!) y al revisar en las propiedades del dispositivo la causa del problema veremos: Error No están instalados los controladores para este dispositivo. (Código 28). En este caso debemos instalar los drivers con el CD de instalación si se tiene o descargándolos por internet dependiendo del sistema operativo que se utilice (en este caso XP).

Figura 24. Error código 28. No están instalados los controladores para el dispositivo

Fuente. Autor

Al hacer clic en las propiedades de un dispositivo específico se muestran varias pestañas donde se puede revisar varias características y el estado de este en el sistema. Dependiendo del tipo de dispositivo se mostrarán las pestañas de información las cuales pueden ser: General (detalles generales del dispositivo), Recursos (recursos del sistema disponibles para el dispositivo), Controlador (detalles del controlador del dispositivo) y Configuración (opciones de configuración).

En la opción Recursos se puede encontrar un cuadro que contiene una lista de dispositivos en conflicto si es que se presentan conflictos. Esta lista indica el conflicto con el código de error.

En la opción de chequeo Usar configuración automática si el sistema operativo Windows detecta el dispositivo correctamente, la casilla debe estar activada y el dispositivo debería funcionar correctamente. Si no es así, y se presenta algún conflicto es posible cambiar la configuración básica que está basada en un número de 0 a 9 por otra configuración, puede ser necesario cambiar la configuración seleccionando una configuración básica diferente en la lista. Si la configuración específica que desea para el dispositivo no se muestra como configuración básica, quizás sea posible hacer clic en el botón Cambiar configuración para ajustar manualmente los valores de recursos. Por ejemplo, para editar la configuración de Intervalo de entrada y salida:

- ✓ Desactivar la opción de verificación Usar configuración automática.

- ✓ Hacer clic en Cambiar configuración.

- ✓ Hacer clic en la opción de intervalo de entrada y salida adecuado para el dispositivo.

Si el problema persiste es recomendable comunicarse con el fabricante de la placa base para consultar la opción de una actualización de la BIOS.

El registro de inicio de Windows también puede ser útil a la hora de verificar problemas con los controladores de los dispositivos. El archivo de registro de inicio de Windows XP (ntbtlog.txt) es un archivo de texto con un listado de los controladores que se cargan o no en el proceso de inicio del sistema y puede servir en un momento determinado para resolver problemas con los controladores de dispositivos. Como Windows XP añade entradas al archivo ntbtlog cada vez que inicia el sistema con el registro de inicio habilitado, siga este procedimiento para poder utilizarlo en la localización y resolución de problemas:

1. Cree un registro de inicio cuando haya instalado un Windows XP con éxito.

2. Utilice la opción de búsqueda para localizar el archivo ntbtlog.txt, este por defecto se encuentra en la carpeta C:/WINDOWS y cambie el nombre a otro, por ejemplo bootlog.txt.

3. Si no encuentra el archivo cree uno habilitando el registro de inicio de Windows. Para ello, justo antes de que arranque Windows pulse la tecla F8, aparecerá un menú. Ahí elija la opción Habilitar Registro de Inicio y la instalación de Windows en la que lo quiere hacer (aunque por defecto sólo hay una). Ahora realice el paso 2.

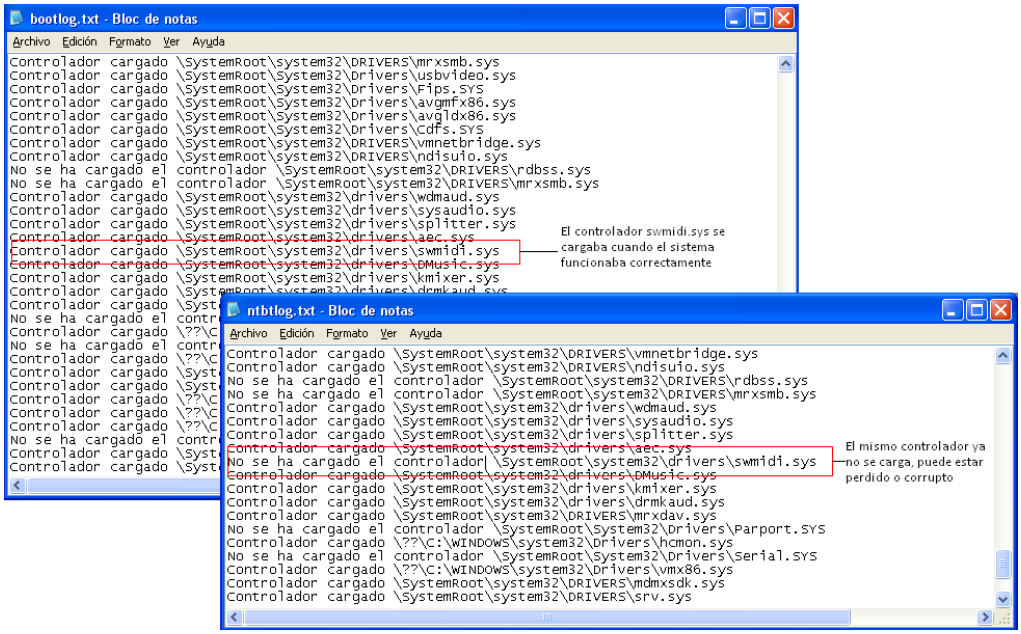
4. Siempre que instale un nuevo hardware y el equipo funcione correctamente, elimine los archivos ntbtlog.txt y bootlog.txt y cree un nuevo archivo bootlog como se describe en los pasos 1 y 2.

5. Cuando exista alguna falla de inicio que puede ser causa de un controlador por ejemplo después de instalar incorrectamente un dispositivo nuevo o cuando necesite verificar si se están cargando todos los drivers normalmente, cree un nuevo registro de inicio como en el paso 3.

6. Reinicie Windows XP en modo seguro y abra bootlog.txt (el registro original que guardamos cuando no habían fallas) y el nuevo archivo ntbtlog.txt que acabamos de generar (muestra el estado actual del computador). Compare los

dos archivos, si hay más de una sección en ntbtlog.txt vaya a la sección encabezada con la fecha y hora de la última creación del registro de inicio.

Figura 25. Archivo de registro de inicio de Windows ntbtlog.txt



Fuente. Autor

7. Compare el registro de inicio original con el más reciente y mire cual es el controlador que ya no se carga. Para volver a instalar un driver hágalo desde el administrador de dispositivos de Windows o descárguelo en internet y ejecútelo localmente.

Para realizar este tipo de tareas de manera más cómoda también existen herramientas como Driver Scanner 2009 o Drivercure o utilice el servicio de Windows Update para actualizar los drivers.

5.5.2 Mantenimiento Correctivo de Software

Mediante el mantenimiento correctivo de Software fue posible solucionar los problemas que se pudieran presentar en los sistemas operativos empresariales o en las aplicaciones sobre estos.

5.5.2.1 Proceso de inicio del Sistema Windows XP

Si el sistema operativo no carga y arranca ninguna de las utilidades del computador

estarán disponibles para ser usadas ya que el sistema operativo es el encargado de controlar los dispositivos, los procesos de las aplicaciones y realizar asignación de recursos. Si el computador completa satisfactoriamente la rutina POST de la BIOS y Windows no arranca puede que se esté presentando uno de los siguientes problemas:

- ✓ Los archivos de arranque están corruptos o el sistema está intentando arrancar desde un disco que no tiene estos archivos.

- ✓ Hay una configuración incorrecta del disco duro en la BIOS del sistema.

- ✓ Hay archivos de Windows o de aplicación dañados o perdidos y que el sistema operativo necesite para arrancar.

- ✓ Hay conflictos de recursos hardware.

- ✓ Hay un virus que modifico la configuración de arranque del sistema impidiendo su inicio normal.

Vista General de los procesos de arranque de la BIOS y el sistema operativo Windows:

La secuencia básica desde que se presiona el interruptor de encendido del computador hasta que se accede al escritorio del sistema operativo es el siguiente:

- o Al presionar el interruptor de encendido del computador se ejecuta en la BIOS el proceso de auto test de encendido POST para asegurarse de que el hardware funciona correctamente. Si existen problemas detectados se verán en pantalla mensajes de error o se oirán códigos sonoros de error indicando cual es el problema, que pueden ser traducidos con el manual de códigos para la BIOS que se esté utilizando.

- o La BIOS busca dispositivos Plug and Play en la placa base y slots de expansión y les asigna recursos hardware.

- o La BIOS busca en el hardware chips de memoria ROM en tarjetas de video y tarjetas de expansión y ejecuta los programas de estos chips para habilitar los dispositivos.

- La BIOS prueba la memoria del sistema en busca de errores.

- La BIOS busca archivos de arranque de sistema operativo en la primera unidad de arranque listada de la configuración de la BIOS. La unidad puede ser un disco flexible, unidad de CD-ROM o un disco duro ATA/IDE. Este proceso es conocido como bootstrapping.

- Si no encuentra esta información en la primera unidad continuará buscando en la lista siguiendo el orden hasta encontrar un archivo de arranque. Si no lo encuentra el sistema mostrará un mensaje de error del tipo “Non-System Disk o Disk Error” (No hay disco o Error de disco) o “Disk Boot Failure” (Fallo en el arranque del disco).

- La BIOS localiza la unidad de arranque y ejecuta las instrucciones para iniciar el sistema operativo.

- Durante el proceso de inicio del sistema operativo este carga los controladores en la memoria para los dispositivos instalados y ejecuta los procesos de inicio configurados para el computador. Al mismo tiempo muestra la pantalla de inicio de sesión si está configurado para esto o de lo contrario accede al escritorio.

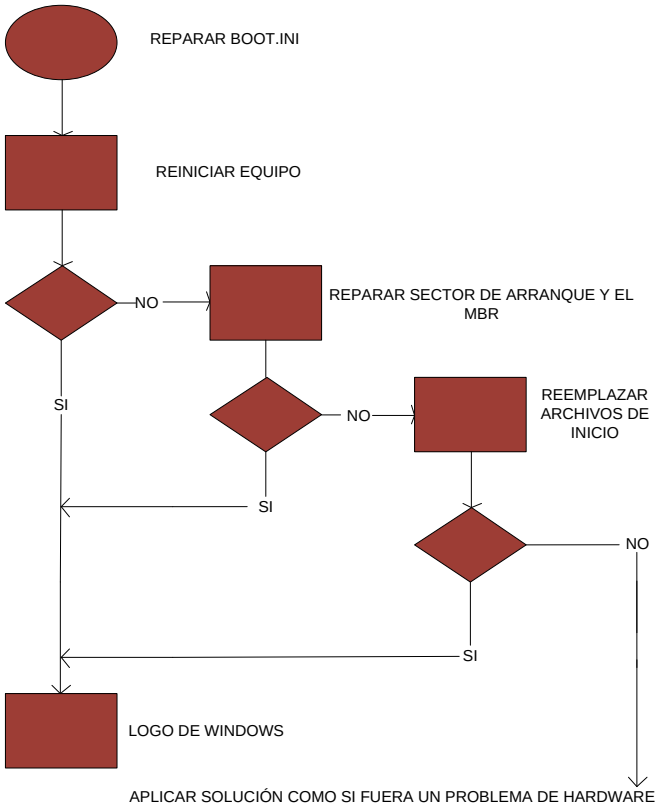
Se debe tener cuidado cuando se realiza un cambio en la configuración de la BIOS o el sistema operativo ya que una mala configuración en valores de estas opciones puede provocar fallas en el arranque del sistema.

5.5.2.2 Solución de problemas de inicio del Sistema Operativo Windows XP

- ✓ Reparar un problema de inicio cuando no aparece logo de Windows en XP

  Solucionar uno de estos errores es más exigente que hacerlo cuando el sistema operativo ya está en ejecución, ya que no es posible acceder al juego completo de herramientas incluidas en Windows para el mantenimiento. Para corregir el error se sigue el siguiente diagrama de flujo.

Figura 26. Diagrama de flujo para solución de problemas de inicio En Windows XP



Fuente. Autor

Si al encender el computador se muestra un mensaje de error que anunciando la ausencia de sistema operativo o del registro de arranque IDE-0, y no hay ningún disquete insertado (que impediría el inicio normal del S.O) puede haber un problema con los archivos de arranque del sistema operativo en el disco duro. Para determinar si la falla es por el registro principal de arranque o por pérdida de archivos de arranque se debe revisar el mensaje de error del sistema. Dependiendo del mensaje de error en la pantalla es posible deducir el problema. Si el problema es un registro principal de arranque (MBR) no válido el mensaje será del tipo “No Boot Sector on Fixed Disk” o “No Boot Device Available” (esto es no ha encontrado el sector o el dispositivo de arranque), el MBR está corrupto. Si el problema es la perdida de archivos de arranque del sistema el mensaje será del tipo “Non-System Disk or Disk error” o “Invalid System Disk” (Esto es ausencia o error de disco o disco invalido), el MBR está bien pero los archivos de arranque se han perdido o están corruptos.

- ✓ Reparar archivos de arranque del sistema. Archivo ntldr y boot.ini

El ntldr es el archivo responsable de realizar la carga del sistema operativo Windows en sus versiones NT, incluyendo a XP Y Server 2003. Este archivo se

encuentra almacenado en la raíz del disco que contiene el sistema operativo (habitualmente el disco C:) y requiere del archivo boot.ini para tomar los parámetros de carga del sistema. Si el sistema no encuentra en el disco configurado para el inicio el archivo ntdlr, el computador lo advertirá con un mensaje de error en pantalla. Para reinstalar este archivo en caso de su pérdida se debe proceder a la restauración del sistema operativo.

Acciones como por ejemplo iniciar desde un sistema operativo instalado en un disco agregado diferente al principal pueden afectar la información de arranque del archivo boot.ini dando como resultado la disfuncionalidad del sistema al no poder arrancar. El boot.ini contiene las instrucciones de inicio de sistema y discos que Ntldr usa para mostrar en pantalla el menú de sistemas operativos (si hay dos o más sistemas instalados o si se pulsa la tecla F8) o iniciar directamente el sistema operativo. Si no aparece el menú o no se localiza e inicia el sistema operativo cuando debería, puede ser necesario editar o reemplazar el archivo boot.ini. En este archivo se encuentra estructurada la información de disco de inicio, partición de inicio, ruta de inicio y opciones de inicio del sistema operativo Windows, y admite la configuración de una entrada por cada sistema operativo instalado en diferentes particiones.

El archivo boot.ini se encuentra ubicado en la raíz del disco que contiene el sistema operativo y por defecto se encuentra oculto por el sistema operativo. Este es un archivo de texto y por lo tanto es posible su lectura y modificación con la ayuda del bloc de notas de Windows u otro editor de texto. Este archivo es esencial para el arranque del sistema operativo, por eso hay que tener cuidado cuando se le realice una modificación y por seguridad es recomendable también guardar una copia con la configuración inicial en un disco diferente al del sistema operativo. En principio, ese archivo no tiene por qué ser modificado manualmente pero es posible realizar modificaciones que para corregir su funcionamiento.

- NTLDR, se encarga de cargar el sistema operativo.
- boot.ini, contiene la lista de opciones de inicio.

Una forma de reparar este archivo es iniciar el computador desde el CD de Windows XP, iniciar la consola de recuperación del CD y después ejecutar la herramienta Bootcfg.exe que permite la generación de un nuevo archivo Boot.ini. Esto se realiza mediante los pasos mencionados a continuación:

1. Encender el equipo con el de Windows XP dentro de la unidad de CD e iniciar el sistema desde el CD, en la ventana de instalación presionar R para iniciar la consola de recuperación de Windows.

2. En la consola de recuperación digitar el comando: bootcfg /list, y presionar la tecla ENTER. Esto mostrará las entradas que tiene el archivo en el momento de la ejecución del comando si es que existe alguna.

3. Para crear un nuevo archivo boot.ini ejecutar el comando: bootcfg /rebuild, y presionar ENTER. Este comando mostrará las instalaciones de Windows identificadas en las particiones y da la opción de elegir si se van a agregar a las opciones de inicio, se eligen las entradas de sistema operativo que se requieran y luego se digita ENTER.

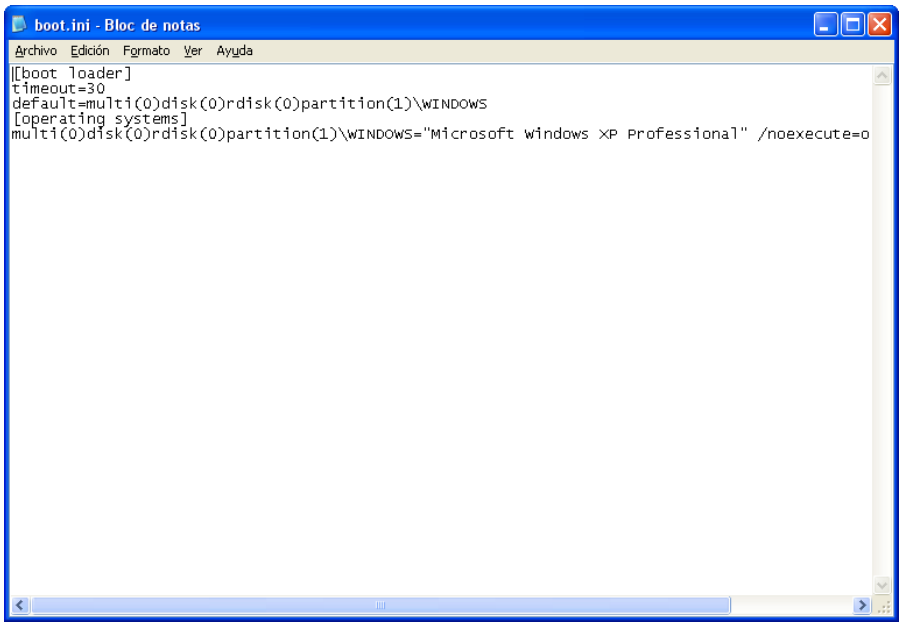
4. Para finalizar el proceso de regeneración del boot.ini se debe digitar exit, presionar ENTER, sacar el CD de Windows y reiniciar el computador.

Este archivo también se puede editar manualmente conociendo su estructura.

- ✓ **Estructura del archivo boot.ini**

Para poder ver y editar este archivo que por defecto se encuentra en la raíz del disco C: se debe deshabilitar la opción de ocultar archivos protegidos del sistema operativo en Herramientas>>Opciones de carpeta>>ver, y se desmarca el check box que oculta estos archivos. También es posible editar este archivo incluso cuando no ha arrancado el sistema operativo, iniciando el sistema con ayuda de un CD vivo (live CD) que tenga cualquier herramienta de edición de texto. Es recomendable por seguridad hacer una copia de este archivo antes de modificarlo.

Figura 27. Archivo boot.ini



Fuente. Autor

El archivo boot.ini contiene dos tipos de información, la [boot loader] donde se encuentran los parámetros de las particiones de inicio del sistema operativo, y está el valor del tiempo en segundos que permanece en pantalla la lista de sistemas para la elección hasta que se arranque el sistema operativo configurado por defecto si hay varias opciones de arranque (timeout), y la [operating systems] es la información del sistema operativo que se encuentra en la partición y con opciones de ejecución. Si al valor de timeout se le da un valor de 0 se cargará siempre el sistema operativo por defecto sin retraso, si se le da un valor de -1 mostrará indefinidamente el menú de elección de sistema operativo hasta que se elija alguno. El archivo ntldr también es el encargado de mostrar el menú con el listado de posibles los sistemas operativos a cargar para que el usuario elija cual desea cargar y si solo existe una opción de sistema operativo no mostrará este listado y cargará el sistema único.

La sección de [boot loader] tiene parámetros de la siguiente forma:

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Los valores numéricos de esta línea expresan valores de configuración como se muestra a continuación representados con las variables W, X, Y y Z.

multi(W)disk(X)rdisk(Y)partition(Z)

- W es un número de control que indica a donde pasa el control la BIOS para que el archivo ntldr realice la carga del sistema operativo. Usualmente su valor es 0.

- X tiene siempre el valor '0' cuando está el parámetro multi.

- Y Indica cual disco duro contiene los archivos del sistema operativo. Para discos ATA los valores son de 0 a 3, y para discos SCSI son de 0 a 7 o de 0 a 15 dependiendo del tipo de adaptador.

- Z Es la partición del disco duro del parámetro Y donde se encuentra el archivo principal del kernel de Windows *Ntoskrnl.exe* para la carga del sistema operativo. El primer valor válido es '1'.

✓ **El Master Boot Record:**

El registro de arranque maestro (Master Boot Record), es un sector de 512 bytes al principio del área de almacenamiento en un disco duro donde se encuentra la información de las particiones del disco y desde cuales es posible arrancar un sistema operativo. Este archivo es frecuentemente un objetivo de los virus informáticos por ser indispensable en la carga del sistema operativo, por este motivo se podría presentar modificaciones a este y la generación de errores en la carga del sistema.

Si el MBR del disco está dañado, el computador no lo puede leer para saber cómo está particionada la unidad ni la localización de los archivos de arranque del sistema operativo.

Para éste problema se puede utilizar el CD de instalación del Windows XP para arrancar el equipo, y después de esto para el disco de la instalación que se quiere reparar en la consola de recuperación, se digita el comando FIXBOOT [disco a reparar] (por ejemplo FIXBOOT D:) para crear un nuevo sector de arranque en la unidad seguido del comando FIXMBR [disco a reparar] para crear o reparar el MBR en el disco a reparar.

También existen otras herramientas en la web, la mayoría gratuitas, como MBRtool que permite manipular el MBR y facilita la tarea de configuración del arranque de Windows.

Otra posibilidad de que el sistema no encuentre el MBR, es que no esté bien configurada la unidad de disco que lo contiene en la BIOS, y esta no puede leer el registro principal de arranque correctamente.

Para revisar este problema acceda a la configuración de la BIOS, si está la configuración definida por el usuario (User-Defined) con el modo LBA habilitado o en Auto, debería poder arrancar la unidad cuando se repare el MBR o se restauren los archivos de arranque. Si el modo LBA no está habilitado no podrá arrancar desde la unidad porque no podrá encontrar los sectores de arranque. Copie los ajustes de configuración de la unidad, restablezca la autoconfiguración, guarde los cambios y reinicie el sistema. Si se hace la configuración de BIOS automáticamente (por DEFAULT) y sigue presentando problemas de arranque o mensajes de error, lo más probable es que haya un problema con los archivos de sector de arranque de la unidad y no con la configuración de la BIOS y se deberá centrar la atención en el sector de arranque del disco.

5.5.2.3 Problemas comunes en el proceso de apagado de Windows XP y posibles soluciones.

A continuación listan los posibles problemas que pueden presentarse al intentar apagar el equipo con Windows XP y sus respectivas posibles soluciones.

- ✓ Si se muestra un mensaje de error cuando se apaga o reinicia el equipo

SOLUCIONES

a) configurar Windows para que no cargue el archivo o el servicio mencionado en el mensaje de error

Si el mensaje de error hace referencia a un archivo o servicio que ya no se encuentra disponible pero aún se tiene registro de él en los servicios de inicio, es posible que este se encuentre activado en la utilidad de configuración del sistema: inicio>>ejecutar>>msconfig.exe. Si aparece el archivo o servicio desactívelo desmarcándolo del Checkbox.

b) ver si se ha eliminado recientemente y de manera incorrecta algún programa del equipo

Si eliminó algún programa o componente del sistema operativo recientemente de forma manual, los registros y la información de este que no se elimino correctamente del equipo puede ocasionar el problema. Reinstale el programa o componente y, a continuación, utilice la herramienta Agregar o quitar

programas del panel de control o siga las instrucciones del fabricante para quitarlo.

Para eliminar correctamente el programa o componente del equipo con toda su información se realizan los siguientes pasos:

Haga clic en Inicio>>Panel de control>> Agregar o quitar programas. En la lista, elija el programa a eliminar y haga clic en Cambiar o quitar. Acepte cuando se solicite la confirmación de eliminación.

Si el programa no aparece en la herramienta Agregar o quitar programas, se pueden utilizar herramientas de optimización de equipo como (TuneUp, Ccleaner, etc.) para tratar de remover los archivos innecesarios del sistema. Si no se repara el problema póngase en contacto con el fabricante del software para obtener instrucciones para quitarlo.

- ✓ El equipo se paraliza y no responde después de intentar apagarlo o reiniciarlo

SOLUCIONES

a) Ejecutar el sistema utilizando el modo seguro de Windows e intentar apagarlo desde ahí

Inicie el sistema en modo seguro. Para esto ingrese a inicio>>ejecutar, digite el comando msconfig para ingresar a la utilidad de configuración del sistema y en la pestaña BOOT.INI, habilite la opción /SAFEBOOT y reinicie el equipo. Otra forma de iniciar en este modo es al reiniciar el equipo, para esto presione la tecla F8 cuando reinicie y seleccione la opción de inicio en modo seguro. Si es posible apagar el equipo de este modo pase al punto a continuación para intentar solucionar los posibles problemas con el con los controladores.

b) revisar el administrador de dispositivos de Windows para verificar si el problema se relaciona con los controladores de algún dispositivo conectado

Utilice el administrador de dispositivos para verificar la configuración mediante software que tienen esta y si están presentando problemas. Se debe tener en cuenta que hay dispositivos como discos duros u otros que tienen que ser configurados manualmente por ejemplo cuando el equipo utiliza interruptores DIP o clavijas de puente, y no por medio de software de configuración.

c) Utilizar la opción de restaurar el sistema que tiene Windows para intentar volver a la una configuración guardada del sistema que funcionaba correctamente

Esta herramienta es accesible haciendo clic en Inicio>>Todos los Programas>> Accesorios>>Herramientas del Sistema>>Restaurar Sistema. Esta herramienta devuelve el sistema operativo a una configuración guardada anteriormente (punto de restauración) de archivos críticos del sistema y algunos archivos de programa. En cualquier momento que se desee se pueden guardar estos puntos de restauración que luego pueden ser utilizados para devolver el sistema a este mismo estado de funcionalidad.

d) Ejecutar la utilidad que tiene el sistema operativo para la restaurar el sistema a la última configuración válida

Si el sistema presenta fallas es posible restaurarlo a la última configuración funcional registrada como última configuración válida conocida, para esto siga los siguientes pasos:

presione la tecla F8 cuando se reinicie el equipo y se vaya a empezar a cargar el sistema para acceder al menú de opciones avanzadas de Windows. Seleccione la opción última configuración válida conocida (la configuración más reciente que funcionó) y presione ENTER. Reinicie el sistema operativo para verificar si se soluciono el problema.

Al realizar estos pasos el sistema operativo se inicia con la información del Registro sin modificación, es decir, la que queda guardada la última vez que se apaga el equipo.

e) Realizar la recuperación del sistema operativo con ayuda del CD de instalación de Windows

Puede reparar una instalación de Windows dañada si ejecuta el programa de Instalación de Windows desde el CD de Windows XP. Con el CD del sistema operativo repare la instalación sin necesidad de reinstalarlo.

f) verificar que la configuración del chip BIOS y la CMOS sean correctas

Si la configuración de los valores de configuración de estos elementos son incorrectos se pueden presentar problemas de inicio y apagado del sistema. Se debe verificar esta configuración con los manuales de los chips y verificar si se soluciona el problema.

g) comprobar si los discos duros y sus sistemas de archivos están funcionando correctamente

Puede que alguno de los discos o su sistema de archivos sea el causante del problema. Para esto utilice la consola de recuperación del CD de Windows utilizando el comando chkdsk, si esta utilidad informa sobre un problema y no lo puede solucionar es posible que el sistema de archivos o el MBR estén dañados, si este es el caso utilice en la consola comandos de reparación del sector de arranque como fixmbr y fixboot o si puede formatee el disco duro y cree nuevas particiones.

5.5.2.4 Restauración de un sistema operativo Windows

Los sistemas operativos Windows desde la aparición de la versión Windows ME implementan una herramienta para la restauración de los equipos que devuelve al equipo a un estado anterior del actual.

Esta herramienta es definitivamente útil en ocasiones donde el computador de repente empieza a presentar fallas, sale un pantallazo azul o bien al reiniciar nos dice que el sistema se ha recuperado de un error grave que puede ocurrir por diversos motivos tanto de hardware como de software. En el aspecto de hardware puede ser un problema con la fuente de alimentación, con un disco defectuoso, con alguna de las tarjetas de memoria RAM o alguna otra tarjeta o dispositivo que hemos instalado y que ocasiona conflictos con el sistema operativo. En el aspecto de software el error puede ser debido a la perdida de algunos archivos del sistema, algún virus o malware en el equipo o un programa que está mal instalado, defectuoso o crea conflictos con nuestro sistema.

La restauración del sistema hace una copia de la configuración de archivos críticos del sistema operativo y de algunos archivos de aplicación que luego pueden ser útiles en caso de necesitar volver a una de estas configuraciones del sistema cuando tenía correcto funcionamiento, por ejemplo, puede ser útil en el caso de que un virus corrompa archivos del sistema y se desee volver al estado de configuración de archivos del sistema antes de la aparición del virus. Por defecto esta utilidad esta activa en el sistema operativo después de su instalación, pero es posible deshabilitar esta opción por cualquier motivo, como la realización de otras configuraciones en el sistema. Si esta opción es deshabilitada en cualquier momento se borraran todos los puntos de restauración guardados con anterioridad y al habilitar de nuevo la utilidad estos ya no aparecerán y no se podrán utilizar.

Con esta utilidad es posible crear un punto de restauración cada vez que lo necesitemos para tener la seguridad de proteger nuestra información en caso de un eventual problema con el funcionamiento del sistema operativo. El sistema operativo

también crea puntos de restauración automáticamente algunas veces cuando se instala nuevo software en el equipo y los usuarios no se enteran de ello, esto es útil por ejemplo cuando se instala un aplicativo que tiene un mal funcionamiento o provoca conflictos con el sistema para con esta opción poder volver a la configuración que tenía el sistema justo el momento antes de la Instalación.

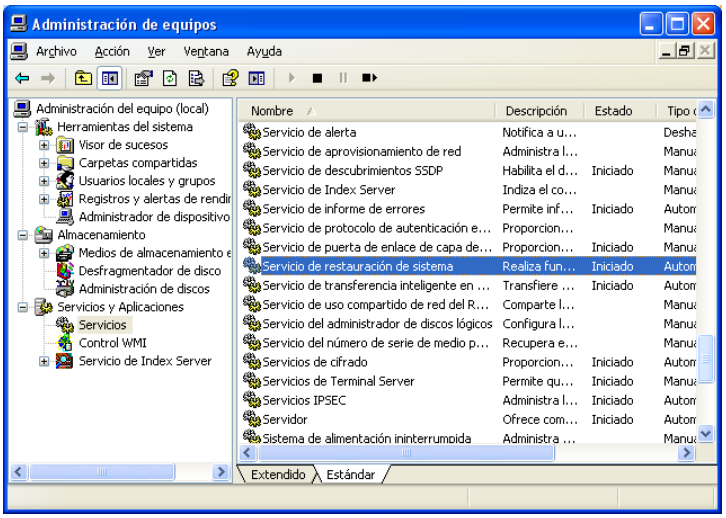
- ✓ Iniciar o parar el servicio de restauración del sistema en Windows XP

Este servicio por defecto se encuentra activado luego de la instalación del sistema operativo. Para verificar que realmente esta iniciado se siguen los siguientes pasos:

Dar clic en inicio>>clic derecho en Mi PC, y se elige la opción administrar (para poder acceder se necesita estar actualmente autenticado con una cuenta de privilegios administrativos):

Allí se despliega una ventana, dar clic en la parte de abajo en de servicios y aplicaciones y luego dar clic en servicios. Otra opción para acceder a la lista de servicios de Windows es digitando el comando services.msc en inicio>>ejecutar.

Figura 28. Administración de servicios de Windows XP



Fuente. Autor

En la lista se busca el servicio de restauración del sistema se verifica si el servicio está iniciado o parado, y aquí mismo se puede cambiar su estado

- ✓ Deshabilitar la utilidad de restauración del sistema

Para desactivar esta utilidad se accede a inicio>>clic derecho en Mi PC>>propiedades.

Allí se despliega una ventana donde se activa la pestaña de restaurar sistema y se marca la casilla desactivar restaurar sistema en todas las unidades:

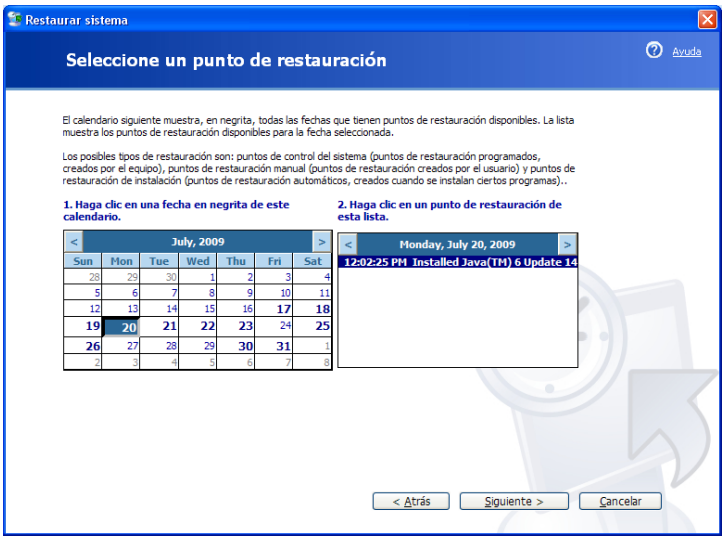
Al desactivar este servicio automáticamente se eliminan todos los puntos de restauración creados anteriormente y posteriormente ya no se puede hacer restauración a esos puntos, por esto antes de proceder y aplicar los cambios el sistema pide una confirmación de esta acción con una ventana de advertencia, se confirma y se da clic en aceptar para cerrar la ventana. Para volverlo a activar basta con desmarcar de nuevo la casilla desactivar restaurar sistema en todas las unidades, aplicar y aceptar.

- ✓ Utilizar restaurar el sistema

para acceder a esta utilidad se da clic en Inicio>>todos los programas>>Accesorios >>Herramientas del sistema>>Restaurar sistema.

En la ventana que se despliega se puede escoger entre las opciones de restaurar el equipo a un estado anterior o crear un punto de restauración para su posterior uso. Desde esta es posible crear un punto de restauración o restaurar el equipo con un punto ya creado

Figura 29. Utilidad de Restauración del Sistema de Windows XP



Fuente. Autor

Con esta misma utilidad se puede deshacer una restauración realizada cuando no se está conformes con los resultados.

5.5.2.5 Reparar la instalación del Sistema Operativo

Si al restaurar el sistema no se arregla el daño es aconsejable reparar la instalación del sistema operativo con el CD de instalación del sistema operativo siguiendo los siguientes pasos:

- Reiniciar el equipo con el CD de instalación dentro de la unidad
- Iniciar desde el CD de instalación (boot CD)
- Elegir la opción instalar Windows XP en el equipo (el equipo busca por versiones ya instaladas del sistema operativo en las unidades)
- Como ya se tiene instalado el sistema operativo en una partición el sistema muestra esta partición, Elegir la opción reparar la instalación del Windows instalado.
- El CD comienza a hacer la reparación del Sistema Operativo como si se estuviera instalando de nuevo, pero guarda la configuración de usuarios, aplicativos y demás que se tenía antes a la reparación.

Este método es muy útil cuando se presentan fallas graves la mayoría de veces por perdida de archivos críticos del sistema operativo, o por virus que lo corrompen.

Es aconsejable también examinar el equipo en busca de virus o malware, y si se encuentra tratar de eliminarlo con herramientas antivirus antes de realizar cualquier otro procedimiento y en caso de cualquier falla.

5.5.2.6 Formateo y reinstalación del sistema operativo

Si no hay forma de reparar alguna falla crítica del sistema con los métodos que se han descrito o cualquier otro método del que se tenga conocimiento, la mejor opción es reinstalar el Sistema Operativo.

Antes de hacer cualquier cosa se debe realizar un backup de todos los datos importantes en las unidades que se van a formatear (Donde se va a instalar el sistema Operativo y las otras que el usuario decida voluntariamente formatear). Después de realizar el backup se recomienda hacerle un scan a éste en busca de virus o programas malignos por precaución y para evitar que si hay algún virus se vuelva a infectar el sistema al restablecer o utilizar el backup.

Después de esto se procede a realizar la instalación del sistema Operativo, para esto se realizan los siguientes pasos:

1. Insertar el disco del sistema operativo en la unidad de CD del computador.

2. Reiniciar el computador en modo de booteo de CD. Para esto se realiza la configuración en la BIOS de opciones de booteo o se presiona la tecla F11 varias veces (puede ser otra como F9 dependiendo de la BIOS) inmediatamente después de reiniciar el equipo y antes de que inicie el cargado del Sistema operativo.

3. Se espera que carguen los controladores y archivos de instalación.

4. Se elige la opción: realizar una instalación nueva de Windows XP.

5. Se elige entre las particiones posibles que muestra el sistema en cual se desea instalar el Sistema Operativo.

6. Se elige el tipo de formateo (NTFS o NTFS Rápida).

7. En este momento se inicia el formateo de el disco o partición para continuar automáticamente con la instalación.

8. Se realiza la configuración básica del Sistema como es: Licencia, configuración regional y de idioma, configuración de hora, configuración de usuarios, configuración de red, actualizaciones automáticas, nombre y descripción del equipo, etc. Algunas de estas se pueden omitir para después configurarlas manualmente.

5.5.2.7 Aplicaciones útiles para reparación y limpieza de equipos

Preferiblemente se deben utilizar las herramientas antimalware en modo a prueba de fallos:

- ✓ Optimización de equipos

- Ccleaner (Software gratuito)
- System Mechanic (Software comercial, licencia de evaluación)
- CleanMyRegistry(Software comercial, licencia de evaluación)
- TuneUp(Software comercial, licencia de evaluación)

✓ Limpieza Malware (Spyware, Virus)

- AVG Free antivirus (Software gratuito)
- Spyware Doctor antispyware (Software comercial, licencia gratis para escaneo offline)
- Malwarebytes Anti-Malware (Software comercial, licencia gratis para escaneo offline)

5.6 SOPORTE A USUARIOS EN PROBLEMAS DE SOFTWARE EMPRESARIAL

En la empresa ATH se manejan muchas diferentes aplicaciones que son útiles y especializadas en tareas relacionadas con las áreas de trabajo de la empresa. El área de soporte a la infraestructura, donde se realizó la práctica empresarial es la encargada de administrar el servidor que contiene varias de éstas aplicaciones empresariales representadas en archivos y también de los recursos físicos en CD que contienen los instaladores de otras varias aplicaciones. Esta área también es la encargada de responder por el buen funcionamiento de todo este software de la empresa instalado en los equipos normales de trabajo.

5.6.1 Herramienta Service Desk

Cualquier falla en alguna de las aplicaciones empresariales es reportada por la persona dueña del equipo donde se presenta la falla a través de una herramienta de servicios de tipo Help Desk llamada Service Desk. Mediante la herramienta Service Desk cualquier persona de la empresa puede realizar un requerimiento a cualquier otra persona o un grupo de personas de un área de trabajo diferente cuando se le presente un problema del cual, a la persona o grupo que se le hace el requerimiento tiene alguna responsabilidad. Cada trabajador de la empresa tiene un usuario activo creado en la herramienta de atención de servicios Service desk, y mediante este

usuario puede crear el requerimiento especificando el problema, la prioridad de respuesta, y otros detalles que describan las características el problema presentado y la urgencia de resolución.

Cuando se presenta la falla en el equipo y el usuario presenta el requerimiento, los integrantes del área de soporte a la infraestructura a los que se le hizo el requerimiento analizan la gravedad del problema para posteriormente plantear posibles soluciones y aplicarlas con el fin de solucionar estos problemas y que la persona que realizó el requerimiento pueda continuar con sus actividades normales de manera satisfactoria.

5.6.2 Base de Conocimientos

Para facilitar la solución de inconvenientes con software, existe en el área una base de datos donde son consignados los problemas más frecuentes presentados en la empresa con sus respectivas posibilidades de solución llamada Base de Conocimientos. Cada vez que se descubre un caso nuevo y su solución, este se consigna dentro de la base de conocimientos para que en una ocasión posterior si este caso se presenta de nuevo cualquier persona del área pueda revisar la base de conocimientos y consultar la posible solución del problema para aplicarla.

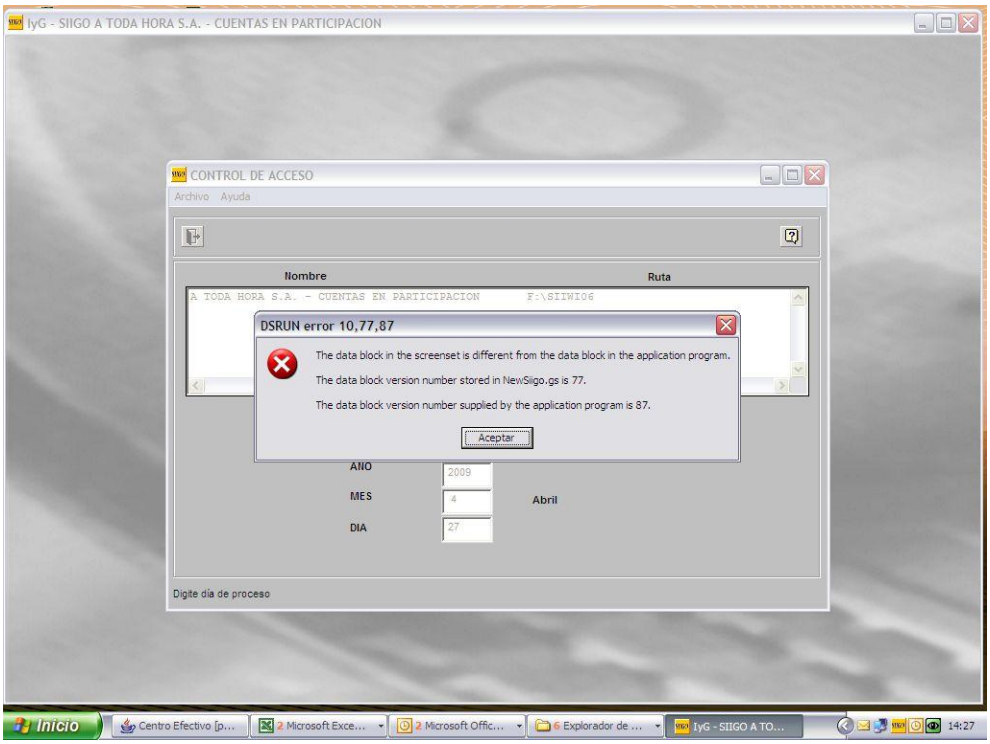
5.6.3 Casos de mantenimiento software consignados en la base de conocimientos de ATH

5.6.3.1 Caso SIIGO

En la empresa se maneja un aplicativo llamado SIIGO utilizado para labores contables en varias de las áreas de la empresa. Este aplicativo es usado desde hace mucho tiempo en ATH y la firma del producto realiza las actualizaciones del aplicativo contable cada vez que es necesario por medio de la eliminación de una carpeta base del aplicativo la cual se encuentra instalada en el servidor para la posterior creación de una nueva carpeta que contiene la misma información del software que la carpeta eliminada pero con las actualizaciones del software correspondientes.

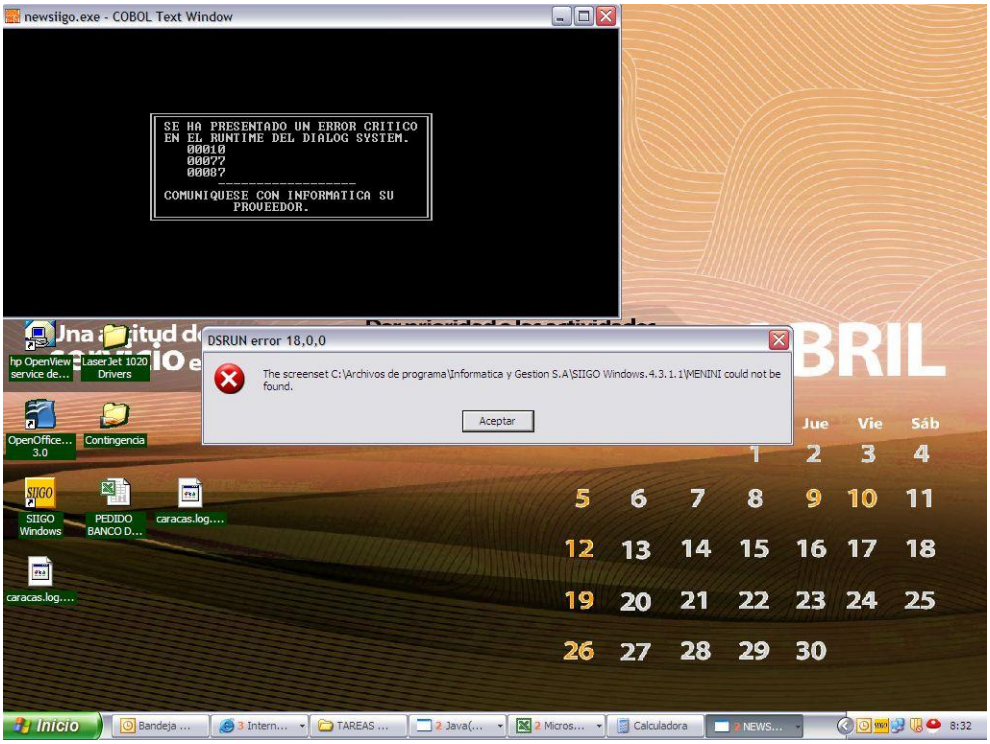
En Febrero se presento un caso de pérdida del medio de instalación de este software y se procedió a utilizar un medio de instalación más antiguo que se encontraba disponible en el inventario del área. Al realizar la instalación con este medio y finalizarla se observaba que el aplicativo no funcionaba correctamente y salían algunos mensajes de error al intentar ejecutarlo.

Figura 30. Error SIIGO Windows 1



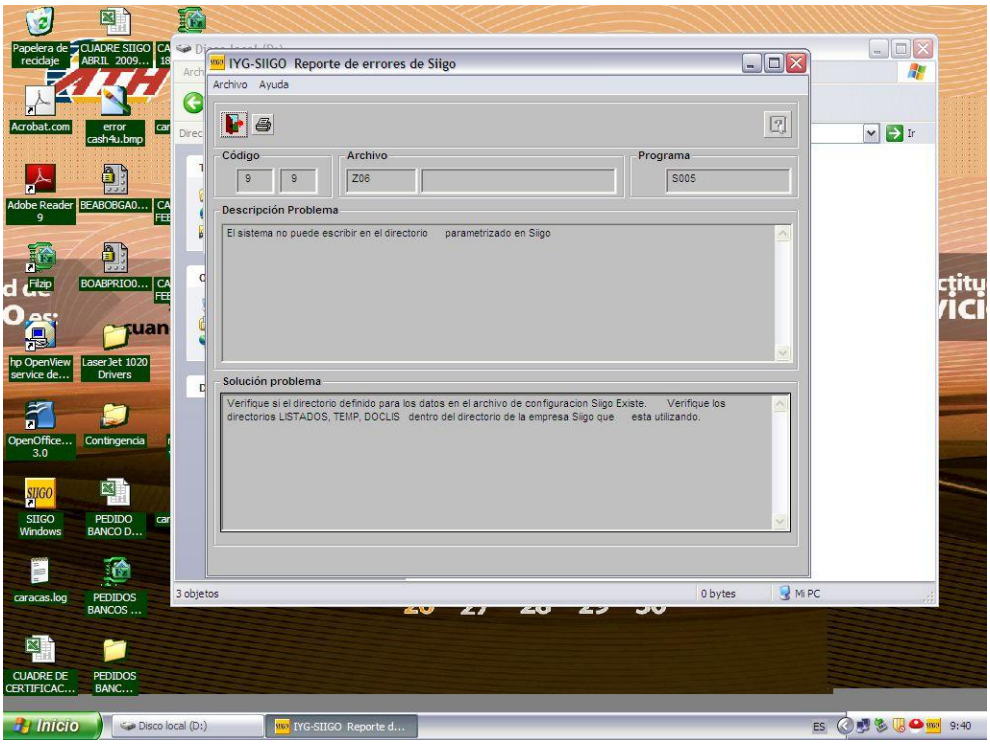
Fuente. Autor

Figura 31. Error SIIGO Windows 2



Fuente. Autor

Figura 32. Error SIIGO Windows 3



Fuente. Autor

Se empezó a realizar la investigación de por qué podría estar fallando el aplicativo y cuál podría ser la solución para su buen funcionamiento. Para esto se inicio verificando, con la ayuda del administrador de permisos de grupo con perfil para ésta aplicación, si el usuario tenía asignados correctamente los permisos para descartar la posibilidad de que pudiera ser algo respecto a los permisos de usuario o de IP. Al ver que todos los permisos estaban asignados correctamente se procedió a analizar cuáles eran las diferencias entre los aplicativos instalados con el CD anterior y el que se utilizaba actualmente para poder corregirlas. Se encontró que la instalación con el CD anterior realizaba unos vínculos a carpetas, archivos y ejecutables que habían cambiado de nombre con anteriores versiones del aplicativo y por esto fallaba el intento de utilización de estos generando los errores que se visualizaban después de la instalación.

SOLUCIÓN: Se procedió a realizar las reparaciones correspondientes a los enlaces en el regedit (editor de registro) en la entrada (MIPC\HKEY_LOCAL_MACHINE\SOFTWARE\SIIGOWINDOWS\SIIGO\3.0.1\new_siigo.exe) y en los accesos directos del aplicativo y también a realizar el registro de este error y su solución en los documentos de la base de datos del área de soporte. Al realizar esta configuración el aplicativo funciono correctamente.

5.6.3.2 Caso Open View Service Desk

En la empresa se utiliza un software muy útil para la solicitud de órdenes de trabajo e implementado desde el 2008 llamado Service Desk. Este software lo utiliza todo el personal de la empresa, es fundamental y muy utilizado en la mayoría de las áreas y se usa para solicitar colaboración requerida en algún tema por parte del solicitante a algún otro trabajador de la empresa que tenga competencias o responsabilidades con el tema de la solicitud. La solicitud se puede hacer a una persona en particular o a un área completa, y tiene la opción de dar la descripción del problema, la prioridad de respuesta, hacer la selección del tipo de problema entre las opciones configuradas en el software, dar la fecha límite de respuesta, etc.

Para este software se presento un caso de error (Java.lang Null Pointer Exception) del cual no se encontraba la solución, y por lo tanto, cada vez que se presentaba este error era necesario desinstalar, reinstalar y volver a configurar el aplicativo para que funcionara correctamente. En ocasiones era necesario hacer este procedimiento de reinstalación varias veces, en algunos casos hasta cinco o seis veces para que funcionara correctamente, perjudicando así el trabajo normal, quitando tiempo laboral y complicando las actividades normales.

Al observar los síntomas del error y analizar su comportamiento se pudo ver que este debía tener causa en algún archivo o información que afectaba el buen funcionamiento del aplicativo ya que se investigo que este error se presenta cuando en java hay una variable nula que va a un puntero y no puede hacerlo. Este error persistía aún cuando se eliminaba y se reinstalaba el software, por lo cual se empezó la búsqueda de esta información de la aplicación que debería ser eliminada o reparada. Para esto se utilizó el aplicativo en un equipo que presentaba la falla y se empezaron a examinar los archivos sospechosos que podrían estar causándola. Se encontraron varios archivos que cambiaban al utilizar el aplicativo pero que se comprobó que no tenía que ver con el problema.

SOLUCIÓN: En especial se encontró una carpeta que contenía datos de cache del aplicativo, y ya que estos datos no son fundamentales para el funcionamiento del aplicativo y estos se crean por si mismos al utilizarlo, se procedió a eliminar la carpeta con la buena respuesta de que al eliminarla, el software volvía a funcionar adecuadamente. Después de ver la solución del problema se encontró una opción en las herramientas del aplicativo para eliminar el caché automáticamente al cerrar el aplicativo la cual se activo para disminuir la probabilidad de fallas futuras en el software Service Desk.

5.6.3.3 Caso conflictos IP's

En la empresa se presento un tiempo donde frecuentemente aparecían equipos con mensajes de conflicto de ip´s en la red debido al nuevo direccionamiento de algunos equipos a causa de la reciente iniciación de pruebas para la implantación del proyecto de segmentación en la empresa en pro de la seguridad. El procedimiento que se realizo fue con ayuda del área de telecomunicaciones donde tienen la mayoría de información acerca de las direcciones MAC de los equipos y direcciones ip's nuevas y antiguas según el proyecto.

SOLUCION: Primero cuando se presentaba el problema se examinaba el registro de eventos del equipo ingresando al ejecutar en el menú inicio de Windows y digitando eventvwr.msc. Al estar en el visor de sucesos se veían los detalles el error que mostraba el sistema donde aparecía el problema con una descripción como esta:

Fecha: 25/04/2009
Origen: TCP/IP
Tipo: Error
Id. suceso: 4199
equipo: ATHCRH19

El sistema ha detectado un conflicto por la dirección 10.130.4.89. La dirección de hardware es 00:1F:67:6A:D0:67, las operaciones de red en este sistema pueden verse afectadas por este problema.

En la descripción se puede ver la dirección MAC del equipo que se encuentra en conflicto de red con este, y podemos comparar la información con un documento donde el área de telecomunicaciones almacena estos datos para proceder al re direccionamiento y solucionar el problema.

El visor de sucesos de Windows (eventvwr) puede ser utilizado como en este caso, para resolver diferentes problemas en la infraestructura.

5.7 OTRAS CONFIGURACIONES BÁSICAS Y RECURRENTES APLICACIONES DE WINDOWS.

Durante la práctica se realizaron tareas de configuración comunes en el ámbito empresarial, para el mantenimiento de aplicaciones frecuentemente utilizadas por casi todos los recursos humanos en ésta, como lo son la aplicación de correo Outlook y los

exploradores de internet. A continuación se describen algunas configuraciones comunes en las aplicaciones Microsoft Outlook y Microsoft internet explorer.

5.7.1 Configuraciones en Outlook.

La herramienta de correo Microsoft Outlook es muy utilizada por todos los recursos humanos empresariales, unos más que otros, como lo es el caso algunas personas de Mercadeo o de otras áreas que frecuentemente realizan envío de correos y tienen alta cantidad de recepción de correos de trabajadores de la empresa o de personas externas que tienen que ver con sus asuntos de trabajo.

Además de ser útil para el envío y recepción de correos, ésta herramienta permite manejar una agenda de citas con la ayuda de su utilidad de calendario para enviar solicitudes y programar citas con otros usuarios, contando con su disponibilidad de tiempo y aceptación.

Siendo una herramienta tan importante, cualquier fallo en esta tiene una alta prioridad de respuesta a atención de problemas. Dos de los problemas más frecuentes se describen a continuación con su correspondiente solución.

5.7.1.1 Outlook se ejecuta cada vez más lento o no responde

En este caso y viendo los síntomas presentados, muy posiblemente el problema se trate de un archivo de datos *.pst que se encuentra al límite de su capacidad.

Los archivos de datos *.pst son archivos que contienen almacenada la información de todos los correos enviados y recibidos por el usuario desde su creación, y aumenta cada vez que se realiza un envío o recepción de correo electrónico cuando se tiene configurado este archivo como predeterminado, ya que es posible tener varios archivos *.pst configurados en una misma cuenta de correo con el fin de poder explorar el historial de correos desde una cuenta de usuario Outlook.

Los administradores del servidor de correo son los que administran la capacidad de los archivos de los usuarios, cuando estos se acercan o llegan a su límite de capacidad se presentan los síntomas de lentitud en la aplicación o la falta de respuesta de esta.

SOLUCIÓN: Para solucionar este inconveniente se realiza el cambio de archivo de datos *.pst mediante la siguiente configuración.

Acceder a Panel de control de Windows>>Correo>>Mostrar Perfiles, seleccionar el perfil de usuario de Outlook de la persona a la que se le presenta el problema, Acceder a Propiedades>>Archivo de datos, Hacer clic en agregar y proceder a dar nombre (se recomienda darle nombre que indique la fecha de creación para efectos de facilidad de administración de estos archivos) y mostrar ubicación de disco donde se debe guardar el *.pst para crear el nuevo *.pst. Por último se debe seleccionar el archivo creado como predeterminado para que los nuevos correos e información se almacenen en este.

5.7.1.2 No deja visualizar la disponibilidad de calendario de otros

Este problema se puede presentar a causa de que la configuración del servidor proxy, las opciones del explorador de Internet pueden tener deficiencias. Si no se configuran correctamente las excepciones del explorador para que no envíe los datos de red interna por medio del servidor proxy, como es el caso del correo interno empresarial, este siempre intentara conectarse desde el proxy y no podrá acceder a la red interna causando este tipo de inconvenientes.

SOLUCIÓN: La solución a este problema es incluir en el explorador de internet las excepciones de proxy de la siguiente manera:

En un explorador de Microsoft acceder a Herramientas>>Opciones de Internet>>Conexiones>>Configuración LAN, en las opciones de proxy seleccionar Avanzadas, y por último en la sección de excepciones de proxy incluir las siguientes excepciones para el caso de la red de ATH:

ath.net;ath.com.co;discover.ath.com.co;email.ath.net

5.7.2 Configuración del proxy del internet explorer

Como en el caso anterior se explicó el servidor proxy sirve como ruta de acceso a la red externa empresarial. Si hay una mala configuración del servidor proxy los usuarios no podrán tener acceso a internet, ni a ninguna otra red externa y por consecuencia no podrán realizar tareas como buscar páginas web, enviar correos externos, entre otros.

Para realizar la configuración de estas opciones se debe tener en cuenta el perfil de usuario ya que existen diferentes servidores proxy que asignan más o menos opciones de utilización de red al usuario dependiendo de sus necesidades laborales. Al tener identificado el servidor proxy para el perfil de usuario, éste se debe ingresar de la siguiente forma:

SOLUCION: En un explorador de Microsoft acceder a Herramientas>>Opciones de Internet>>Conexiones>>Configuración LAN, en las opciones de proxy marcar la casilla de verificación: Usar un servidor proxy para la LAN, e ingresar el número IP del proxy correspondiente, por ejemplo: 10.130.0.147. También se debe verificar que se encuentre marcada la casilla: No usar servidor proxy para direcciones locales y que se encuentren correctamente configuradas las excepciones del proxy como se indico en la sección anterior.

6. MANUAL DE SEGURIDAD INFORMATICA ENFOCADA EN LOS SISTEMAS OPERATIVOS Y LA INFRAESTRUCTURA DE ATH

INTRODUCCIÓN

La empresa ATH es una empresa de carácter financiero, la cual se hace cargo de la prestación de servicios de cajeros automáticos y de comunicaciones de las entidades bancarias del grupo AVAL y sus empresas filiales, por lo tanto maneja información con un alto grado de confidencialidad y de gran importancia como información de usuarios de los bancos, información de tarjetas debito y crédito y claves de los usuarios, información de transacciones financieras, información de estado de los cajeros, etc.

Para asegurar de la mejor forma posible ésta información en todos los aspectos y proteger los intereses de la empresa, ATH cuenta con varias características de seguridad implementadas y manejadas a diferentes niveles dependiendo del entorno donde se haga la implementación, necesidades de seguridad presentadas y disponibilidad de recursos empresariales.

En este manual se muestran algunos de los aspectos de seguridad implementados en ATH, empezando por la seguridad de los sistemas Operativos e infraestructura en toda la empresa, algunas políticas y procedimientos de seguridad utilizados, normas legales con que se rige la empresa en cuanto a la seguridad informática, descripción de algunos riesgos que se presentan en la organización, y algunas soluciones a inconvenientes presentados.

Siendo ATH una empresa financiera y de prestación de servicios de telecomunicaciones del Grupo Aval y algunas otras entidades, la empresa ATH cuenta con diversas implementaciones en el campo de la seguridad de la información para protegerse de diversas variables que podrían afectar la viabilidad de la empresa.

El área que se hace cargo de la mayor parte en este campo es el área de Seguridad de la información donde se trabaja en aspectos como implementación y administración de Firewalls y zonas desmilitarizadas (DMZ), implementación de políticas y procedimientos, realización de pruebas de vulnerabilidades y otros similares. Otra área que también participa en procesos de seguridad son el área de Soporte a la infraestructura que se encarga de algunos aspectos del antivirus como configuración de antivirus y alertas, monitoreo de alertas, respuesta a ataques (junto con seguridad de la información y el soporte de la firma antivirus), también se encarga de la

administración de permisos de usuarios del directorio activo y locales de toda la empresa, y también lo que tenga que ver con la seguridad de la infraestructura tecnológica. El área de telecomunicaciones también tiene que ver con procesos de seguridad cuando se tratan por ejemplo aspectos de la red como segmentación de redes o cosas por el estilo. Otra área que se hace partícipe de parte de los procesos de seguridad es el área de auditoría que es el encargada de controlar que la organización lleve a cabo como se deben todos los procesos empresariales (entre los cuales se encuentran todos los relacionados con la seguridad de la información) siguiendo las normativas internas y externas y guiándose por los objetivos empresariales. Vemos así como la seguridad empresarial es una parte indispensable y compleja que se maneja en distintos campos y requiere de la participación de varios agentes para su correcta aplicación en el ámbito empresarial.

6.1 SEGURIDAD EN LOS SISTEMAS OPERATIVOS

La seguridad de la información debe ser vista como una unidad, como un concepto sistémico donde todos sus elementos están relacionados entre sí de algún modo dentro del mismo contexto. La seguridad de los sistemas operativos es un elemento de esta unidad y está relacionada con todos los demás elementos de la seguridad empresarial como lo son la seguridad de las redes, la seguridad de los datos, las aplicaciones de seguridad, seguridad del software, etc.

6.1.1 Realización de backups de seguridad

Por backup se entiende una copia de los datos de uno o varios archivos de manera automatizada o no desde un medio hacia otro medio o soporte que permita su posterior recuperación en caso de cualquier evento que afecte la información. Los backups o copias de seguridad son necesarios para garantizar la protección plena de los datos, protegiendo los aspectos de integridad y disponibilidad de la información. Estos procesos de realización de copias de seguridad y recuperación de información son indispensables y muy útiles en caso de presentarse fallas de software o hardware que impida el acceso o la recuperación de datos importantes y fundamentales que se poseen. Estos procedimientos permiten recuperar o en su caso reconstruir los datos y los archivos dañados o eliminados.

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

- ✓ Determinar los medios adecuados de realización de backups que se deben adquirir dependiendo de la importancia de la información, redundancia necesaria, necesidades de tiempos de copiado, espacios físicos y recursos económicos con que se cuenta, etc.

- ✓ Los backups deben ser almacenados en lugares físicos diferentes y distantes de donde se encuentra la información original con miras a tener más seguridad de no perder esta información en caso de desastres, robos, u otros eventos en el establecimiento donde se encuentran estos datos.

- ✓ Se deben tener políticas de revisión y control del estado de los backups para prevenir el darse cuenta que están mal realizados, dañados o por cualquier motivo ya no se encuentran disponibles hasta el día que se requiera de ellos. También se debe contar con mecanismos de custodia de los medios de almacenamiento de backups para prevenir su modificación, robo, destrucción y garantizar así su integridad, estos mecanismos deben ser confiables.

- ✓ Se deben implementar mecanismos de encriptación a la información más crítica con fines de proteger de una mejor manera su confidencialidad.

- ✓ Deben haber procedimientos de borrado o destrucción para los medios de almacenamiento de backups que dejen de ser utilizados y sean sacados del área o de la empresa por cualquier motivo, teniendo en cuenta la importancia de la información que contenía el disco y para prevenir la recuperación de información que estuvo almacenada en estos.

- ✓ Tener previsto como proceder cuando se necesite acceder de manera rápida a la información de los backups para colaborar con la continuidad del negocio en caso de ser necesario.

En ATH se realizan backups dependiendo del área y de la calidad de la información a resguardar, algunos ejemplos son:

- ✓ **Backups de usuarios en los sistemas operativos:**

Los backups normalmente se pueden hacer solo moviendo la información importante a otro medio distinto al medio de almacenamiento y en los sistemas operativos más conocidos se puede realizar solo con instrucciones de copiado y pegado. Esta opción de realización de Backups es muy recomendable cuando se necesita hacer un backup que casi nunca se requiere y cuando se desea corroborar que toda la información que necesita el usuario se va a proteger correctamente mediante algún tipo de almacenamiento redundante. Este tipo de realización de backups es el más utilizado

por el área de soporte a la infraestructura de la empresa de la práctica y es requerida en diferentes ocasiones.

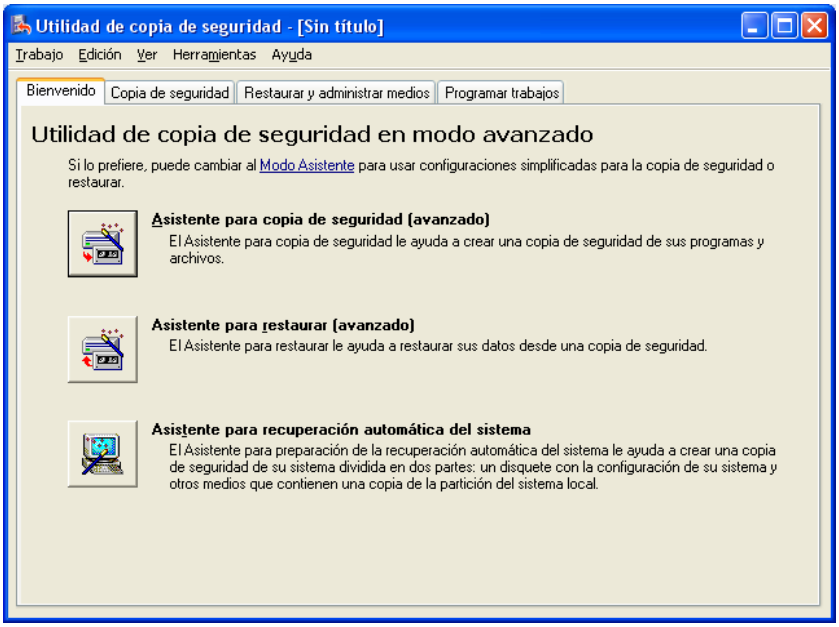
También existen herramientas que sirven para automatizar, facilitar o mejorar estos procesos de copiado, todo dependiendo de la importancia de la información.

Los más recientes sistemas operativos Windows como server 2003, XP y vista (los sistemas operativos más utilizados en ATH) cuentan con herramientas que permiten la realización de backups según las preferencias de usuario (NT Backup en XP, Backup and Restore Center en Vista, etc.). En XP los archivos de Backup se guardan por defecto con extensión .bkf y con la misma herramienta se puede hacer la restauración de estos datos en la ubicación deseada.

Como usar la Utilidad de copias de seguridad en Windows XP:

- Se accede a Inicio >> todos los programas >> Accesorios >> Herramientas del sistema >> Copias de seguridad.

Figura 33. Utilidad de Copias de Seguridad de Windows XP 1

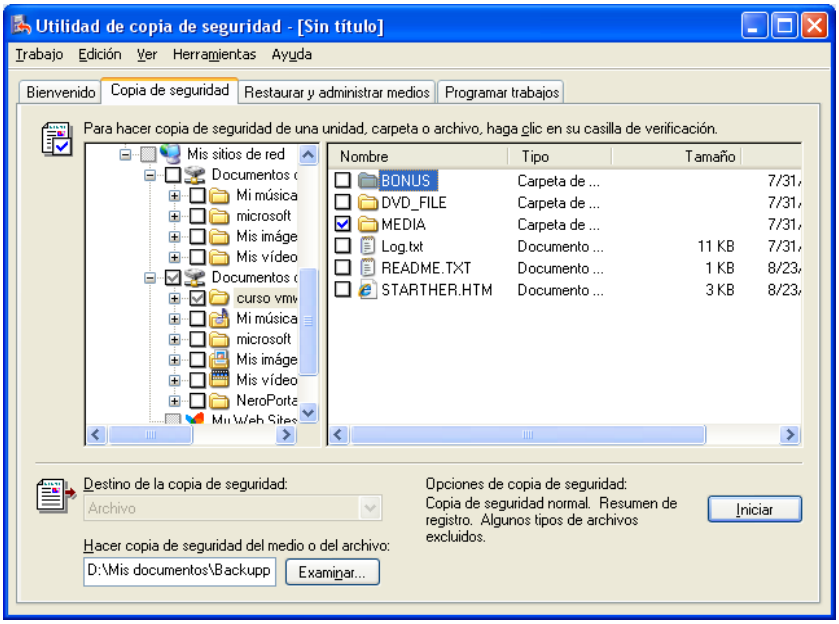


Fuente. Autor

- Allí es posible realizar varias tareas como crear copias de seguridad de los directorios que se elijan y en el directorio que se especifique (en la pestaña copia de Seguridad), restaurar copias de seguridad realizadas con anterioridad y en el directorio que se especifique (de los archivos *.bkf en la pestaña

Restaurar y administrar medios), o programar trabajos de realización de backup de acuerdo a las necesidades que se tengan (en la pestaña Programar trabajos). También se puede utilizar los asistentes para realizar cada una de estas tareas con mayor facilidad.

Figura 34. Utilidad de Copias de Seguridad de Windows XP 2



Fuente. Autor

- ✓ **Otros métodos de backups implementados en ATH**

  - o **HP Data Protector**

Para proteger datos de gran importancia en la empresa se emplean diferentes mecanismos de backup, por ejemplo para los datos de los servidores con información de cajeros se utiliza la herramienta Data Protector que es una herramienta software profesional y especializada para la realización de backups de discos o cd's en cintas magnéticas de manera muy sencilla y con opciones de configuración que se pueden adaptar fácilmente a las necesidades de la empresa.

  - o **Cobian Backup**

Otra implementación realizada en la empresa es el software open source Cobian backup, que automatiza los procesos de realización de copias de

seguridad según el criterio de configuración que se tenga. Este software da opciones de backups locales o en red, se puede configurar la automatización por tiempos desde días hasta meses haciendo copias completas, diferenciales o incrementales y también da otras opciones como compresión en formato ZIP o cifrado de datos con 4 diferentes métodos posibles.

6.1.2 Procesos de recuperación de datos y documentos del disco duro en ATH

Cuando se "elimina" un archivo desde Windows no se borra la información del disco duro, lo que se hace realmente es hacer que desaparezcan los directorios y ya no se encuentre en la lista de archivos del disco duro, pero la información magnética permanece guardada en sectores del disco que no se están utilizando, y esto hace posible la posterior recuperación de datos con la utilización de herramientas que se pueden encontrar (algunas mejores que otras), las cuales hacen un scan de todos los sectores del disco y hacen posible la recuperación de los datos.

Es preciso aclarar que no siempre es posible recuperar todos los datos eliminados ya que esto solo se puede realizar cuando la información que se necesita no ha sido sobrescrita, es decir, si estos sectores donde se encuentran los datos que han sido desvinculados del sistema de directorios en el sistema operativo no se han vuelto a utilizar posteriormente para el almacenamiento de nueva información. Si la información eliminada es sobrescrita se hace imposible recuperar esta información ya que nadie hasta el momento ha podido validar ninguna teoría que pruebe que sea posible recuperar información coherente de datos que han sido sobrescritos. Una teoría publicada en el año de 1996 por Peter Gutmann, científico en computación de la universidad de Auckland (Nueva Zelanda), sugería que si era posible recuperar la información magnética incluso si esta estaba sobrescrita, indicando que cuando esto sucede y con la utilización de microscopios electrónicos era posible analizar los datos magnéticos residuales en los discos y reconstruir la información perdida, documento que se puede encontrar en la web[14], pero esta teoría no ha sido comprobada y ha sido cuestionada por muchas personas con argumentos como el de que estos trabajos de investigación de Gutmann fueron realizados con discos que tenían una capacidad máxima de 130 MB y actualmente el tamaño y la distancia entre las pistas de los discos se han reducido en varios órdenes de magnitud haciendo imposible la recuperación de datos residuales, o argumentando también que aun si se pudieran recuperar datos residuales no serviría de nada ya que el magnetismo no es como la tinta, así que no se puede definir cronológicamente cuando se ha introducido la información o que datos son mas nuevos o están encima de otros. Tampoco ninguna persona u organización ha podido demostrar que esto sea posible y la mayoría de

[14] **Gutmann P**, Secure Deletion of Data from Magnetic and Solid-State Memory. Department of Computer Science, University of Auckland.
http://www.cs.cornell.edu/people/clarkson/secdg/papers.sp06/secure_deletion.pdf

expertos y trabajadores de este campo de recuperación de información concuerdan en que esto no es posible.

- ✓ **Proceso de recuperación**

El proceso de recuperación de datos en ATH de información no crítica ni confidencial lo realiza el área de Soporte a la Infraestructura con previo requerimiento a través del aplicativo Service Desk por parte del afectado y con ayuda de este para tratar de salvar las carpetas o documentos importantes. Para ésta tarea se utilizan distintas herramientas con interfaces muy sencillas de las cuales se escoge una a preferencia del que las va a utilizar.

Herramientas para la recuperación de la información utilizadas en ATH:

- ✓ Nucleus Kernel for FAT and NTFS
- ✓ EasyRecovery Professional
- ✓ Undelete PLUS
- ✓ GetDataBack for NTFS

Existen muchas otras herramientas para este objetivo pero en lo personal recomiendo las dos primeras.

Vale la pena aclarar que estas herramientas nombradas funcionan para formatos de archivo de Windows que son los sistemas que se utilizan en ATH. Los sistemas de archivos de Windows actualmente son del NTFS aunque aun algunos trabajan con el sistema FAT 32 que no es tan robusto y no tiene la seguridad que ofrece el sistema NTFS. Para realizar tareas de este tipo en otros tipos de Sistemas Operativos que manejen otros formatos de archivos se deben buscar herramientas que sean compatibles con el formato.

6.1.3 Gestión de cuentas de usuario

En ATH se tiene control estricto de los perfiles y cuentas de usuario de lo cual se ocupan varias áreas incluyendo a soporte a la infraestructura, limitando de la mejor forma posible las opciones de configuración del sistema operativo y de acceso a

recursos en la red, procurando que los usuarios puedan cumplir con las actividades laborales y cuenten estrictamente con los permisos necesarios para éstas labores. La gestión de cuentas de usuario constituye un elemento fundamental dentro de las políticas de seguridad de una organización, ya de de la asignación de permisos de estas cuentas y su correcto uso dependen cosas como el control de acceso lógico a recursos del sistema o el registro de actividad de usuarios. En los sistemas operativos generalmente existen dos tipos de usuarios que son el usuario administrador y el usuario limitado.

En relación con las cuentas de usuario con privilegios administrativos en ATH se hace especificación de hasta qué punto y en que determinadas condiciones este usuario o usuarios podrán hacer uso de los privilegios administrativos para acceder a carpetas o archivos de otros usuarios, hacer uso de la red, instalar o desinstalar aplicaciones, cambiar la configuración de los equipos, etc.

6.1.3.1 Gestión de usuarios en Windows XP

En la gran mayoría de equipos de la empresa se utiliza el sistema operativo Windows XP, que cuenta con herramientas que permiten dar seguridad de acceso y manejo de carpetas y archivos. Si se inicia sesión en un equipo utilizando la cuenta de usuario administrador se dispone de todos los privilegios de configuración para el hardware y software del equipo, se puede tener acceso a todos los archivos, cambiar opciones de configuración, eliminar y crear archivos sin ninguna restricción, instalar y desinstalar software y componentes software y administrar (crear, modificar y eliminar) todas las cuentas del sistema y sus propiedades. El usuario administrador también tiene la capacidad de cambiar la asignación de permisos del computador en todos los archivos y carpetas que este tenga. Si se inicia sesión con un usuario limitado tiene restricciones dependiendo de qué tipo de usuario sea**,** por ejemplo no podrá realizar modificaciones de configuraciones del sistema operativo, no tendrá acceso a los archivos de otros usuarios si un administrador o el dueño de la información no asigna estos permisos, no tendrá acceso a algunos archivos del sistema operativo y solo podrá crear o modificar información en su perfil de usuario limitado, este usuario solo podrá utilizar, compartir y otorgar permisos a los recursos creados con su cuenta (de su propiedad). La gestión de las cuentas de usuario en XP se realiza en el panel de control >> Cuentas de usuario, y tiene más utilidades de configuración y control cuando los usuarios se organizan en un servidor de directorio activo como en la mayoría de empresas.

6.1.3.2 El problema de trabajar con cuenta administrativa

En ATH existen muy pocos usuarios que tienen cuentas de dominio o locales con privilegios de administración ya que el usar este tipo de cuentas en empresas que

manejan el tipo de información que se maneja en las entidades financieras representa un riesgo para la seguridad de la información, y para tener un buen nivel de seguridad en éstas entidades se debe tener varias restricciones al acceso de la información. El problema de estas cuentas radica en que los usuarios con éste tipo de cuentas van a tener muchas más opciones de configuración y control sobre el sistema, y por ejemplo a un empleado desleal que cuente con una cuenta como estas de privilegios administrativos se le haría mucho más fácil acceder a la información confidencial de la red utilizando técnicas o herramientas de hacking que si lo intentara con una cuenta restringida. También en muchas ocasiones y más que todo en empresas como ésta existen amenazas de intrusiones de agentes externos a los recursos protegidos o virus que pueden afectar el computador. Si se trabaja con una cuenta administrativa y alguien toma control sin permiso del computador o algún virus entra en el sistema va a tener control total sobre éste pues va a tener los permisos de esta cuenta. Así cualquiera que sea el caso, la amenaza podrá tener acceso a todos los recursos del sistema sin ningún tipo de restricciones y podrá hacer cosas como auto reproducirse, realizar cambios en la configuración del sistema creando vulnerabilidades, acceder a información crítica, deshabilitar el antivirus y el firewall, etc. Por esto en la mayoría de empresas incluyendo ATH existen políticas para el control de los permisos de usuario que se encargan de que los usuarios tengan estrictamente los permisos necesarios para sus actividades laborales.

6.1.3.3 Gestión de privilegios de usuario y control de acceso a recursos en ATH

Las áreas de Soporte a la infraestructura, Soporte técnico y seguridad de la información son las encargadas en ATH de la gestión de cuentas de usuario en todos los equipos personales de los trabajadores de la empresa. Esta se maneja con las opciones de gestión de usuarios de Windows junto con el directorio activo. En el área de seguridad de la información se crean los perfiles de usuario para dar y denegar permisos de usuario y de recursos a los usuarios dependiendo de las necesidades de cada trabajador(a que servidores, ip's, unidades mapeadas, aplicaciones web, etc. necesitan acceso para sus labores cotidianas). En el área de Soporte Técnico junto con el área de Soporte a la infraestructura se administran todos los permisos que tienen que ver con el usuario empresarial (del directorio activo) creado al ingreso de cada persona al trabajo, en Soporte técnico son los encargados de administrar el servidor de directorio activo e implementar todas las políticas de grupo, crear nuevos usuarios asignando un perfil de dominio específico, hacer administración de recursos y seguridad junto con el área de seguridad de la información. El área de soporte a la infraestructura se pueden cambiar los permisos de usuario de dominio (directorio activo) y también tiene la capacidad de crear cuentas de administración local y administrar sus permisos en los equipos, pudiendo así en cualquier momento cambiar o modificar aspectos de los privilegios de usuario en el directorio activo, esto con la ayuda de una cuenta de administración global implementada en todos los equipos de la organización.

El control de acceso a recursos se maneja a través del perfil de usuario y a través de la administración de permisos a carpetas, discos u unidades que se realiza con la

ayuda de las herramientas de compartir y seguridad del sistema operativo Windows. Esta administración de recursos se debe realizar con extremo cuidado y conocimiento de su manejo ya que su mala configuración puede traer consecuencias a la seguridad de la información en todos sus aspectos. Para mejorar la seguridad de la empresa se manejan varias políticas como políticas de passwords, de intentos de login, de restricción de unidades, etc. que tienen que ver con este campo y mejoran la seguridad de usuarios y acceso a los equipos y a la información.

Cuando se comparten recursos en la red también de la empresa se debe hacer la asignación de permisos de acceso y uso de estos a usuarios o grupos haciendo uso de las herramientas que tiene el sistema operativo para este fin (compartir y seguridad) detallando quienes tienen acceso y que acciones son permitidas por las personas que tienen acceso a los recursos compartidos.

Para habilitar las opciones de configuración de seguridad avanzadas al compartir archivos de Windows es necesario desactivar la casilla Utilizar uso compartido simple de archivos, que se encuentra abriendo cualquier carpeta del explorador y dando clic en Herramientas>>Opciones de Carpeta>>Ver, (es la última casilla que aparece).

6.1.4 Administración avanzada de los Sistemas Operativos Windows

6.1.4.1 Dominio

Como la mayoría de empresas medianas o grandes de la actualidad ATH cuenta con redes de computadores que ayudan a optimizar las actividades diarias y también sirven como herramienta de comunicación y trabajo dando muchas posibilidades y utilidades a los usuarios.

En un sistema operativo Windows se puede organizar la red de computadores de dos formas diferentes que se mencionan a continuación:

- ✓ En un grupo de trabajo (workgroup)

  De esta forma se hace una agrupación lógica de máquinas, solamente para compartir archivos y realizar algunas operaciones básicas de red. En este tipo de red para poder acceder a recursos de un computador a otro remotamente el usuario que intenta acceder debe tener creada una cuenta en dicho computador y debe contar con los permisos necesarios asignados por el dueño de los recursos o por un administrador para poder accederlos. Esta organización de red es mayormente utilizada para redes caseras o de pocos computadores que no necesiten de administración ni centralización de recursos.

- ✓ En un dominio (domain)

  Esta forma de implementación de red es la más utilizada en ámbitos empresariales, donde se deben administrar, controlar y proteger los recursos y la información de manera eficiente en toda la infraestructura. En un Dominio la información administrativa de la red se encuentra centralizada, haciendo que la gestión y administración de los aspectos de la red, entre ellos la seguridad, se realice de una forma mucho más fácil de lo que sería si no se contara con éstas herramientas.

El DNS del dominio de la empresa es ATH.NET

6.1.4.2 Servidores de dominio

Para poder conformar un dominio se debe contar con la disposición de uno o varios servidores con funciones de controlador de dominio como el Windows server 2003 que es el más utilizado en la empresa (otros pueden ser Windows server 2000 o Windows server 2008) donde se recoge, almacena y suministra a los demás equipos del dominio la información de los recursos en este y las configuraciones administrativas.

En este o estos servidores controladores de dominio se administran de manera centralizada todos los recursos del dominio y se maneja su configuración de seguridad.

Los sistemas operativos Windows cuentan con muchas herramientas avanzadas de administración que se complementan con el servidor del directorio activo y facilitan el control de los sistemas operativos empresariales.

6.1.4.3 El directorio activo (Active directory)

En los controladores de dominio de Microsoft Windows se implementa el concepto de directorio activo que es un servicio de directorio o almacén de datos de los servidores Windows. El directorio activo representa la estructura jerárquica que almacena la información sobre recursos a manera de objetos de la red en el controlador de dominio. El directorio activo está diseñado para administrar el control de acceso de los usuarios y aplicaciones a los recursos de la red entre otras cosas, y esta implementado siguiendo varios estándares y protocolos existentes, ofreciendo interfaces de programación de aplicaciones que facilitan la comunicación con otros servicios de directorio. Algunos de los protocolos y estándares que utiliza el directorio activo son:

- ✓ DHCP (Dynamic Host Configuration Protocol). Protocolo para la asignación automática y dinámica de Ip's.

- ✓ DNS (Domain Name System). Servicio de nombres de dominio que relaciona los nombres de los computadores con las direcciones ip para su identificación siguiendo unos parámetros preestablecidos.

- ✓ SNTP (Simple Network Time Protocol). Protocolo simple de tiempo de red, que permite disponer de un servicio de tiempo distribuido para sincronización del tiempo en todos los computadores.

- ✓ LDAP (Lightweight Directory Access Protocol). Protocolo que utilizan las aplicaciones que requieren acceder o hacer alguna modificación al directorio activo.

- ✓ Kerberos V5. Protocolo que realiza autenticación de usuarios y equipos del Dominio.
- ✓ Certificados X.509. Estándar de seguridad que permite la distribución o replicación de información de manera confiable en los equipos conectados en la red.

El directorio activo está disponible para consulta en todos los computadores del dominio, y está disponible para su modificación en todos los controladores de dominio. Para administrar los servidores de dominio se debe tener buen conocimiento del tema, para así, poder modificar de forma adecuada los objetos del directorio que representan los recursos del sistema (usuarios, grupos, equipos, dispositivos, etc.) con la mejor implementación de seguridad posible.

El directorio activo es una utilidad de los servidores de Windows y se habilita después de instalar el sistema operativo servidor por ejemplo en Windows 2003 con el comando dcpromo en inicio>>ejecutar, después de haber instalado los servicios que se consideren necesarios como por ejemplo el servicio DNS.

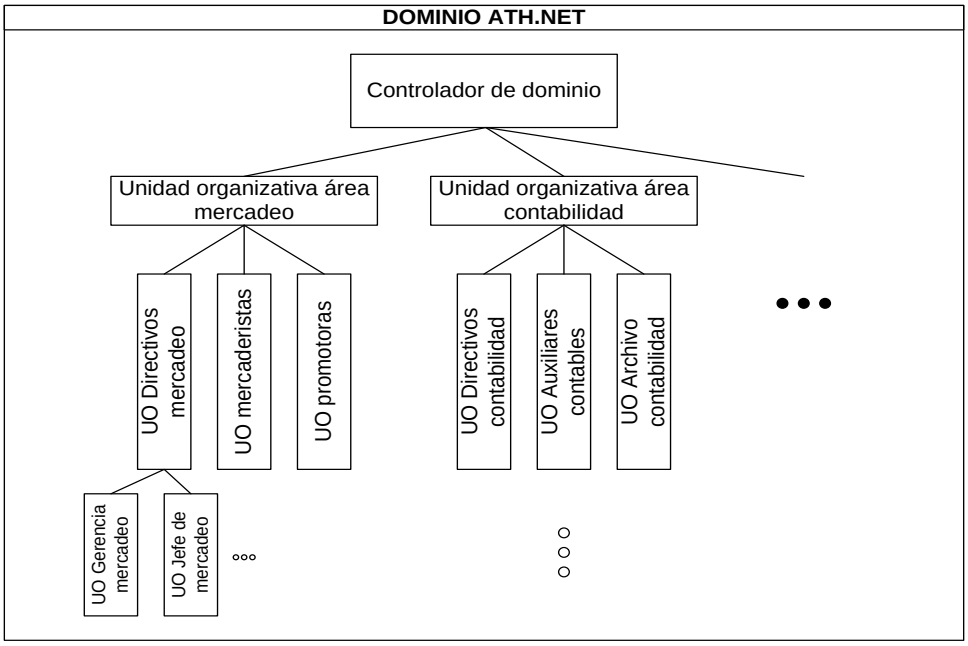
6.1.4.4 Unidades Organizativas (UO)

El directorio activo da la opción de agrupar con estructuras lógicas y jerárquicamente cuentas de usuarios, grupos, equipos y otras unidades de la red en contenedores denominados unidades organizativas y en estas solo se pueden incluir objetos de un solo dominio. Estas unidades organizativas son utilizadas en ATH para organizar la red de forma que sea más fácil de administrar, creando unidades con recursos que tengan los mismos perfiles de uso para poder implementar medidas de seguridad y

control de forma óptima a estos recursos. A estas unidades organizativas se les puede delegar autoridades administrativas o se pueden asignar directivas de grupo.

En función del modelo organizacional de ATH se tienen varias unidades Organizativas como podemos ver en el siguiente ejemplo con las áreas de mercadeo y contabilidad:

Figura 35. Jerarquía unidades organizativas en dominio ATH



Fuente. Autor

6.1.4.5 Directivas de grupo GPO (Group Policy Object)

Gran parte de la administración de seguridad de los sistemas operativos Windows, ya sea localmente o en un dominio se realiza mediante las directivas de grupo. En ATH la mayoría de políticas implementadas en lo que respecta a la seguridad de los sistemas operativos tiene que ver con la administración del directorio activo y las políticas de grupo las cuales son implementadas por el administrador de directorio activo pero son evaluadas por todo el personal competente en el tema de seguridad de la empresa que son las personas de seguridad, telecomunicaciones, soporte técnico y soporte a la infraestructura.

Con las directivas de grupo es posible administrar todos los aspectos del configurables del sistema en lo que tenga que ver con seguridad o entorno de los sistemas. En ATH estas políticas de grupo se aplican mediante el directorio activo por parte de su administrador, quien es el encargado de organizar y administrar de la mejor forma posible el directorio de tal forma que la seguridad y funcionalidad de la red estén

configuradas de la manera más optima. También si el usuario desea configurar políticas localmente y siempre y cuando tenga asignados los permisos para hacer esto es posible realizarlo mediante el comando gpedit.msc en inicio >> ejecutar de los sistemas operativos Windows.

Las directivas de grupo tienen dos funcionalidades principales que son como ya se dijo administrar la seguridad y el entorno del sistema. Las funciones administración de la seguridad con que cuenta el directorio activo y que se implementan mediante estas políticas a los objetos son muchas, algunos ejemplos de estas políticas en ATH son:

- ✓ Configuración de requisitos mínimos para contraseña de usuarios
- ✓ Reproducción automática de cd's (autorun)
- ✓ Uso de dispositivos externos
- ✓ Políticas de bloqueos de cuentas
- ✓ Auditar el sistema (sucesos, accesos, uso de privilegios,…)
- ✓ Asignación de derechos de usuario en el sistema
- ✓ Seguridad en la red

Las funciones de configuración del entorno también abarcan todos los aspectos del sistema como por ejemplo:

- ✓ configuraciones de asistencia remota
- ✓ Panel de control
- ✓ Inicios de sesión
- ✓ Hora del sistema
- ✓ Conexiones de red
- ✓ Informes de errores del sistema
- ✓ Perfiles de usuario
- ✓ Componentes del sistema operativo

6.1.5 Asignación de permisos NTFS de usuario del directorio activo

Con la administración de red mediante el directorio activo se dispone de muchas características de seguridad entre ellas las de permisos a carpetas, subcarpetas y archivos de los sistemas. Si los formatos de archivos de un computador es FAT32 no será posible realizar una detenida configuración de seguridad ya que este formato actualmente está casi que inutilizado y solo permite denegar o dar permiso de acceso a los usuarios sin definiciones más detalladas, entonces en este tipo de archivos si alguien tiene acceso a una carpeta, tiene permisos totales (lectura, escritura, modificación,…) de la carpeta, subcarpetas y archivos.

Si el formato de archivos es NTFS, que es el que se utiliza en la mayoría de computadores de ATH (si no en todos), es posible administrar de una forma más controlada y detallada los permisos a los recursos compartidos con el Active Directory proveyendo de un mayor nivel de seguridad al sistema y configurándola con la opción de compartir y seguridad de los recursos.

Los permisos NTFS permiten asignar una serie de privilegios o restricciones a usuarios y grupos creados en el Active Directory de acceso carpetas, subcarpetas y archivos del sistema. Estos permisos permiten una gran cantidad de opciones de configuración para personalizar la capacidad de cada usuario de acceso a la información.

Los permisos que se pueden otorgar o denegar en carpetas varían a los de carpetas, a continuación se muestran las posibilidades para cada uno de estos recursos:

Tabla 7. Permisos NTFS de Carpeta

Permisos NTFS de carpeta	Permisos que otorga al usuario
Leer	Ver archivos y subcarpetas dentro de la carpeta. Conocer quién es su propietario, y saber que atributos tiene tales como sólo lectura, oculto, archivo y sistema.
Escribir	Crear nuevos archivos y subcarpetas dentro de ésta carpeta, modificar atributos de la carpeta, conocer el propietario y los permisos asociados a la carpeta.
Listar contenido	Ver nombres de archivos y subcarpetas dentro de la carpeta.
Lectura y ejecución	Acceder a las subcarpetas y archivos dentro de esta carpeta incluso si el usuario no cuenta con permisos sobre estas carpetas, realizar acciones permitidas por los permisos leer y listar contenido de la carpeta.
Modificar	Eliminar la carpeta, realizar acciones permitidas por los permisos Escribir y Lectura y ejecución.
Control Total	Modificar los permisos, tomar la propiedad, eliminar subcarpetas y archivos y realizar acciones permitidas por todos los demás permisos NTFS de carpeta.

Fuente. Microsoft

Tabla 8. Permisos NTFS de Archivo

Permisos NTFS de archivo	Permite al Usuario
Leer	Leer el archivo y ver sus atributos, propietario y permisos.
Escribir	Sobrescribir el archivo, modificar sus atributos, ver el propietario y permisos de archivo.
Lectura y ejecución	Ejecutar aplicaciones además de poder ejecutar las acciones del permiso leer.
Modificar	Modificar y eliminar el archivos, además de realizar las acciones permitidas por los permisos Escribir y lectura y ejecución.
Control total	Modificar los permisos, tomar propiedad, además de las acciones permitidas por todos los demás permisos NTFS de archivo.

Fuente. Microsoft

También existen otra clase de permisos aparte de los comunes ya nombrados denominados permisos especiales que pueden ser aplicados con opciones avanzadas:

Tabla 9. Permisos especiales sobre Archivos o Carpetas

Permisos especiales	**Control total**	**Modificar**	**Leer y ejecutar**	**Mostrar el contenido de la carpeta**	**Leer**	**Escribir**
Recorrer carpeta o ejecutar archivo	sí	sí	sí	sí	no	no
Listar carpeta / Leer datos	sí	sí	sí	sí	sí	no
Atributos de lectura	sí	sí	sí	sí	sí	no
Atributos extendidos de lectura	sí	sí	sí	sí	sí	no
Crear archivos / Escribir datos	sí	sí	no	no	no	sí
Crear carpetas / Anexar datos	sí	sí	no	no	no	sí
Atributos de escritura	sí	sí	no	no	no	sí
Atributos extendidos de escritura	sí	sí	no	no	no	sí

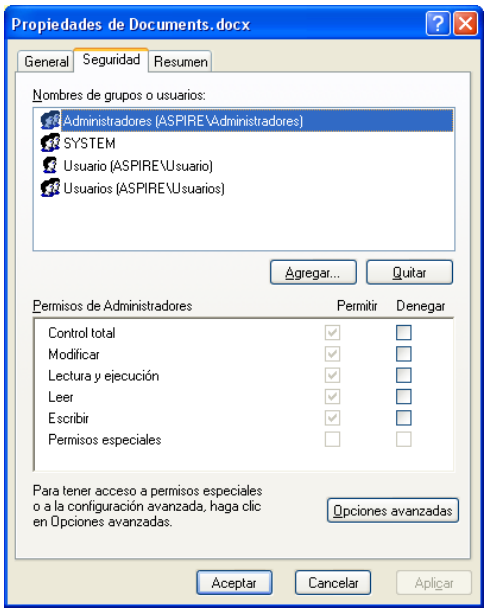
Eliminar subcarpetas y archivos	sí	no	no	no	no	no
Eliminar	sí	sí	no	no	no	no
Leer permisos	sí	sí	sí	sí	sí	sí
Cambiar permisos	sí	no	no	no	no	no
Tomar posesión	sí	no	no	no	no	no
Sincronizar	sí	sí	sí	sí	sí	sí

Fuente. Microsoft

Los permisos de Carpeta también cuentan con la opción de ser heredados a todas sus subcarpetas y archivos de manera automática si en algún momento se requiere. Si se utiliza esta opción, todas las subcarpetas y archivos contenidos en la carpeta Padre heredarán sus mismos permisos de usuario y de grupos.

Para realizar asignación de permisos a usuarios y grupos es necesario primero activar esta opción. Para habilitar las opciones de configuración de seguridad avanzadas al compartir archivos de Windows es necesario desactivar la casilla Utilizar uso compartido simple de archivos, que se encuentra abriendo cualquier carpeta del explorador y dando clic en Herramientas>>Opciones de Carpeta>>Ver, (es la última casilla que aparece). Después de esto ya es posible la asignación de permisos de usuario y grupos haciendo clic derecho en la carpeta o archivo donde se requiera modificar sus privilegios, y accediendo a Propiedades>>Seguridad.

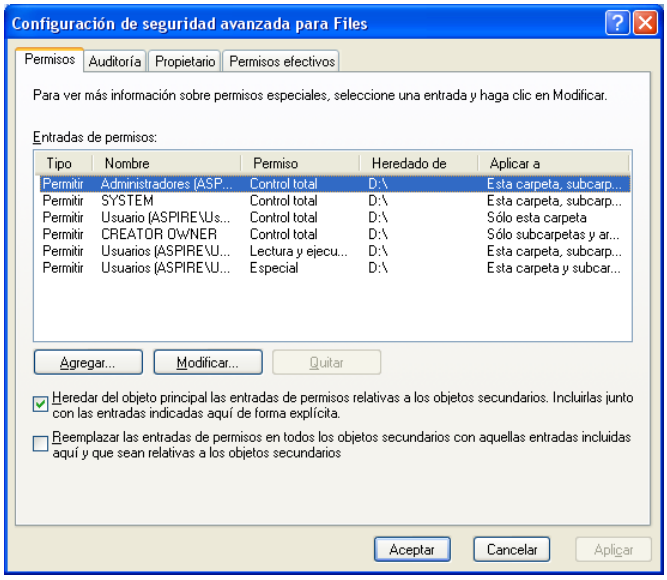
Figura 36. Asignación de permisos de seguridad a un usuario sobre un Archivo



Fuente. Autor

Con esta herramienta es posible relacionar los usuarios con estos archivos y realizar la asignación de permisos correspondientes a cada uno de ellos. Mediante las opciones agregar y Quitar se pueden ligar y desligar usuarios dentro del directorio activo a los archivos para realizar asignación o denegación de servicios a estos usuarios. Mediante las opciones avanzadas de esta utilidad es posible heredar permisos, revisar permisos efectivos, revisar y modificar la propiedad de los recursos y otras opciones de configuración de seguridad para archivos y carpetas.

Figura 37. Configuración de propiedades de seguridad avanzadas para una Carpeta



Fuente. Autor

6.1.5.1 Lista de control de acceso ACL

Cuando hay un volumen de disco con formato NTFS existe una lista ACL (Access Control List), utilizada para almacenar el registro de cada archivo o carpeta con la información de los permisos garantizados de usuarios o grupos que tienen acceso a estos. Las entradas de esta lista son conocidas como ACE (Access Control Entries), que asocian un archivo o carpeta del registro con un usuario o grupo garantizando algún privilegio que tenga el usuario o grupo sobre el recurso. Por ejemplo si un usuario solicita modificar un archivo determinado debe existir una ACE dentro del registro en la ACL del archivo que garantice este permiso a el usuario o a un grupo al que este pertenezca para que pueda realizar esta acción.

6.1.5.2 Permisos NTFS Múltiples

Con este sistema de asignación de permisos es posible que se presenten múltiples permisos sobre los mismos recursos para un mismo usuario. Para saber cuáles son los permisos que prevalecen cuando se presenta esta situación es necesario conocer las prioridades de los permisos y como estos pueden ser heredados.

La suma de los permisos entre los de carpeta y archivo que son asignados a un usuario o grupo son conocidos como permisos efectivos.

Cuando se le asignan permisos al cualquier usuario sobre un archivo y también sobre la carpeta que contiene este archivo hay que tener en cuenta que tienen prioridad los permisos de archivo sobre los de carpeta, es decir, el sistema va a otorgar los permisos que tienen los archivos en primer lugar y en caso de no tener asignados permisos de archivo otorga los permisos de la carpeta donde se encuentra el archivo, esto siempre y cuando se cuente con el permiso de omisión de comprobación cruzada en el sistema.

Si un usuario tiene permisos de acceso sobre un archivo pero no tiene permisos de visibilidad de la carpeta que lo contiene, puede acceder al archivo siempre y cuando tenga la ruta completa del archivo, porque de otra forma no puede revisar la ubicación del archivo y se hace casi imposible adivinarla

También el sistema tiene la opción de denegación de permisos, la cual sobrescribe y anula cualquier otra asignación de permisos realizada e impide que un usuario o grupo cuenten con privilegios sobre carpetas o archivos.

Entonces las reglas de permisos NTFS cumplen con lo siguiente:

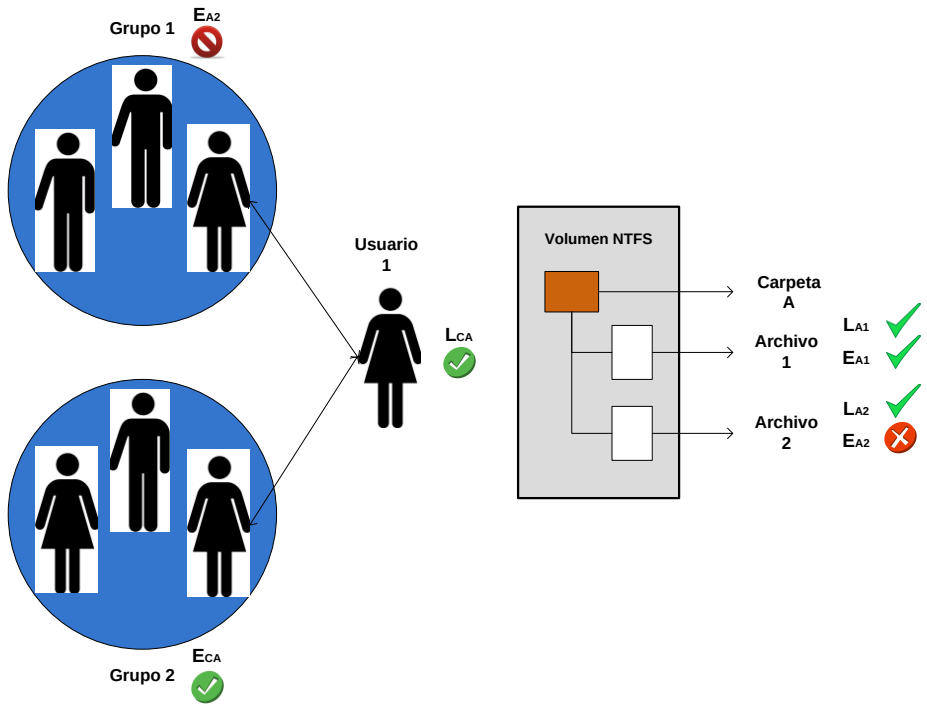
- ✓ Los permisos NTFS son acumulativos

- ✓ Los permisos de archivo sobrescriben los permisos de carpeta

- ✓ Denegar un permiso sobrescribe a otros permisos

A continuación se muestra un ejemplo de múltiple asignación de permisos y su resultado a partir de las prioridades de la asignación de estos:

Figura 38. Prioridades y sobre escritura de permisos de Carpeta y Archivo



Fuente. Autor

- ➢ La carpeta A contiene los Archivos 1 y 2
- ➢ El Usuario 1 Pertenece a los Grupos 1 y 2
- ➢ El Usuario 1 tiene asignados permisos de escritura en la Carpeta A
- ➢ El Grupo 2 tiene asignados permisos de escritura en la Carpeta A
- ➢ El grupo 1 Tiene denegados los permisos de escritura en el Archivo 2

Como resultado de esta asignación de permisos el Usuario 1 podrá leer y escribir el archivo 1 y también podrá leer el archivo 2, pero no podrá escribir el archivo 2, ya que la denegación de escritura que tiene en el grupo 1 sobre este archivo, sobrescribe los permisos de escritura en la Carpeta A que tiene en el Grupo 2.

6.1.6 Configuración de directivas de seguridad en cuentas de usuario de un Dominio

Para aumentar la seguridad de la autenticación mediante cuentas de usuario en los sistemas empresariales basados en sistemas operativos Windows y centralizados mediante un Dominio existen las directivas de cuenta, que son configuraciones de seguridad para las cuentas de usuario.

Las directivas de cuenta se dividen en tres grupos: directiva de contraseñas, directiva de bloqueo de cuenta y directiva de Kerberos.

6.1.6.1 Directiva de contraseñas

Las directivas de contraseñas se utilizan en cuentas locales o cuentas de Dominio por igual, y tienen el fin de exigir y hacer cumplir los parámetros de seguridad que el administrador del sistema crea convenientes entre varios parámetros posibles de configuración que son los siguientes:

Tabla 10. Directivas de Contraseñas

Directiva	Utilidad
Forzar el historial de contraseñas	Indica el numero de contraseñas nuevas y diferentes que el usuario ha utilizado en el cambio de contraseñas para que pueda repetir una contraseña ya utilizada
Duración máxima de la contraseña	Indica el número de días máximo que el usuario puede utilizar una misma contraseña antes de que el sistema le exija que La cambie. Esta puede configurarse entre 1 y 999 días.
Duración mínima de la contraseña	Indica el número en días que el usuario haya utilizado una contraseña antes de que el sistema le permita cambiarla. Puede ser un número entre 1 y 998 días y debe ser menor al número de duración

	máxima de contraseña.
Longitud mínima de la contraseña	Indica el número mínimo de caracteres que debe tener una contraseña de usuarios. Tiene valor entre 1 y 14, o puede ser 0 si el sistema no requiere de contraseña. Esta opción mejora la seguridad de las contraseñas ante ataques de fuerza bruta, ya que un carácter más va aumentando su dificultad de adivinación ya que cada carácter puede contener uno entre 94 caracteres entre mayúsculas, minúsculas, caracteres especiales y números.
Las contraseñas deben cumplir los requerimientos de complejidad	Si se habilita esta opción el sistema exige unos requisitos de seguridad predeterminados para la elección de contraseña de usuario que son: No deben contener partes significativas del nombre de cuenta del usuario o nombre completo, tener como mínimo seis caracteres de longitud, Estar compuesta por caracteres de tres de las siguientes categorías: Letras mayúsculas, de la A a la Z Letras minúsculas, de la a a la z Dígitos en base 10, de 0 a 9 Caracteres no alfabéticos (por ejemplo, !, $, #, %)
Almacenar contraseñas usando cifrado reversible	Indica si se debe utilizar cifrado reversible para el almacenamiento de las contraseñas. El cifrado reversible aporta compatibilidad para las aplicaciones que utilizan protocolos que requieren conocer la contraseña del usuario para la autenticación permitiéndoles acceder a las contraseñas mediante formato de texto plano. Esta directiva no debe habilitarse nunca, a menos que los requisitos de la aplicación sean más importantes que la necesidad de proteger la información de las contraseñas.

Fuente. Microsoft

- ✓ Longitud de la contraseña

A mayor longitud de la contraseña se protege mucho más la seguridad frente a ataques como los de fuerza bruta que intentan descifrar la contraseña utilizando todas las combinaciones de caracteres posibles.

A continuación se muestra como aumenta la dificultad de adivinación de contraseñas con el aumento de caracteres en ésta:

Los posibles caracteres dentro de la contraseña son:

- 26 caracteres en minúscula
- 26 caracteres en mayúscula
- 32 caracteres especiales
- 10 caracteres de números

En total serían 94 opciones posibles para cada carácter de la contraseña.

Si por ejemplo se usa una contraseña con 6 caracteres existirían 94 a la 6 posibilidades de contraseñas, es decir hay 689’869.781.056 contraseñas posibles de 6 caracteres de las cuales solo 1 es la elegida por el usuario.

Existen programas que utilizan ataques de fuerza bruta, de diccionario o muchos otros para intentar adivinar una contraseña de usuario y así vulnerar la seguridad de los sistemas de información. A mayor longitud de contraseña se disminuye enormemente la posibilidad de que esta sea descifrada aumentando así la seguridad en el sistema como se vea continuación:

- ✓ 6 caracteres: 689869781056 posibilidades
- ✓ 7 caracteres: 64,847,759,419,264 posibilidades
- ✓ 8 caracteres: 6,095,689,385,410,816 posibilidades

- ✓ 9 caracteres: 572,994,802,228,616,704 posibilidades

- ✓ 10 caracteres: 53,861,511,409,489,970,176 posibilidades

6.1.6.2 Directiva de bloqueo de cuentas

Las directivas de bloqueo de cuenta son útiles para casos donde una cuenta de usuario sea sospechosa y represente algún peligro para la seguridad de la información. Las opciones de configuración que tiene esta característica son:

- o Duración del bloqueo de cuenta: Determina el número en minutos permanecerá bloqueada en caso de suceder esto para que el sistema la desbloquee automáticamente. Si se establece en valor 0 la cuenta durará bloqueada permanentemente hasta que un administrador de Dominio la desbloquee personalmente. El valor en minutos puede estar entre 1 y 99.999. Para que esta directiva tenga sentido debe especificarse un umbral de boqueo de cuenta.

- o Umbral de bloqueos de cuenta: Determina el máximo número de reiteración de intentos fallidos de ingreso contraseña para el inicio de sesión con una cuenta, posibles antes de que se bloquee la cuenta automáticamente. El valor que puede tomar la configuración de esta opción va desde 1 hasta 999 intentos, si se le da valor de 0 la cuenta no se bloqueará por intentos fallidos de inicio de sesión.

- o Restablecer la cuenta de bloqueos: Determina el número en minutos que debe transcurrir después de un intento fallido para que el contador se restablezca a 0 intentos fallidos. Esta opción de configuración puede tomar un valor entre 1 y 99.999 minutos. Si se ha definido un Umbral de bloqueo de cuenta el tiempo de restablecimiento debe ser menor o igual a este.

6.1.7 Otras herramientas de administración para la configuración de seguridad en el dominio.

Las herramientas que se describen a continuación se utilizan para administrar las políticas de seguridad en computadores, Unidades Organizativas (UO), o Dominios.

Tabla 11. Herramientas de administración para la configuración de la seguridad en el Dominio

Herramientas de administración para la configuración de seguridad	Descripción
Plantillas de seguridad	Una plantilla de seguridad es un archivo que representa una configuración de seguridad o la política de seguridad. Estas plantillas, posteriormente, pueden aplicarse a su directiva de equipo local o importarse a un objeto de directiva de grupo (GPO).
Análisis y configuración de seguridad	Se puede utilizar esta herramienta para analizar o configurar la seguridad de un equipo utilizando una plantilla de seguridad.
Extensiones de ajustes de seguridad a Políticas de Grupo	Se puede utilizar esta herramienta para editar la configuración de seguridad individual de un dominio, sitio o unidad organizativa.
Políticas de seguridad Local	Se puede utilizar esta herramienta para editar la configuración de seguridad individual para un equipo local.
Configuración de tareas automáticas de seguridad	Se puede utilizar esta herramienta para automatizar las tareas de configuración de seguridad.

Fuente. Microsoft

6.1.8 Problemas encontrados con la administración de permisos en Windows con el directorio activo

El área de Soporte a la infraestructura cuenta con un servidor de información y aplicaciones del área que no deberían poder acceder los demás usuarios de la empresa. Para proveer de seguridad este servidor se creó un grupo en el directorio activo llamado gsoporte, que lo conforman todos los usuarios del área de soporte a la infraestructura, y después de esto se configuró la seguridad del servidor de tal forma que solo este grupo pudiera acceder a los recursos de éste servidor y tener permisos sobre ellos mediante una contraseña generada. Cada vez que algún usuario

autorizado de soporte necesitara cualquier recurso del servidor podía acceder a este remotamente desde el equipo de cualquier usuario de la empresa.

El problema que se encontró fue que en este sistema de autorización de acceso y permisos a usuarios de Windows se presentaba una falla, ya que al acceder utilizando la contraseña a los recursos del servidor de Soporte desde cualquier equipo y con cualquier sesión que tuviera iniciada este, los permisos permanecían en el equipo hasta que no se cerrara sesión o se reiniciara el equipo, entonces si cualquier usuario autorizado accedía al servidor y salía de éste, cualquier otro usuario podría acceder de nuevo a estos recursos sin ningún requerimiento de autenticación mientras siguiera trabajando en la misma sesión en la que estuvo accediendo el usuario autorizado. Este es un grave problema viéndolo desde el punto de vista de la seguridad, ya que en este servidor en particular se maneja información confidencial a la cual no debería acceder más que el grupo autorizado, y además así puede haber más servidores con el mismo problema. No se pudo encontrar una configuración o cualquier tipo de solución que acabara con este problema.

6.1.9 Control y monitoreo de registros de seguridad

El área de auditoría empresarial se en carga de implementar directivas de auditoría para supervisar los eventos ocurridos en el sistema, con el fin de detectar posibles anomalías en estos y tomar las acciones necesarias para la protección de la seguridad de la información empresarial. Para ingresar el contenido del registro de seguridad por defecto que tienen los sistemas XP se puede ingresar a la ubicación: Inicio>>Panel de Control>>Herramientas administrativas>>Visor de sucesos.

Para revisar los sucesos de seguridad se elige dentro del árbol de opciones la de seguridad, donde los sucesos de este tipo que hayan tenido éxito aparecerán junto a un icono en forma de llave, mientras que los que hayan fallado aparecerán junto a un icono en forma de candado. Para ver en detalle un suceso requerido se selecciona con doble clic.

6.1.10 Gestión de la Auditoría en el Dominio

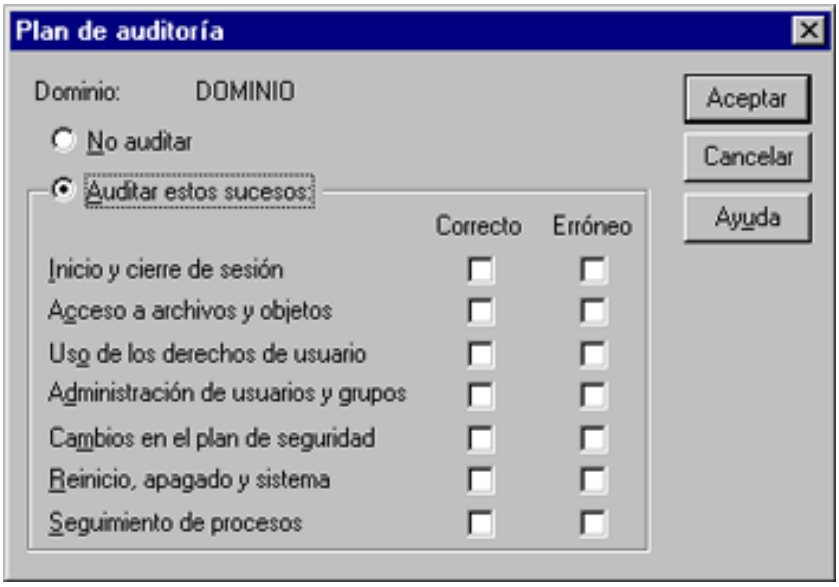
6.1.10.1 Auditoría de sucesos

La auditoría de recursos informáticos en la empresa donde se realizo la práctica se hace de manera centralizada con la ayuda de los controladores de Dominio y el directorio Activo de los servidores Windows. Para implementar un sistema de auditoría

con las características de seguridad que requiere la empresa existen varias utilidades de las cuales se explicará su funcionamiento.

Para realizar la activación de planes de auditoría se debe acceder en el Administrador de usuarios para Dominios a >>Directivas>>Auditorías>>Auditar sucesos para utilizar la herramienta Plan de auditoría desarrollada para este fin. En esta herramienta es posible elegir entre varias opciones que tipos de sucesos se requieren auditar.

Figura 39. Auditoría de sucesos en el Dominio



Fuente. Autor

- ✓ **Inicio y cierre de sesión:** Inicio o finalización de sesión por parte de un usuario del Dominio, finalización de la conexión con un servidor.

- ✓ **Acceso a archivos y objetos:** Accesos a Archivos, carpetas o impresoras configurados para ser auditados. Esta opción debe ser seleccionada para auditar recursos de carpetas, archivos o impresoras.

- ✓ **Uso de los derechos de usuario:** Privilegios utilizados por un usuario (con excepción de los de inicio y finalización de sesión).

- ✓ **Administración de usuarios y grupos:** Creación, modificación o eliminación de cuentas de usuario o de grupo, o configuración de sus características. (Activar, modificar contraseñas, deshabilitar, etc.).

- ✓ **Cambios en el plan de seguridad - Directivas:** Realización de cambios en permisos de usuario, auditoría o relaciones de confianza.

- ✓ **Reinicio, apagado y sistema:** Registros de inició y apagado de equipos o otros registro de seguridad.

- ✓ **Seguimiento de procesos:** Seguimiento detallada de diferentes sucesos, como la activación de programas.

6.1.10.2 Auditoría de Carpetas y archivos

También es posible auditar los eventos relacionados con las carpetas y archivos dentro del directorio Activo con volúmenes que tengan formatos NTFS. Este tipo de auditorías se hacen con fines de protección de la información, pudiendo auditar intentos de acceso a archivos, accesos de usuarios a información crítica, modificación de archivos sensibles, etc., todo mediante el análisis de los registros que se guardan en el sistema con la implantación de estas auditorías. Con las utilidades de los servidores de Dominio Windows se pueden configurar estas auditorías de modo que se cuenten con controles más estrictos para la información más sensible y se puedan determinar exactamente cuales acciones se requieren auditar y sobre cuales recursos se va a hacer auditoría.

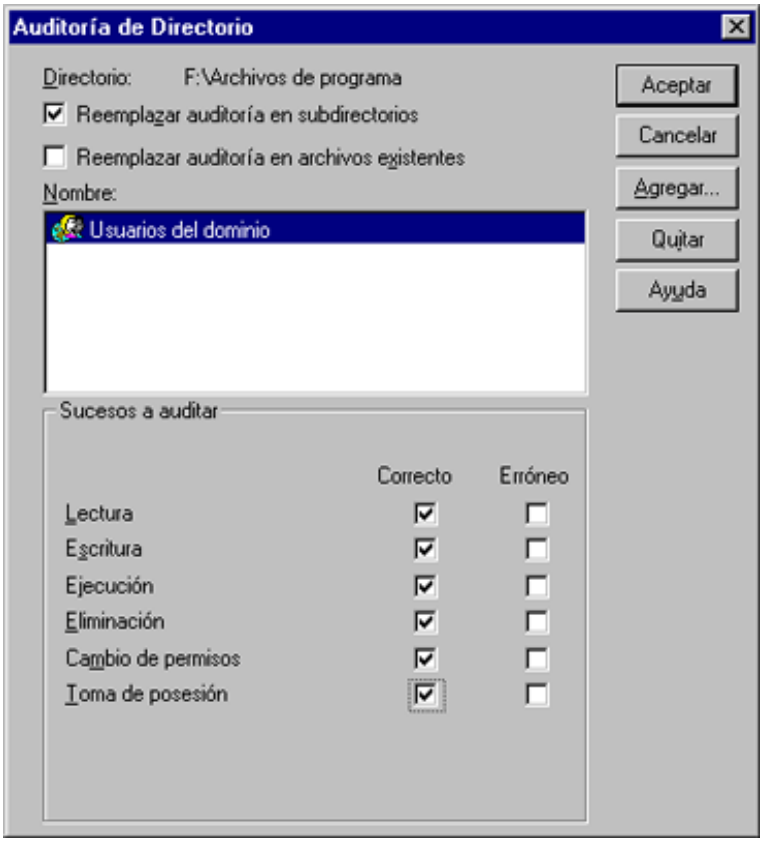
Para implantar la auditoria de un archivo o carpeta en el Dominio primero se debe abrir el explorador de Windows y se debe seleccionar el recurso de directorio activo al que se le piensan implantar los registros de auditoría. Después de seleccionar el archivo o carpeta se accede a Archivo>>Propiedades>>Seguridad y se hace clic en la opción Auditoria. Desde esta utilidad es posible agregar o eliminar usuarios o grupos a los cuales se requiere o no auditar, se pueden configurar todas las opciones de sucesos que se requieren auditar como lo son Lectura, Escritura, ejecución, modificación, eliminación, cambio de permisos y toma de propiedad de los recursos.

Tabla 12. Auditoría de Carpetas y Archivos en el Dominio

Sucesos a auditar	Carpeta	Archivo
Lectura	Mostrar datos, permisos, atributos y propiedad de la Carpeta.	Mostrar Nombre, permisos, atributos y propiedad del Archivo.
Escritura	Crear carpetas y subcarpetas, cambios en los atributos, permisos y propietario.	Modificar datos, permisos, atributos y propiedad del archivo.
Ejecución	Acceder, modificar carpetas y subcarpetas.	Utilizar archivos, mostrar atributos, permisos y propiedad del archivo.
Eliminación	Eliminar carpeta.	Eliminar archivo.
Cambio de permisos	Modificar privilegios de usuario en la carpeta	Modificar privilegios de usuario en el archivo.
Toma de posesión	Cambiar propietario de la carpeta	Cambiar propietario del archivo

Fuente. Microsoft

Figura 40. Auditoría de Carpetas en el Dominio



Fuente. Autor

Para eliminar usuarios o recursos auditados se seleccionan y se utiliza la opción quitar.

6.1.11 Recursos compartidos en el dominio y recursos compartidos por defecto

Cuando se comparte una carpeta de la red empresarial, ésta también se puede publicar en el directorio activo creando un objeto del tipo recurso compartido y asociándole un nombre simbólico que no es necesariamente el mismo de la carpeta, para que luego este recurso pueda encontrarse mediante una consulta al directorio.

También cada vez que un equipo Windows en la red se agrega al dominio, automáticamente se crean por defecto varios recursos compartidos que son los siguientes (estos recursos no deben modificarse ni prohibirse ya que son propios del sistema y son necesarios para la realización de algunas operaciones en red):

- ✓ letra_de_unidad$. Cada partición de un sistema Windows están compartidas por defecto y pueden ser accedidas por Administradores de Dominio u operadores de Dominio desde cualquier equipo conectado por red al equipo objetivo. Las particiones de disco también pueden ser accedidas por cualquier otra persona que conozca una cuenta de usuario del equipo al cual se quiera acceder remotamente. El acceso se realiza mediante el comando \\IP_del Equipo Objetivo\Letra_de_unidad$ (por ejemplo: \\10.130.0.89\c$), en Inicio>>Ejecutar, y se realiza la autenticación de usuario para poder acceder.

- ✓ ADMIN$. Recurso que utiliza el sistema al hacer administración remota sobre un equipo en el Dominio.

- ✓ IPC$. Comando que permite el acceso a recursos compartidos desde una Shell DOS. Se utiliza para acceder remotamente con cuenta administrativa a un equipo mediante la siguiente instrucción en la Shell: net use \\IP_del_Equipo\IPC$ /user:Dominio_de_la_cuenta\cuenta_administrativa password_de_la_cuenta.

- ✓ NETLOGON. Servicio de los controladores de dominio que permite la validación y autenticación de cuentas que pertenecen a éste a través de la red.

- ✓ SYSVOL. Directorio público y compartido en los equipos de Dominio, que permite la replicación de información como políticas de grupo y otros en los controladores de Dominio.

6.2 CUMPLIMIENTO DE LA LEGISLACIÓN VIGENTE EN ATH

El área que tiene mayor responsabilidad de que se cumplan todas las normas que rigen a la empresa es el área de auditoría ya que ATH es una empresa es vigilada por la superintendencia financiera de Colombia y cumple con todas las normas legales que imponen la superintendencia y el gobierno de Colombia para poder ejercer sus funciones de manera correcta y sin ninguna clase de problemas legales.

La empresa cumple con todas las normas implantadas por la ley como la ley 1273 de la protección de la información y de los datos descrita anteriormente, y tiene la capacidad de adaptarse cada vez que alguna norma es modificada o implementada como la recientemente implementada por la superintendencia financiera de Colombia y publicada en la conocida circular 052[15] que debe estar completamente implementada en todas sus fases para el primero de enero de 2010.

Esta nueva norma muestra los criterios de seguridad con que se deben regir las entidades financieras en muchos aspectos como tercerización (outsourcing), divulgación de información, cajeros automáticos (ATM), call centers (centros de servicio a llamadas) y otros. ATH empezó a trabajar en adecuarse en todos los aspectos de esta norma desde su divulgación. Entre estos aspectos se encuentran algunos relacionados con los sistemas operativos y la infraestructura tecnológica como lo son: Seguridad y calidad, Documentación, Sistemas de acceso remoto a clientes, Internet, Reglas de actualización de software y análisis de vulnerabilidades. Algunas de estas normas, tomadas del documento Circular 052, y que deben ser cumplidas por las entidades financieras incluyendo a ATH y tienen que ver con aspectos de seguridad de infraestructura y sistemas operativos son:

- ✓ Seguridad y calidad

    - Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.

    - Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible.

[15] SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Circular Externa 052. Norma por la cual se definen los requerimientos mínimos de seguridad y calidad en el manejo de la información a través de medios y canales de distribución de productos y servicios para entidades financieras., 2007.

- Cuando la información que la entidad remite a sus clientes sea de carácter confidencial y se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.

- Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

- Velar por que la información enviada a los clientes esté libre de software malicioso.

- Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.

- Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

- Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.

- Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

- Tener en operación solo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

- Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

✓ Sistemas de acceso remoto para clientes

- Las entidades que ofrezcan servicio de acceso remoto para la realización de transacciones deberán contar con un módulo de seguridad de hardware para el sistema, que cumpla al menos con el estándar de seguridad FIPS-140-2 (Federal Information Processing Standard), el cual deberá ser de propósito específico (appliance) totalmente separado e independiente de cualquier otro dispositivo o

elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, de servidores de acceso remoto (RAS) y/o de concentradores.

- ✓ Internet

  - Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.

  - Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.

  - Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

  - Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

- ✓ Reglas para la actualización de Software

  - Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

- ✓ Análisis de vulnerabilidades

    - Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

    - Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.

    - Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

    - Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

6.3 POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN EN ATH

ATH implementa muchas políticas empresariales en el campo de la seguridad informática. Podemos definir política de seguridad como una “declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran”.

En la política de seguridad se describe la forma adecuada y óptima para el uso de los recursos de un sistema informático (parte lógica y parte física), a su vez reparte las responsabilidades y los derechos que tanto usuarios como administradores de la red poseen. Una política de seguridad implica la elaboración de procedimientos y planes que permitan salvar los recursos de la red contra pérdida, daño, alteraciones, etc.

Para la realización de una política de seguridad el área de seguridad de la empresa tiene presentes los siguientes aspectos:

- ✓ Recursos críticos a proteger.

- ✓ Personal encargado de proteger cada recurso.
- ✓ Cuál es la posibilidad de ataque a una vulnerabilidad.
- ✓ Que tanto se debe proteger un recurso.
- ✓ Selección de las mejores medidas a implementar teniendo en cuenta recursos económicos y efectividad de la medida.
- ✓ Control y cambio de medidas tomadas para adaptar el sistema y mejorarlo según nuevas tecnologías y métodos de seguridad.

6.3.1 Elementos de una Política de Seguridad Informática

Una política de Seguridad informática (PSI) considera:

- ✓ Alcance de la política, incluyendo recursos humanos y tecnológicos involucrados.
- ✓ Definición de sus objetivos y descripción de elementos implicados.
- ✓ Responsabilidades en la implementación y el control de la política.
- ✓ Requerimientos necesarios para su implementación.
- ✓ Definiciones de quebrantamientos y sanciones a quien vulnere aspectos de la política de seguridad.
- ✓ Grado de confidencialidad de la política.

En ATH están implementadas varias políticas para el tema de seguridad y los respectivos procedimientos. Las políticas indican el “qué hacer", los procedimientos indican el "cómo hacerlo"; es decir los procedimientos permiten ejecutar las políticas. Las políticas de Seguridad en ATH como en cualquier otra empresa deben seguir un proceso de actualización ya que las técnicas de hacking con el pasar del tiempo son

mejoradas, lo que pondría en riesgo la estabilidad de la organización; por tal razón las políticas deben ser estudiadas y revaluadas periódicamente para establecer estándares de Seguridad que permitan crear un ambiente informático fiable, de lo cual se encargan el área de seguridad de la información (para políticas relacionadas con este campo) y el área de organización y métodos de la empresa.

Durante el proceso de elaboración de una política de Seguridad se deben identificar los activos organizacionales, evaluación de posibles amenazas y riesgos, implementación de herramientas que permitan contra atacar a los riesgos. Dentro de las políticas de Seguridad debe implementarse una auditoria, la cual se encargará de regular y vigilar el funcionamiento del sistema informático.

6.3.2 Identificación de los activos informáticos a proteger de la organización

Es de gran importancia la elaboración de una lista en la cual se encuentren todos los recursos del sistema informático que requieran Seguridad; los recursos suelen dividirse en:

- ✓ Hardware: Parte física del sistema de cómputo (computadores, switches y demás elementos de red).

- ✓ Software: Conjunto de aplicaciones referentes a programas, ya sea de utilidades, de comunicaciones, sistemas operativos, entre Otros.

- ✓ Datos: Conjunto de información que manipula la organización dentro del sistema informático.

- ✓ Recursos humanos: Personal de trabajo en el sistema informático dentro de la organización.

- ✓ Documentación: Referencia escrita o digital, de programas, software, procedimientos administrativos y demás partes del sistema informático y la seguridad.

- ✓ Accesorios: Material impreso, cintas, formularios, relacionados con la información empresarial.

6.3.3 Ejemplo de política corporativa implementada en la empresa ATH para manejo de certificados digitales: Política de declaración de prácticas de certificación digital

En el Anexo 2 del presente documento se presenta un ejemplo de implementación de política una de seguridad en la empresa ATH. La política contiene la Declaración de las prácticas de certificación digital empresariales.

Además de la ya mencionada existen muchas más políticas corporativas implementadas en la empresa que protegen cada uno de los aspectos de la seguridad y reducen los riesgos que implica el manejo de la información valiosa como en el caso de las entidades de servicios y de cajeros automáticos. Algunas más entre estas políticas implementadas en ATH son:

- Política de seguridad de la información
- Política de administración de Firewalls
- Política de manejo de los dispositivos de almacenamiento USB
- Política de alteración de equipos en producción
- Política de administración de llaves de encriptación para cajeros
- Política de control del módulo SCA
- Política de integridad de las llaves de producción
- Política de accesos no autorizados a equipos de procesamiento PIN

6.4 PROCEDIMIENTOS DE SEGURIDAD EN ATH

Los procedimientos de seguridad representan acciones previstas a seguir y responsabilidades del personar empresarial en la realización de estas acciones cuando se presente algún evento relacionado con la seguridad de la información. Dentro de un procedimiento de seguridad se describe detalladamente cada paso a seguir y las personas involucradas en cada paso para los eventos de seguridad determinados. Los pasos descritos en el documento del procedimiento deben estar siempre al alcance de quienes deben ejecutarlo, deben ser lo suficientemente claros y entendibles y no deben tener contradicciones o elementos que puedan incitar

confusión o difícil entendimiento de estos. Estos procedimientos también deben estar lo más resumidos que sea posible expresando únicamente aspectos importantes de las acciones a seguir, y si se necesita detallar cualquier aspecto, se debe apoyar en documentos que deben ser relacionados con estos procedimientos, donde se especifiquen las acciones con el nivel de detalle que se quiera aplicar.

6.4.1 Ejemplo de procedimiento utilizado en ATH

A continuación se muestran dos ejemplos de los procedimientos de seguridad implementados en ATH, uno relacionado con virus informáticos y otro relacionado con procesos del Firewall:

- ✓ Prevención detección y eliminación de virus informático
  - o Objetivo

Definir la metodología para la elaboración del informe consolidado de los eventos asociados con

Penetración de virus a la estructura de ATH (SERVIDORES, y PCs) a través del aplicativo SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE.

- o Actividades del proceso
  - ✓ Consultar en el aplicativo SYMANTEC

    El Analista que se encuentre en el turno dos es el encargado de elaborar el informe de virus informático que consolida los eventos registrados de virus presentados en el día, y posteriormente debe remitirlo al área de Soporte a la infraestructura, para la toma de acciones correspondientes.

  - ✓ Análisis y construcción del informe

    Una vez obtenida la información se realiza análisis del comportamiento de los eventos; es decir su periodicidad, la máquina que los registró y selecciona los siguientes elementos para construir el informe:

- El conglomerado general es decir la totalidad de los eventos de virus registrados en el día

- Los diez equipos más infectados

- Los diez virus más frecuentes registrados en el día

✓ La acción que aplicó SYMANTEC para contrarrestarlo usualmente la aplicación toma alguna de las siguientes medidas:

- Limpiado

- Sospechoso

- Bloqueado

- Puesto en cuarentena

- Suprimido

- Recién infectado

- Todavía infectado: Para este tipo de calificación, el Analista emite alerta y sugerencias dentro del informe, de modo que Soporte actué oportunamente sobre el virus registrado.

El área de soporte a la infraestructura debe cerciorarse de que los computadores tengan instalada la última versión del antivirus.

o Envío del informe

Una vez se ha seleccionado la información antes mencionada, se integra en la plantilla predefinida para tal fin. El envío del informe se hace mediante correo electrónico.

o Periodicidad de generación del informe

El informe se genera diaria, semanalmente, y mensualmente. El procedimiento para su generación, y construcción es el mismo.

6.5 PLAN DE RESPUESTA A INCIDENTES Y CONTINUIDAD DE NEGOCIO EN ATH

Este plan pretende garantizar una respuesta eficaz en caso de presentarse cualquier tipo de incidente en la infraestructura y sistemas empresariales que amenazaran con afectar el funcionamiento de los procesos normales de trabajo perjudicando a la organización.

6.5.1 Objetivos de la Respuesta a Incidentes

- ✓ Detectar cualquier tipo de incidente que se presente en la Empresa.
- ✓ Velar por que los procesos empresariales sean afectados de la menor manera posible por los incidentes ocurridos y contar con herramientas que permitan continuar con procesos afectados mientras se resuelve el incidente.
- ✓ Determinar las causas del incidente y tomar medidas para que estos no se vuelvan a presentar.
- ✓ Detectar amenazas a los recursos empresariales y tomar las medidas necesarias para corregir vulnerabilidades y aplicar sanciones a los responsables.
- ✓ Mejorar la seguridad de la información y proteger los procesos empresariales, colaborando con la continuidad del negocio.
- ✓ Hacer un seguimiento a los procedimientos de respuesta a incidentes y procurar que su gestión sea adecuada.

6.5.2 Definición de Incidente

Un incidente es cualquier evento que afecte la normalidad de los procesos empresariales incluyendo la seguridad de la información y procesos elementales para la continuidad del negocio, o que represente peligro para cualquiera de estos, algunos ejemplos de posibles incidentes son:

- ✓ Afectación de datos informáticos empresariales por ataques o eventos desafortunados (robo, alteración no autorizada, perdida, etc.)

- ✓ Afectación a recursos físicos empresariales por ataques o eventos desafortunados (Infraestructura tecnológica primordialmente)

- ✓ Ataques o eventos de Denegación de Servicios.

- ✓ Infección de equipos por Malware.

- ✓ Detección de intrusiones en la Infraestructura Organizacional.

- ✓ Comportamiento inusual o no debido de los Sistemas empresariales.

6.5.3 Contingencia de los servidores de producción en ATH

Dentro del plan de respuesta a incidentes de ATH se encuentra el plan de contingencia de los servidores de producción, los cuales son indispensables para la correcta operación de procesos vitales en la empresa porque éstos prestan la mayoría de los servicios que ofrece la empresa a sus clientes. Este plan de contingencia es uno de los más importantes en la empresa y se ejecutaría en caso de algún evento de cualquier naturaleza que dañara o inhabilitara los servidores de producción.

Este plan de respuesta a incidentes de ATH cuenta con un centro de recursos que conforman una réplica de los servidores de producción necesarios para continuar con la operación de los procesos fundamentales que maneja la empresa como son transacciones, información de cajeros, y otros procesos indispensables en el negocio. Los recursos están ubicados en un lugar distinto a la ubicación central de las instalaciones para que en caso de que la falla se presente por desastres naturales o eventos desafortunados como incendios o ataques terroristas no se afecten los dos sistemas. A este centro de recursos también se le hace controles, mantenimiento y monitoreo para mantenerlo en condiciones óptimas de funcionamiento y correctamente actualizado, y cuenta con su propio personal de trabajadores encargados de monitorearlo y administrarlo.

El plan también cuenta con distintos tipos de procedimientos a realizar dependiendo del incidente presentado con el fin de que en caso de presentarse estos la afectación a

los procesos de la empresa sean mínimos y se logre restablecer la normalidad y continuidad del negocio en el menor tiempo posible.

6.6 CONTROL DE LOS VIRUS INFORMÁTICOS EN ATH

6.6.1 Virus en ATH

Durante el periodo de la práctica empresarial fue posible ver el proceso llevado a cabo cuando se presentan casos de virus que afectan varios equipos de la red interna de la empresa. Estos virus afectan varios aspectos de la seguridad, se reproducen rápidamente y producen bastantes pérdidas a las empresas.

Uno de los casos presentados fueron los virus blaster y sasser que son virus ya viejos pero que aún afectan a los computadores con sistemas operativos antiguos (Windows NT, Windows 2000) o a computadores con Windows XP que no tengan los parches y actualizaciones de seguridad al día. Estos virus afectan los equipos provocando cambios en la configuración del sistema y apagando los equipos, afectando así las labores de la empresa y retrasando todos los procesos de las áreas afectadas.

Estos dos virus afectaron mayormente al área de cuadre de cajeros, que es el área encargada de revisar y verificar las transacciones de los clientes de la entidad y los valores que estos representan para corregir algunas transacciones mal registradas por el sistema encargado de esto y la justificación o corrección de transacciones, como respuesta a quejas presentadas por clientes o directivos de la empresa. El motivo de que esta área fuera la más afectada es que en ésta, la mayoría de equipos tienen sistema operativo Windows 2000 a causa de que manejan aplicaciones que aún no han podido hacerse compatibles con otros Sistemas Operativos.

Para realizar la limpieza de estos virus fue necesario contar con la ayuda del personal de soporte de la empresa que presta los servicios de antivirus en la compañía (Symantec). Ellos nos facilitaron las herramientas de eliminación de estos virus, nos ayudaron a implementarlas y también a poner los parches de seguridad necesarios para evitar un posterior ataque de estos mismos.

Otros casos presentados en ATH fueron los de el virus w32.sality (Sality y sus diferentes variaciones) y el w32.downadup (conocido como Conficker). Estos dos virus afectaron mucho los equipos de la red interna de ATH y causaron varios tipos de problemas en la empresa.

El virus Sality lograba deshabilitar el antivirus y el administrador de tareas de Windows y borrar archivos del sistema operativo hasta tal punto de dejarlo inmanejable para los usuarios, y en últimas, dando únicamente la opción de formatear el equipo para eliminarlo. Este virus también afecto mucho la seguridad de la empresa ya que este es capaz de realizar cosas como crear puertas traseras (backdoors), captura de datos de teclado (keylogger), obtener información crítica del equipo (usuarios, contraseñas, …), infectar archivos ejecutables, borrar archivos relacionados con el antivirus o el firewall y otros archivos del sistema operativo, crear y modificar archivos del sistema operativo, capturar muchos otros datos de autenticación, redes, hardware y software del equipo y enviarla por protocolos como el SMTP a cualquier destino, y muchísimas otras cosas más que afectan la seguridad empresarial.

Para removerlo fue necesario utilizar las herramientas subministradas por Symantec (w32.sality removal tool) no mucho después de ocurrida la infección, ya que si ha pasado mucho tiempo después de infectado el virus habrá alterado muchos archivos del sistema y no será posible remover el virus con éstas herramientas, y en este caso la única opción es realizar un backup de los archivos importantes vigilando muy cuidadosamente que ninguno de estos archivos contenga el virus y luego proceder a formatear el equipo. Después de suprimir el virus deben instalarse los parches y aplicar las acciones correspondientes para prevenir posteriores infecciones.

El virus Conficker es un virus que aprovecha una vulnerabilidad de desbordamiento de buffer (buffer overflow) del servicio server de Windows afectando a todos los sistemas operativos recientes de éste. Este virus es capaz de desactivar servicios de seguridad, actualización y reporte de errores de Windows, es capaz de auto propagarse por cualquier tipo de red en algún sistema, recolectar y enviar información crítica del sistema, descargar y ejecutar malware adicional en el equipo y unirse a sí mismo a procesos legítimos del sistema como svchost.exe, explorer.exe y services.exe.

En ATH por ejemplo este virus realizaba ataques de intento de autenticación por fuerza bruta a los equipos, provocando así el bloqueo de muchos usuarios debido a la política de seguridad de bloqueo después de tres intentos fallidos. Esto provoco muchos problemas operativos en las áreas de la empresa infectadas que fue un porcentaje alto del total.

Para eliminar este virus fue necesario ejecutar la herramienta de eliminación del w32.downadup proporcionada por Symantec en todos los computadores infectados.

Después de eliminar los virus con todas las herramientas disponibles es importante y necesario instalar todas las actualizaciones y parches de los sistemas operativos para evitar que se vuelvan a presentar situaciones como estas.

En estos procesos se conto con el apoyo del área de seguridad de la información quienes eran los responsables de detectar los equipos infectados y los equipos desde los cuales se estaban realizando ataques a otros equipos para poder retirarlos de la red y proceder con las acciones de eliminación de virus y protección de la información.

6.6.2 Uso y administración de programas Antivirus

El antivirus es una de las principales medidas que se debe tomar en cualquier sistema informático para combatir la amenaza que representan los virus y otros programas dañinos, conviene siempre mantenerlo actualizado y configurado utilizando todas las herramientas con que este cuente.

Por otra parte las empresas pueden implementar opciones perimetrales, mediante la instalación de un programa antivirus en un servidor proxy que controle la conexión corporativa al internet, en un servidor de correo o en un dispositivo que filtre todo el tráfico entrante y saliente de la red corporativa.

La eficacia de estas herramientas depende de la buena medida de actualización de definiciones nuevas de virus (firmas), así como del soporte que preste la empresa desarrolladora del software antivirus.

El funcionamiento de un antivirus se distingue dos bloques o módulos principales:

- ✓ **Modulo de control**, encargado de las siguientes funciones:
    - Seguimiento de la actividad en el sistema informático.
    - Protección preventiva del sistema.
    - Detección de códigos malignos.
    - Configuración del funcionamiento del programa antivirus.
- ✓ **Módulo de respuesta,** responsable de las siguientes tareas:
    - Generación de alarmas y registro de incidencias.
    - Bloqueo de servicios y programas sospechosos.

- Desinfección de programas y documentos infectados (“file cleaning”).

Por otra parte, los programas antivirus suelen combinar distintas estrategias de detección de los códigos malignos que se describen a continuación:

- ✓ Escáner a demanda basado en el reconocimiento de “firmas" (secuencias de código) de códigos malignos, utilizando para ello una base de datos de virus conocidos. El problema de esta alternativa es que el continuo crecimiento de la base de datos de virus (en algunos casos ya supera las l00.000 firmas de códigos malignos) puede afectar al rendimiento del sistema, ya que el antivirus consume cada vez mayores recursos, a medida que se va actualizando su base de datos.

- ✓ Monitor residente, que permite ofrecer una protección en tiempo real, analizando cualquier archivo antes de que sea utilizado (copiar, ejecutar, instalar) o al ser descargado de internet, sin embargo, esta alternativa presenta el inconveniente de una mayor carga del sistema, así como de ocasionar posibles interferencias con otros servicios instalados, ya que el antivirus se encarga de interceptar y monitorizar todas las llamadas al sistema y la gestión de interrupciones en el equipo informático.

- ✓ Análisis heurístico (basado en la “experiencia"), que permite detectar virus nuevos al reconocer código con un comportamiento sospechoso. En este caso, el problema podrían venir a consecuencia de la aparición de falsos positivos, es decir, de archivos legítimos que puedan ser detectados como virus por el programa antivirus.

- ✓ Comprobación de la integridad de los archivos del sistema (estrategia de “integrity checking”, también conocida como "vacunación" de archivos), en este caso el programa antivirus se encarga de generar una base de datos con una suma de control o código de integridad de cada archivo del sistema, para de este modo poder detectar y alertar al usuario de cualquier cambio en el tamaño de los archivos. Sin embargo, hay que tener en cuenta que algunos virus ya tienen en cuenta esta posibilidad y tratan de engañar al sistema ofreciendo información falsa sobre el tamaño y el código de comprobación del archivo infectado.

- ✓ Análisis del comportamiento, tratando de detectar todas las acciones sospechosas o potencialmente peligrosas que se realicen en el sistema

informático: escribir en el sector de arranque del disco duro, modificar un archivo ejecutable, etc.

En los últimos años se han presentado en el mercado distintas soluciones globales contra las amenazas de seguridad y los códigos dañinos, constituidas por dispositivos que integran varios servicios como el programa antivirus, el filtrado de contenidos, un Sistema de Detección de intrusiones (IDS), un cortafuegos para la seguridad perimetral y un servidor VPN[16] para crear túneles seguros y habilitar las conexiones remotas. Además, estos dispositivos ("appliances"), que se instalan en el punto de conexión de la red corporativa de la empresa con el exterior, cuentan con un servicio de actualización y mantenimiento remoto por parte del fabricante. Entre ellos podríamos citar Symantec Gateway Security, Panda GateDefender, Mcafee Foundstone o TrendMicro IWSA (InterScan Web Security Appliance).

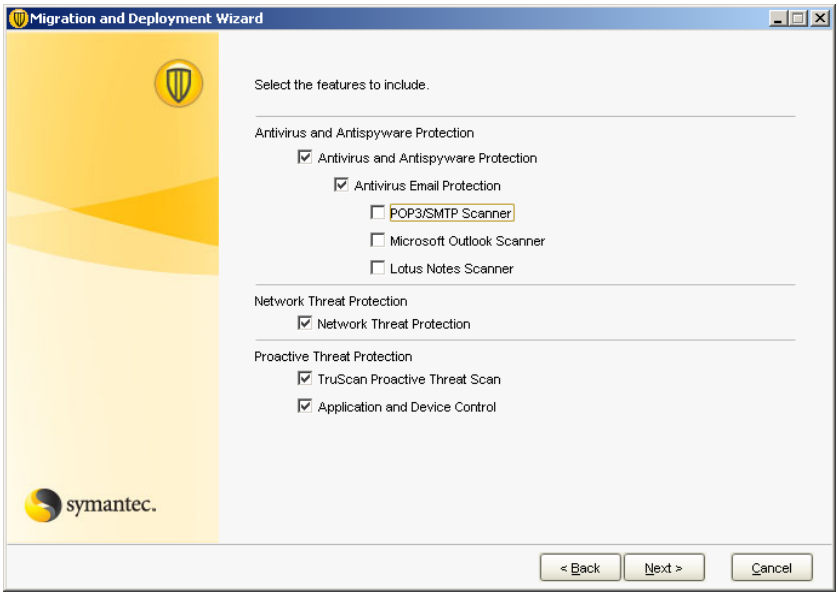
6.6.2.1 Antivirus Symantec en ATH

La empresa ATH utiliza el servicio la reconocida Firma Antivirus Symantec para su implementación en toda la infraestructura de la empresa (Cajeros, Servidores, Equipos) la cual también brinda soporte de su producto cuando se solicita y que es administrada en su mayoría por el área de soporte a la infraestructura, la cual realiza las tareas de instalación, monitoreo y control de estos antivirus.

A continuación se muestran algunas gráficas del proceso de configuración en la creación de paquetes del antivirus Symantec para cajeros, servidores, computadores o portátiles en ATH

[16] Conexión de dos o más computadores mediante una red virtual que aísla a los computadores pertenecientes a la red virtual de los que no pertenecen a esta.

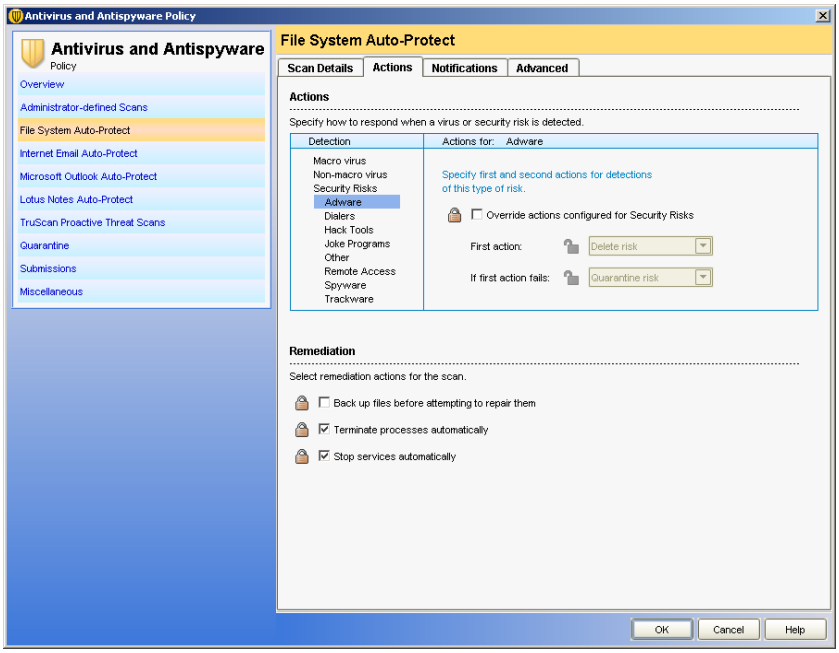
Figura 41. Implementación Antivirus Symantec 1



Fuente. Autor

Protección antivirus y antispyware, protección de correo electrónico, protección de virus de la red, protección proactiva (en línea) de amenazas.

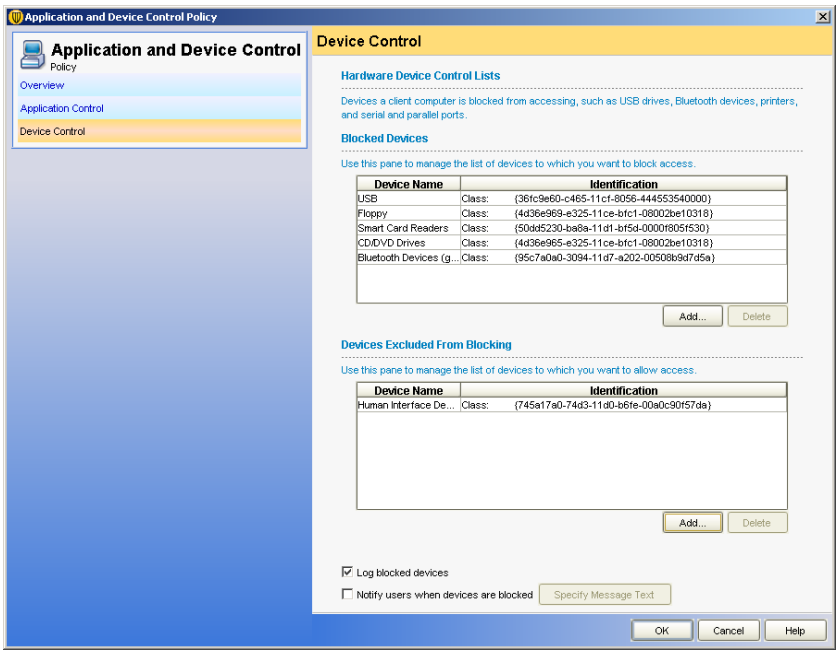
Figura 42. Implementación de Antivirus Symantec 2



Fuente. Autor

Acciones a seguir en la detección de los riesgos de seguridad: Adware, Dialers, Herramientas Hack, Programas Joke, Otros, Acceso remoto, Spyware, Trackware.

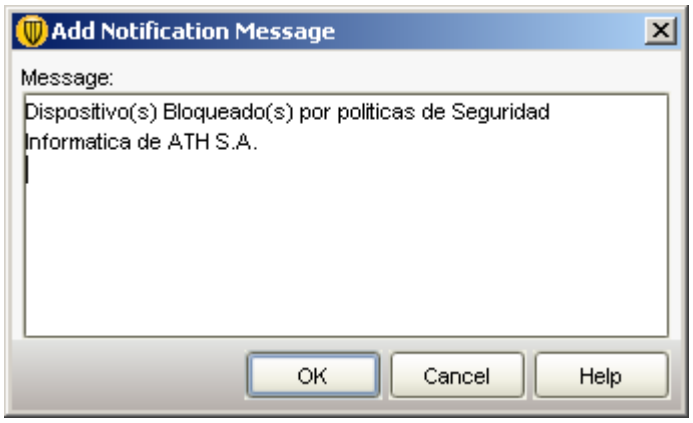
Figura 43. Implementación de Antivirus Symantec 3



Fuente. Autor

Control de dispositivos. USB, Floppy, Smart Card Readers, CD DVD Drives, Bluetooth.

Figura 44. Mensaje de Bloqueo de Dispositivo por políticas empresariales



Fuente. Autor

Texto de notificación al usuario por política de bloqueo. “Dispositivo bloqueado por políticas de seguridad ATH S.A.”

6.7 CAPTURA DE INFORMACIÓN EN LA RED

Cualquier sistema en la actualidad está expuesto a los atacantes que aprovechan las redes de comunicaciones para capturar información de carácter confidencial. Para

disminuir este riesgo es importante contar con sistemas para encriptar datos en todos los protocolos de transferencia de datos del sistema, pero de igual forma no siempre es suficiente usar las técnicas de encriptado para proteger los datos. El área de seguridad de la información en ATH se encarga de vigilar, tener control y administrar la seguridad de la transferencia de datos en la red mediante el uso de distintas técnicas y herramientas de seguridad y evaluación de vulnerabilidades entre las cuales están los anti-sniffers, los packet-sniffers, los honeypots, etc.

6.7.1 Packet sniffers

Los Sniffers son herramientas software que utilizan tarjetas de red o hardware especial con el fin de realizar un monitoreo de datos que circulan por la red y los protocolos usados para el envío de estos. Estos Sniffers que capturan los paquetes de datos que circulan por una red y tienen diferentes utilidades dependiendo del Sniffer entre las cuales las más comunes son clasificación de paquetes, alarmas de paquetes sospechosos, y descifrado de datos. Lo más común para realización de Sniffing es utilizar un equipo conectado a la red con su tarjeta de red (NIC) configurada en modo promiscuo (Modo de captura de datos de la red), para poder procesar todo el tráfico que recibe aunque vaya dirigido a otros equipos. Por otra parte, existen sniffers especializados en la captura de contraseñas u otros datos sensibles (como números de cuenta o tarjetas de crédito).

Herramientas como Ethereal y otras de este tipo son utilizadas en ATH para tareas como monitoreo de la red, evaluación de vulnerabilidades, asignación y remoción de permisos en la red, etc. Estás herramientas facilitan a los encargados de la seguridad tener control y saber que está pasando en la red para analizar la transferencia de datos y por ejemplo revisar paquetes de alguna comunicación que ha alertado un Detector de Intrusos como sospechoso y controlar posibles ataques a la seguridad de la información.

Esta herramienta puede ser utilizada como en el caso empresarial para mejorar la seguridad de la información, pero también puede ser utilizada con fines malintencionados como descubrir contraseñas que viajan por la red, robar información confidencial, y otras. Entre las utilidades para mejorar la seguridad que proporcionan los sniffers, están la detección de virus en la red, la detección de ataques a la red, y otros que se basan en el análisis de la información capturada por la herramienta.

Un ejemplo de uso de esta herramienta es en los Ataques que aprovechan las características del protocolo IP denominado ataque SYN, utilizado para la denegación de servicios de red. Este ataque aprovecha el método que utiliza el protocolo IP para informar del envío y la recepción de datos desde un equipo a otro. Para explicar el funcionamiento del ataque es necesario describir brevemente como se realiza el

establecimiento de una conexión de comunicación mediante el protocolo IP. Primero el Equipo que inicia la comunicación (cliente) envía un paquete SYN al equipo con quien requiere la comunicación (servidor), indicando la solicitud de conexión, luego el servidor responde con un paquete SYN/ACK aceptando la comunicación con el cliente, y por último el cliente valida la conexión con un paquete ACK enviado al servidor. El ataque se realiza enviando ráfagas de paquetes SYN al servidor que se quiere bloquear, con una dirección de remitente que no corresponda a la del cliente desde donde se envían las ráfagas, sino que en cambio, contengan una dirección valida pero que se encuentre fuera de servicio, con el fin de que el servidor intente realizar la comunicación con esta dirección (que no lo va a poder hacer porque esa dirección está fuera de servicio y no va a responder), y así, el servidor espere un tiempo mientras decide anular el intento de conexión. En este tiempo que el servidor intenta establecer la conexión y no puede, el servidor va a estar fuera de servicio ya que no va a poder atender otras solicitudes mientras está intentando el establecimiento de la conexión, por lo tanto mientras trata de establecer todas las conexiones de la ráfaga de solicitudes enviadas, el servidor no responderá a otras solicitudes.

Este ataque es uno de los tantos que es posible detectar con un Sniffer mediante el análisis de las características de los paquetes y protocolos. Entre la gran variedad de sniffers destacan por su importancia los siguientes: TCPDUMP , DARKSTAT Y TRAFFIC-VIS, NGREP, SNORT, NWATCH, ETHEREAL, ETTERCAP y KISMET.

6.7.2 Protección Anti Sniffers

Para prevenir la captura de datos no autorizada en la empresa, ATH también hace uso de las herramientas anti-sniffers que vigilan el tráfico de la red asegurándose de que no existan ninguna clase de amenazas de este tipo. Un ejemplo de la utilidad de estas herramientas es la detección de tarjetas de red inalámbricas configuradas para la captura de datos que se utilizan para el robo de contraseñas de acceso a la red inalámbrica o cualquier otra información que circule por la red wirelless.

Se pueden nombrar "sniffers" y analizadores de protocolos como Nmap, Ntop, NetScanTools, LANSleuth o Ethereal, que permiten detectar protocolos y servicios no autorizados por la organización, además de llevar a cabo un completo análisis del tráfico habitual en la red de una organización (protocolos y servicios utilizados, Cantidad de información transmitida, evolución de la situación por franjas horarias y por días de la semana, comportamiento por segmentos de la red. . .), ya que de este modo será más fácil la detección de situaciones anómalas.

Los sistemas "anti-sniffers" son herramientas capaces de detectar la existencia de tarjetas de red que se encuentren funcionando en modo promiscuo para capturar todo el tráfico de la red. También pueden resultar de gran ayuda las herramientas para la evaluación de vulnerabilidades. Estas herramientas, entre las que se pueden nombrar a Nessus o a Internet Security Scanner, se encargan de llevar a cabo un análisis automático de un sistema informático, para tratar de localizar algunas de las

vulnerabilidades más conocidas. Además, el sondeo de Seguridad complementa al análisis de vulnerabilidades con tareas como la detección y la revisión de la instalación y configuración de los equipos de Seguridad (cortafuegos, antivirus, IDS, etcétera), En este caso, se podrían realizar pruebas de intrusión (tests de penetración), en las que no Sólo se detectasen las vulnerabilidades, sino que se tratasen de explotar aquellas que hayan sido identificadas y que pudieran comprometer el sistema, así como otros sistemas accesibles desde el afectado. Esta tarea se puede completar posteriormente con un análisis de riesgos en el sistema informático, en el que Se pretende determinar cuál es el nivel de riesgo a partir del análisis de posibles amenazas y vulnerabilidades.

Para prevenir el monitoreo no autorizado de paquetes en la red empresarial es aconsejable utilizar los anti-Sniffers, que detectan software y equipos utilizados para estos fines y ayudan a evitar la utilización de estos con fines malintencionados. Existen varias soluciones Anti-Sniffers en el mercado entre las cuales está la de Microsoft llamada PromqryUI y otros.

6.8 SEGURIDAD EN CONEXIONES REMOTAS

Otro aspecto importante en la seguridad empresarial son las conexiones remotas ya que muchas veces son necesarias para la realización de algunos procesos ya sea por comodidad o porque no hay otra forma de ejecutarlos. En los sistemas de ATH se implementan políticas y procedimientos que protegen este aspecto de la seguridad de la información en varios puntos. Estas políticas están diseñadas para garantizar la seguridad mediante el uso de varias herramientas como los protocolos de encapsulamiento de datos de Redes privadas virtuales (VPNs) que son el IPSec,

PPTP, L2F, L2TP o SSL. También con estas políticas se garantiza la confidencialidad, autenticidad e integridad de la información con el uso de algoritmos criptográficos robustos en este tipo de conexiones.

Por otra parte, en lo referente a seguridad de los clientes remotos, hay que tener en cuenta que los equipos de los usuarios remotos son más vulnerables que los internos y están más expuestos a la introducción de virus y otros códigos dañinos fuera de la empresa que dentro de la empresa ya que no cuentan con las medidas de seguridad implementadas en ésta, por esto fuera de la empresa está más expuesta la revelación de información sensible empresarial (por ejemplo si el equipo con conexión remota permitida cae en manos de usuarios maliciosos). Por todo ello, al crear conexiones remotas en ATH se implementan medidas de seguridad adicionales, entre las cuales están:

- ✓ Aislamiento de los equipos remotos: se debe limitar los permisos de acceso de estos equipos y registrar toda actividad sospechosa.

- ✓ Registro de las sesiones abiertas por usuarios remotos, estableciendo temporizadores para detectar y cerrar las sesiones inactivas.

- ✓ Utilización de herramientas (como VNC) para controlar los equipos remotos y poder conectarse a éstos para realizar tareas administrativas o incluso, para proceder a su bloqueo.

Para acceder a la implementación y realizar procedimientos de conexión remota en ATH el usuario que los necesite debe presentar al área de seguridad de la información la solicitud indicando el porqué necesita de éstas herramientas y quién autoriza ésta solicitud (si alguien lo hace), con un formato que se describe a continuación.

- ✓ Formato de solicitud de la conexión remota.

    - o Justificación de la conexión remota: descripción de la finalidad o de las tareas que se van a realizar a través de esta conexión remota.

    - o Recursos requeridos para la conexión.

    - o Periodo y horarios que requiere de ésta conexión.

    - o Adjuntar autorizaciones de Jefes o Personas con autoridad.

Una vez se apruebe la solicitud del usuario, el área de seguridad de la información procede a realizar una capacitación y asesoramiento de cómo se debe realizar la conexión llevando a cabo todos los procedimientos de seguridad para proteger la información de la empresa. También se hace firmar al usuario un documento donde conste que el usuario acepta las condiciones de la empresa, entre las cuales están que va a realizar todas las implementaciones de seguridad indicadas por el personal de seguridad, que no va a divulgar las instrucciones dadas por el personal de seguridad, que no va a divulgar la información entregada para la realización de la conexión remota y cualquier otra información de carácter confidencial.

Después de la inducción se entregan los documentos al usuario:

- ✓ Documentación que se entrega al usuario remoto:

    - Procedimientos de seguridad básicos a seguir para la realización de la conexión remota.
    - Personas de contacto dentro de la organización para poder notificar y tratar de resolver cualquier incidencia.
    - Manuales de instalación y configuración de software para la conexión remota.
    - Confirmación de aceptación de las condiciones de uso de la conexión remota.

Entre las condiciones de seguridad para proceder a la realización de la conexión se encuentra el software necesario de instalar:

- ✓ Software necesario en el equipo remoto para la implementación de la conexión remota

    - Anti-Spyware
    - Firewall
    - Antivirus
    - Anti-Key logger

Así mismo el área de seguridad se encarga de los siguientes aspectos:

- ✓ Aspectos a tener en cuenta por el área de seguridad

    - Mecanismos de autenticación y control de acceso a los recursos
    - Periodo de validez de la conexión.
    - Horario y días en que se permite la conexión.
    - Persona responsable que autoriza la conexión.

6.9 VULNERABILIDADES DE LOS SISTEMAS OPERATIVOS WINDOWS Y EL WSUS

Los sistemas operativos están expuestos a la explotación de vulnerabilidades de seguridad en todo momento y con todo tipo de técnicas ya conocidas como lo son las de Desbordamiento de búfer, Cross Site Scripting, Format strings, Inyección SQL y muchas otras, ya que es imposible contar con un sistema totalmente seguro.

Para proteger este tipo de vulnerabilidades ATH cuenta con el servidor de actualizaciones de Windows WSUS (Windows Server Update Services), que provee a la red empresarial de las actualizaciones de seguridad para corregir vulnerabilidades encontradas en los sistemas operativos Windows. Este Servidor almacena todos los parches y actualizaciones de seguridad que son descubiertas cada día en los sistemas operativos Microsoft Windows y distribuye las actualizaciones a los equipos clientes según la configuración que haya establecido el administrador de WSUS para la red.

En ATH la persona encargada de administrar el servidor WSUS es responsable de la configuración de éste de tal forma que se efectúen las actualizaciones más críticas en todos los equipos y todas las demás posibles sin afectar servicios o generar problemas que puedan afectar los procesos empresariales. Junto con el administrador también las áreas de seguridad, soporte técnico y soporte a la infraestructura están encargadas de este tema y son responsables vigilar los procesos de actualización, informar fallas reportadas y resolver problemas que puedan presentarse con las actualizaciones de los sistemas.

En la web[17] se pueden encontrar las vulnerabilidades y estadísticas encontradas en los sistemas operativos, navegadores, aplicaciones web, puertos, firewalls, etc., incluyendo las más recientes.

Algunas herramientas útiles para la detección de vulnerabilidades son:

- ✓ NSLOOKUP
- ✓ NESSUS
- ✓ NMAP
- ✓ JHON THE RIPPER

[17] Datos actualizados de últimas vulnerabilidades encontradas recientemente en sistemas operativos y aplicaciones, y otros aspectos relacionados con la seguridad informática.
http://www.securityspace.com/smysecure/index.html

6.10 OTRAS VULNERABILIDADES ENCONTRADAS EN ATH

6.10.1 Vulnerabilidad 1: Firewalls inadecuados

La empresa ATH no cuenta con los firewalls externos adecuados para la protección de acceso ya que utilizan firewalls software que no son recomendables para compañías grandes como esta y que manejan el tipo de información crítica que maneja la empresa.

Los firewalls o cortafuegos son programas que se encargan de controlar, permitiendo o denegando las conexiones entrantes y salientes de un computador. Las conexiones ocurren de forma general cuando el usuario se encuentra conectado a Internet o una red local. Estos establecen una barrera entre el computador y la red a la que está conectado, bloqueando el tráfico, discriminando entre aplicaciones permitidas y las que no lo están. Ofrece diferentes niveles de seguridad en función del uso y conocimientos del usuario. En algunos casos también ofrecen la detección de virus y otros códigos dañinos e incorporan filtros anti-spam.

6.10.1.1 Firewalls por software

Los firewall por Software son firewalls básicos que monitorean y bloquean, siempre que sea necesario, el tráfico de Internet. Muchos de estos son gratuitos pero también existen los comerciales que funcionan de la misma forma que uno gratuito (como el de Windows), pero normalmente incluye protecciones extra y mucho más control sobre su configuración y funcionamiento.

Las empresas que producen software de seguridad venden la aplicación firewall exclusivamente o como parte de un paquete de seguridad que incluye otros productos que complementan esta protección, como es el caso de los antivirus. La mayoría de sistemas operativos tienen incluida la instalación de su propio firewall o firewall personales.

Los firewalls por software son los más comunes en empresas pequeñas y medianas, ya que aparte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla. Eso sí, presentan algunos problemas inherentes a su condición: consumen recursos del computador, algunas veces no se ejecutan correctamente o pueden ocasionar errores de compatibilidad con otro software instalado.

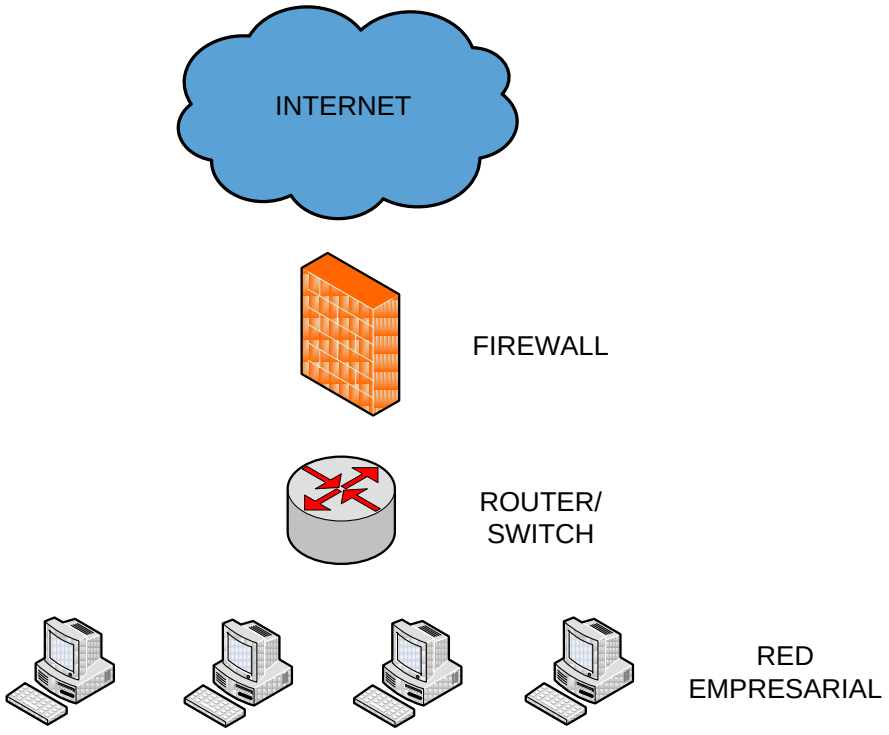
Actualmente, los sistemas operativos más modernos de Windows y Linux integran soluciones básicas de firewall, que pueden ser muy potentes y flexibles, pero requieren un gran conocimiento en redes y puertos necesarios para las aplicaciones.

6.10.1.2 Firewalls por hardware, seguridad apoyada en hardware

Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Estos firewall son exclusivamente diseñados para su trabajo, además tienen el soporte y la garantía del fabricante dependiendo de la calidad y prestigio de los desarrolladores de este y es por eso que son definitivamente la opción más aconsejable de protección perimetral firewall. Los Firewall hardware normalmente son dispositivos que se colocan entre el router empresarial y la red externa, pero todo depende de las necesidades y la infraestructura de la empresa. Como ventajas, se puede destacar, que al ser independientes del computador, no es necesario configurarlos cada vez que se reinstala un sistema operativo, no consumen recursos del sistema y como son exclusivos para esto funcionan de manera óptima.

La correcta conformación de una infraestructura empresarial debería ser parecida a la siguiente gráfica:

Figura 45. Modelo de Infraestructura con firewall por Hardware



Fuente. Autor

6.10.2 Vulnerabilidad 2: Falta de segmentación de red

ATH no cuenta con redes segmentadas adecuadamente en el momento y esto perjudica de muchas maneras la seguridad corporativa, ya que la segmentación de redes mejora muchos de los aspectos de este campo y con un buen estudio e implementación adecuada de la segmentación en la empresa se podrían prevenir cosas como la propagación de virus, ya que si se aíslan los segmentos, un virus que ataque un segmento no se propagaría en las otras redes y así sería mucho más fácil de manejar esta clase de situaciones, o también mejorar la protección de información confidencial ya que los segmentos que no necesiten ningún tipo de conexión con otros que manejen información confidencial serán aislados y no podrán tener acceso a esta información, además de estas también hay otras ventajas al implementar la correcta segmentación de una red.

En este momento en ATH se está empezando a realizar el estudio y las pruebas de implementación que permitan hacer viable la segmentación de la red LAN en segmentos que dividan las áreas para poder hacer una mejor administración de esta red y mejorar aspectos de la seguridad sin afectar el buen funcionamiento de la red para lo que tiene que ver con las actividades laborales.

6.10.2.1 Segmentación de la red

Existen muchas motivaciones que incentivan a realizar una segmentación en redes empresariales. Una de las más importantes es la seguridad de la información empresarial. Al realizar subdivisión de la red en segmentos, cada segmento quedará aislado de los otros y con un correcto análisis e implementación en el proyecto de segmentación se pueden separar los grupos de computadores que requieren tener conexión por red y bloquear el acceso entre computadores que no necesitan conexión a otros según los requerimientos de la empresa. También con la segmentación se hace más fácil la implementación y administración de políticas de seguridad ya que es posible configurar de forma diferente las políticas en cada segmento y personalizar más la seguridad empresarial.

Otro aspecto importante de la segmentación de redes es que con este se pueden configurar las subredes de modo que los equipos que requieran más ancho de banda de red en la empresa, como por ejemplo el departamento de mercadeo que comúnmente trabaja con aplicaciones multimedia en la web o áreas como el de soporte a la infraestructura que requieran constante traslado de archivos por la red empresarial, dispongan de mayor ancho de banda, y las áreas que no requieran muchos recursos de red dispongan de menor ancho de banda, para evitar cuellos de botella e ineficiencias de la red de datos.

También es posible después de realizar el subneteo, implementar dispositivos que adapten la red a las necesidades empresariales, como routers y switches que permitan la conexión de las subredes con características de seguridad personalizadas, firewalls entre subredes que garanticen únicamente los accesos autorizados, y cualquier otra herramienta que permita ordenar la infraestructura tecnológica de la mejor manera posible para cumplir con los objetivos empresariales.

6.10.2.2 Corrección del problema

Actualmente la segmentación de la red de ATH no está correctamente configurada, y debido a los inconvenientes de seguridad que se han venido presentando en la empresa como propagación de virus y accesos no autorizados en la red, se empezó a hacer el diseño de una nueva configuración de la segmentación cuyo principal objetivo es el de dividir la empresa en segmentos de red los cuales abarquen un área de la empresa cada uno.

Esta tarea no es fácil de realizar ya que no solo se trata de realizar la segmentación de la red, sino de hacerlo de tal forma que se puedan implementar fácilmente después todos los demás aspectos de la seguridad del sistema como accesos a recursos, VLANs, comunicación con servidores, etc. El fin de realizar este tipo de segmentación es corregir varios aspectos de la seguridad de la información en la empresa sin alterar las condiciones de trabajo actuales.

Actualmente este proyecto se encuentra en etapa de realización de pruebas para su implementación del cual están a cargo varias áreas de la empresa incluyendo seguridad de la información, telecomunicaciones, soporte técnico, auditoria y soporte a la infraestructura.

7. CONCLUSIONES

La práctica empresarial fue útil para la continuidad de los procesos empresariales dependientes de la infraestructura tecnológica y de comunicaciones, y también se aporto de gran forma en el mejoramiento de estos procesos mediante la realización de exploración de software libre, la aplicación de herramientas especializadas y el aporte en conocimientos de cada uno de los miembros en el área de soporte a la infraestructura, donde se realizó la práctica empresarial. También se respondió de manera eficaz y eficiente a todos los problemas presentados en el software y hardware de los equipos de usuarios empresariales tanto de la sede de la práctica como de las sedes regionales de todo el país, atendiendo los requerimientos para posteriormente analizar los síntomas y proceder a aplicar los correctivos necesarios para normalizar su funcionamiento.

Durante la práctica empresarial se observaron diferentes eventos y situaciones que se viven en el día a día de las labores cotidianas de una empresa de gran magnitud donde se manejan tecnologías de información y comunicaciones muy estructuradas y se tienen varios controles para mantener su correcto funcionamiento. En el presente documento se encuentran dos manuales con información útil que puede servir a cualquier persona que requiera información en temas de mantenimiento a la infraestructura y seguridad de la información enfocados en ambientes empresariales y en la experiencia de la realización de la práctica, donde se ven reflejados acontecimientos usuales o extra usuales de las labores empresariales, en una organización del tipo financiera como lo es la empresa donde transcurrió la práctica.

Es de gran importancia para la competitividad empresarial estar a la vanguardia en todos los aspectos para lograr mantener su imagen por encima de otras empresas del mismo tipo y demostrar que el cumplimiento de sus objetivos empresariales se realiza siguiendo todas las pautas que se están utilizando en la actualidad para posicionarse en el primer lugar del mercado y mejorar la calidad de servicio. Estas pautas de innovación también abarcan las tecnologías de información empresariales y por esto la empresa intenta utilizar las mejores tecnologías de información disponibles en el mercado que permitan satisfacer los aspectos de funcionalidad y seguridad requeridos por la empresa. Durante la práctica se pudo observar cómo se realiza la implementación de innovaciones tecnológicas, mediante la virtualización de la infraestructura de servidores transaccionales de la empresa con la solución virtual Infrastructure.

También de la práctica se concluye que cada vez se están encontrando más y mejores herramientas bajo licencias de software libre que pueden ser implementadas en ambientes empresariales con miras a realizar aportes en cualquier proceso y

mejorando las condiciones de trabajo para el cumplimiento de los objetivos empresariales sin afectar otros procesos y realizándolo con el visto bueno y bajo la aprobación de las directivas empresariales y de las autoridades competentes. Durante la práctica se implemento la herramienta para la realización de inventario de recursos hardware y software e implementación de paquetes OCS Inventory NG, que mejoro los procesos del área de la práctica, haciendo que estos procesos de inventariado y distribución de software se simplificaran y se manejaran digitalmente.

En conclusión, el área de soporte a la infraestructura es de enorme importancia en empresas que manejan importantes tecnologías de información, y dependen del funcionamiento de estas para el cumplimiento de los objetivos empresariales, y con la buena gestión de ésta es posible alcanzar muchos objetivos, incluyendo objetivos económicos, como el posicionamiento en el mercado, la maximización de beneficios, y objetivos sociales como el servicio al cliente y la comodidad de los trabajadores, que son posibles con la implementación de metas representadas en acciones a corto y largo plazo.

8. RECOMENDACIONES

En cualquier procedimiento que se realice a los sistemas de información y que pueda afectar su funcionamiento, es necesario hacer un análisis previo antes de proceder a ejecutar cualquier acción que pueda perturbar algún aspecto de la normalidad de los procesos empresariales, ya que un error causado por la mala toma decisiones o por una acción realizada a la ligera puede ocasionar graves daños a la empresa, y empeorar el problema que se está intentando resolver en vez de finalizarlo con una intervención adecuada. Para esto se debe estudiar y revisar documentación detallada sobre el tema a resolver, y aplicar los conocimientos adquiridos para buscar la solución más adecuada entre las posibles presentadas, analizando sus posibles efectos y consecuencias antes de implementarlas.

Se hace necesario revisar todas las normas legales e institucionales que puedan relacionarse con cualquier proceso que se desee realizar, y además de esto consultar a las autoridades competentes, como los directivos empresariales, revisor fiscal u otras personas que puedan dar su opinión sobre la realización de cualquier acción que pueda perjudicar a la empresa si se incumplen normas establecidas. Por ejemplo en el caso de la implementación de software libre primero se debe consultar con los encargados de la seguridad de la información para la evaluación de vulnerabilidades del software, y también se debe consultar con el encargado de la gerencia tecnológica para evaluar su posible implementación sin afectar otros procesos empresariales.

La cooperación entre las partes de las diferentes áreas empresariales hace posible la viabilidad de proyectos complicados, facilitando las tareas gracias al aporte de conocimientos y gestión de cada uno de los implicados. Se recomienda la realización de proyectos con el apoyo de personas que puedan aportar al desarrollo de sus procesos, en los cuales estas personas tengan experiencia o posean conocimientos que puedan servir para darle continuidad cuando se dificulten las gestiones o no se tenga claridad de cómo proceder en cualquier evento.

También es necesario priorizar las actividades a realizar de acuerdo a las necesidades empresariales, empezando por la realización de actividades críticas para las labores empresariales y dejando en último lugar las actividades de mínima importancia que puedan esperar sin ser perceptibles y sin afectar ningún elemento indispensable en la infraestructura.

9. REFERENCIAS

LIBROS

[1] Anderson Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems. Softcover Black & White International Edition, U.S.A., 2008.

[2] Daltabuit Godás E., Hernandez Audelo L., Mallén Fullerton G., Vázquez Gómez J., La Seguridad de la Información. LIMUSA NORIEGA EDITORES. México, 2007.

[3] Gómez Vieites Á., Enciclopedia de la seguridad informática. ALFAOMEGA GRUPO EDITOR, S.A de C.V., México, 2007.

[4] Laporte Leo y Soper M. Edward, Mantenimiento y reparación del PC. Editorial ANAYA MULTIMEDIA. Madrid, España, 2007.

[5] MCSA/MCSE, Guía de estudio oficial de certificación 70-270. Microsoft Windows XP Professional. McGRAW-HILL/INTERAMERICANA DE ESPAÑA, S.A.U, Madrid, 2002.

[6] Stallings W., Sistemas Operativos, Principios e Interioridades. PRENTICE HALL, PEARSON EDUCACIÓN, S.A., Madrid, 2001.

DOCUMENTOS

[7] ATH Políticas y procedimientos, Documentos de políticas y procedimientos públicos, implementados en la empresa A Toda Hora S.A.

[8] OCS_Inventory_NG Installation and Administration Guide 1.9 EN.pdf, Documento guía para la instalación y configuración de la herramienta OCS Inventory NG para inventario informático e implementación de paquetes.

[9] Vmware Infrastructure 3: Install and Configure, Manual de Instalación y configuración de la infraestructura virtual VMware en ATH.

SITIOS WEB

[10] e-TECH SOLUTIONS, Contenidos de libros, revistas, periódicos y mapas de librerías virtuales de todo el mundo, que aportan conocimiento sobre tecnologías de información entre otros. http://www.etechwebsite.com

[11] Ferrer F., Blog Al Final de la Rambla, Contenidos sobre administración del Departamento de Sistemas Informáticos y computación (DSIC) de la Universidad Politécnica de Valencia, España. http://fferrer.dsic.upv.es

[12] GNU Operating System, Sistemas Operativos GNU/Linux desarrollados desde una colección de librerías, aplicaciones y herramientas de desarrollo en software libre. http://www.gnu.org/

[13] Informática Jurídica, Contenidos actualizados de la legislación jurídica en varios países incluyendo las leyes Colombiana. http://www.informatica-juridica.com/legislacion/colombia.asp

[14] Kioskea, Contenidos Informáticos. Página web con todo tipo de contenidos (foros, artículos, software, …) relacionado con informática. http://es.kioskea.net/

[15] Microsoft, Empresa multinacional Estadounidense, desarrolladora de Tecnologías Informáticas. http:// www.microsoft.com

[16] OCS Inventory next generation, Sistema de Inventarios e implementación de paquetes para sistemas Operativos Windows y Unix. http://www.ocsinventory-ng.org/
[17] Reyes F. Artículos, Artículos relacionados y enfocados en la administración de Sistemas Operativos Microsoft. http://freyes.svetlian.com

[18] TechNet, Comunidad que proporciona una amplia perspectiva sobre temas actuales de tecnologías de información. Los contenidos más manejados son seguridad, Optimización de Infraestructura y Sistemas Operativos Microsoft. http://technet.microsoft.com/es-es

[19] VMware Inc, Corporación desarrolladora de herramientas software de virtualización para equipos o infraestructuras. http://www.vmware.com/

[20] Wikipedia, Enciclopedia de libre acceso. Proyecto de la fundación sin ánimo de lucro Wikimedia, que contiene artículos de toda clase de temas y en diferentes idiomas, útiles para el desarrollo del conocimiento. http://www.wikipedia.org

10. ANEXOS

Anexo A. Ley de la protección de la información y de los datos

Ley aprobada por:

El presidente del horable senado de la república: Hernan Andrade Serrano.

El secretario general del honorable senado de la república: Emilio Ramon Otero Dajud.

El presidente de la honorable cámara de representantes: German Varon Cotrino.

El secretario general de la honorable cámara de representantes: Jesus Alfonso Rodriguez Camargo.

“

Ley nº 1273 05 ene 2009

"POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO - DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACÍÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES".

El congreso de Colombia Decreta:

ARTÍCULO 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTÍCULO 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique *o* emplee códigos personales, datos personales contenidos en archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en

los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO

De las atentados informáticos y otras infracciones

ARTÍCULO 2691: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

ARTÍCULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

ARTICULO 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:
A**rticulo 58 CIRCUSTANCIAS DE MAYOR PUNIBILIDAD**. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos ó telemáticos.

ARTICULO 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Articulo 37. DE LOS JUECES MUNICIPALES. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el titulo VII Bis.

ARTICULO 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal."

Anexo B. Ejemplo de política corporativa implementada en la empresa ATH para manejo de certificados digitales: Política de declaración de prácticas de certificación digital

Política implementada en la empresa ATH que describe el manejo que se le debe dar a las certificaciones digitales utilizadas en la Organización.

Aprobada por: Presidencia ATH

“

- ✓ **Objetivo de la política**

Implementar una entidad certificadora cerrada que permita garantizar la confidencialidad e integridad en el envío y recepción de correo electrónico Microsoft Exchange. Garantizar la confidencialidad de la información almacena en los discos duros de las estaciones de trabajo de los funcionarios de ATH S.A.

- ✓ **Alcance de la política**

La entidad certificadora cerrada debe ser utilizada por todos los funcionarios de ATH que tengan instalado el cliente de correo electrónico Microsoft.

- ✓ **Introducción al servicio de certificación digital**

  - o **Aspectos Generales**

La entidad de certificación requerida por el grupo Aval, es necesaria para la generación de certificados digitales de múltiples propósitos que permiten, entre otras funcionalidades, el establecimiento de conexiones seguras en la red, el cifrado de información, el envío de mensajes de correo electrónico seguros y el aseguramiento de servidores Web. Los certificados digitales emitidos por la entidad de certificación cerrada de ATH serán interoperables al interior de la organización y con los suscriptores externos de la entidad de certificación. Estas características se vuelven indispensables para mantener la seguridad general de los diferentes sistemas, y para protegerlos de accesos no autorizados, tanto a los equipos como a la información almacenada en los mismos.

La Entidad de Certificación Cerrada tiene una raíz que se ubicará en ATH y que será la encargada de expedir certificados para las diferentes subordinadas o ramas del árbol de la entidad de certificación cerrada, las subordinadas de esta raíz se ubican en cada uno de los árboles de directorio activo para hacer la emisión de los certificados específicos de cada árbol, siendo administradas por personal específico en cada entidad y supervisadas por el administrador principal de la entidad de certificación cerrada de ATH - A Toda Hora S.A. De esta forma la Base de Datos de los certificados digitales expedidos por cada subordinada podrá ser accedida y gestionada independientemente de las demás Entidades de Certificación del Grupo. Dicha Base de Datos residirá en el servidor donde se implementará dicho servicio. A la fecha se encuentran una raíz de certificación y 5 subordinadas una ubicada en ATH, una en el Banco de Bogotá y una en el Banco de Occidente.

- Funciones de la Entidad de Certificación Digital

Las funciones de la Entidad de Certificación son la configuración, expedición, renovación y revocación de los certificados digitales, tanto para usuarios de la red como para equipos o servidores que los requieran. El administrador de la Entidad estará en capacidad de administrar todas las funcionalidades de la misma y de configurar los parámetros relacionados con la expedición de certificados digitales.

- Funciones de los certificados digitales

Los certificados digitales contienen información sobre el usuario o equipo al que son emitidos, la llave pública del certificado, la Entidad de Certificación que lo emitió y otra información adicional como un número id. único, una fecha de inicio y finalización de la validez del certificado, el propósito del certificado (función o servicio que presta), los algoritmos de cifrado y firma digital, y la ubicación de las listas de revocación (CRL) donde se puede verificar si el certificado ha sido o no revocado, entre otros.

Tabla 13. Tipos de servicios o certificados digitales emitidos por la entidad certificadora.

Tipo de certificado o servicio	Descripción
Correo electrónico Seguro	Permite el envío de mensajes de correo electrónico tanto firmado como cifrado para proteger su contenido durante la transmisión, así como identificar su origen.
Autenticación segura	Permite la autenticación de los usuarios a los servidores de forma segura por medio de la utilización de

	certificados digitales.
Aseguramiento de servidores Web	Permite cifrar el tráfico entrante y saliente del servidor Web hacia los clientes Web para proteger su contenido de usuarios no autorizados.
Protección de comunicaciones	Permite el cifrado del tráfico entre dispositivos de red y servidores por medio del protocolo IPSec utilizando certificados digitales.
Protección de Información Almacenada	Permite cifrar el contenido de archivos y directorios en las máquinas de los usuarios de forma que no pueda ser accedida por usuarios no autorizados.
Definición de Entidades Subordinadas	Permite emitir certificados a Entidades de certificación Subordinadas para ampliar la jerarquía de certificación y distribuir los servicios de la Entidad en la Organización.
Firmado de código	Permite firmar digitalmente los componentes de software desarrollados de forma que se garantice su origen y su integridad cuando son instalados por los usuarios.

Fuente. ATH

Los certificados digitales emitidos por la Entidad cumplen con el estándar X.509 versión 3 de la IEEE, lo que garantiza un óptimo nivel de confiabilidad en el aseguramiento de la información y una amplia compatibilidad con el software existente. Siempre que un dato o un certificado sean alterados sin previa autorización, el usuario podrá enterarse de la situación mediante notificaciones del software para tomar las medidas del caso.

- Vigencia de los certificados Digitales:

Los certificados digitales expedidos por la Entidad de certificación para los usuarios tienen una vigencia de un año, luego del cual los certificados podrán ser renovados o revocados de acuerdo a las necesidades. La Entidad de Certificación cuenta con una base de datos de certificados, entre los que se encuentran los certificados emitidos, pendientes y revocados y con base en la cual se generan los archivos con las listas de revocación (CRL) que son usadas por el software de los clientes para verificar el estado de los certificados.

Así mismo, el certificado digital de la Entidad de Certificación pude tener una validez que será definida por ATH por el número de años que se requiera, período luego del

cual dicho certificado podrá ser renovado. El valor recomendado y que sugieren las mejores prácticas es de 5 años, y que puede ser renovado en cualquier momento por los Administradores de la Entidad de Certificación. El proceso de renovación de la Entidad no requiere que se cambien configuraciones en particular para la Entidad, ni que se re-generen los certificados de los usuarios, ya que se puede habilitar la opción de conservar las llave existentes durante la renovación.

Sólo en el caso en que se sospeche del compromiso de la llave privada de la Entidad, se deberá revocar el certificado actual y renovarlo con un juego nuevo de llaves, en cuyo caso, se deberán expedir de nuevo los certificados para los usuarios que previamente obtuvieron certificados de la Entidad Original.

Considerando que los certificados digitales emitidos por la Entidad nunca pueden tener un período de validez superior al del certificado de la Entidad misma, se debe ejecutar la renovación del certificado de la Entidad por lo menos con un (1) año de anticipación (es decir al cumplirse el cuarto año de validez de la Entidad) para evitar que los certificados expedidos por la misma tengan períodos de validez de menos de un (1) año.

El proceso de renovación del certificado de la entidad de certificación no altera el funcionamiento de los certificados previamente emitidos ya que se puede conserva el mismo juego de llaves criptográficas durante la renovación.

- Normatividad del uso de los certificados digitales:

ATH definirá cuáles serán las normas que rijan el uso de los Certificados Digitales, qué personas dentro de la empresa podrán solicitarlos y cuál será la política de renovación y revocación de los mismos. Las normativas básicas necesarias para la implementación y operación de la Entidad de Certificación se encuentran incluidas en los manuales “Manual de instalación de la Entidad” y “Administración de la Entidad”.

- Funcionarios de la Entidad de Certificación:

Para la gestión y operación de la Entidad de Certificación se requiere personal con el siguiente perfil:

- ✓ Administrador de la Entidad: Personal capacitado en Sistema Operativo Windows 2000 Server y en conceptos de Entidades de Certificación, encargado de la configuración y gestión de la Entidad.

- ✓ Autoridad de registro (RA): Personal idóneo de alta confianza y con conocimientos en el Sistema Operativo Windows 2000 Server y en Entidades de Certificación, encargado de verificar la identidad y autorizar a las personas o entidades que solicitan certificados digitales a la Entidad.
- ✓ Soporte de la Entidad: Personal capacitado en Sistema Operativo Windows 2000 Server y en conceptos de Entidades de Certificación, encargado de la operación, respaldos e instalación de los certificados digitales para los diferentes propósitos.

- ✓ **Declaración de prácticas de Certificación**

La entidad de certificación cerrada prestará servicios de emisión de Certificados Digitales a los empleados, clientes y proveedores de ATH que requieran por sus cargos o relación con la Organización de este tipo de servicio, este documento recopila la información sobre las normas establecidas para su puesta en marcha y operación.

- o Repositorios

Los sistemas de almacenamiento de los certificados digitales para los usuarios y las listas de revocación para consulta se encuentran ubicados en los siguientes puntos. La información sobre la Raíz Enterprise de la Entidad de Certificación Cerrada de ATH - A TODA HORA S.A. es:

Nombre Servidor: Root1.organización.net
Nombre CA: ROOTAVALCERTIFICA
Dominio: organización
Email: rootac@ath.com.co
Ubicación CRL Externa: iAs
Ubicación CRT Externa: iAs
URL Sitio Web de la Entidad: www.ath.com.co

La información sobre la Subordinada Enterprise de la Entidad de Certificación Cerrada de ATH - A TODA HORA S.A. Ubicada en ATH es:

Nombre Servidor: DCBOGATH1
Nombre CA: ATHCERTIFICA
Dominio: organización
Email:
Ubicación CRL Externa: iAs

Ubicación CRT Externa: iAs
URL Sitio Web de la Entidad: www.ath.com.co

La información sobre la Subordinada Enterprise de la Entidad de Certificación Cerrada de ATH - A TODA HORA S.A. Ubicada en Banco de Bogotá es:

Nombre Servidor: Zeus 1
Nombre CA: BancodeBogotaEnt
Dominio: BancodeBogota.net
Email: Backoffice@bancodebogota.com.co
Ubicación CRL Externa:
http://servicios.bancodebogota.com:443/CAEnterprise/CRL/BancodeBogotaEnt.crl
Ubicación CRT Externa:
http://servicios.bancodebogota.com:443/CAEnterprise/Cert/zeus01.bancodebogotaEntnet_BancodeBogota.crt

- ✓ **Provisiones Generales**
    - Obligaciones y responsabilidades

El acuerdo de suscripción se proporciona como un apéndice, todo usuario (interno o externo) debe aceptar este acuerdo para aplicar para la emisión de un certificado.

Aquí se deben incluir adicionalmente las normativas y responsabilidades internas y de terceros o proveedores para el uso de los certificados en los diferentes casos, de acuerdo con lo que defina la Gerencia de la Organización de ATH. Algunos de los puntos que se deben incluir son:

- Emisión de certificados por primera vez
- Procedimiento de entrega y configuración
- Actualización de datos
- Cambio de empleados
- Solicitud de renovación de certificados
- Solicitud de revocación de certificados
- Procedimiento de paz y salvo en caso de retiro de empleados
- Procedimiento en caso de compromiso de la llave privada de un usuario (Revocación y expedición de un certificado nuevo)

Es responsabilidad de los administradores de la Entidad Subordinada, el mantener la plataforma de forma que se garantice la disponibilidad de los servicios descritos

anteriormente en este documento y de acuerdo con los procedimientos y manuales definidos para los diferentes casos descritos en este documento.

- ✓ **Identificación y Autenticación**

    - Unicidad de Nombres (convenciones)

Cada certificado digital expedido por la entidad corresponderá a un usuario en particular y es de uso personal e intransferible. A su vez cada usuario podrá utilizar más de un certificado digital dependiendo de las necesidades de su cargo.

    - Método para probar posesión de la llave privada de los certificados de las Entidades sub-ordinadas expedidas por la Entidad Raíz

Solo el personal autorizado de ATH está autorizado para generar llaves privadas para la entidad de certificación. Este personal autorizado deberá ser miembro del grupo de Administradores de la Entidad de Certificación. Adicionalmente el lugar donde se almacene la copia de respaldo de la llave privada de la entidad de certificación debe ser seguro para no comprometer la integridad de la misma.

En el caso en que se sospeche del compromiso de la llave privada de la Entidad, se deberá revocar el certificado actual y renovarlo con un juego nuevo de llaves, en cuyo caso, se deberán expedir de nuevo los certificados para los usuarios que previamente obtuvieron certificados de la Entidad Original.

Además de los aspectos ya mencionados en la política de seguridad se incluyen los aspectos siguientes:

- ✓ Consideraciones y Requerimientos Operacionales

- ✓ Seguridad Física, Tecnológica, Procedimental y de Personal

- ✓ Respaldo y Contingencia

- ✓ Administración de la entidad de certificación

- ✓ Procesos asociados

- ✓ Documentos y registros referenciados

”