AUDITORÍA INFORMÁTICA A LA PARTE FÍSICA Y LÓGICA DE LA RED DE DATOS EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. SEDES CORPORATIVA PASTO Y SEDES ALTO PUTUMAYO

DIEGO ALEXANDER ACOSTA
HEIDER HENRY QUETAMA CAICEDO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

AUDITORÍA INFORMÁTICA A LA PARTE FÍSICA Y LÓGICA DE LA RED DE DATOS EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. SEDES CORPORATIVA PASTO Y SEDES ALTO PUTUMAYO

Trabajo de grado presentado como requisito para optar al título de Ingeniero de Sistemas

DIEGO ALEXANDER ACOSTA
HEIDER HENRY QUETAMA CAICEDO

Director
FRANCISCO SOLARTE SOLARTE
Mg. Maestría en Docencia

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

NOTA DE RESPONSABILIDAD

"Las ideas y conclusiones aportadas en el presente trabajo son de responsabilidad exclusiva de su autor".

Art. 1º del Acuerdo No. 327 del 11 de octubre de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

"La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor".

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico

NOTA DE ACEPTACIÓN

_____
_____
_____

_____
Jurado

_____
Jurado

San Juan de Pasto, Abril 2015

AGRADECIMIENTOS

A nuestros padres y familiares que nos apoyaron a lo largo de nuestra carrera que estuvieron junto a nosotros brindándonos su comprensión y su apoyo incondicional, para cumplir con nuestro sueño de ser profesionales.

Al ingeniero Francisco Solarte por orientarnos, brindarnos sus conocimientos, por su apoyo y compromiso en el desarrollo de este trabajo de grado.

Al ingeniero Edgar Rodríguez, por su apoyo, asesoría y compromiso con el desarrollo de este trabajo de grado.

Al ingeniero Harold Caicedo, Jefe del Área de Sistemas de Emssanar E.S.S, por permitirnos aplicar y ampliar nuestros conocimientos en esta reconocida empresa de salud, por brindarnos su confianza y apoyo.

Al ingeniero Diego Bastidas, administrador de la red, auxiliar de mantenimiento y soporte técnico en el área de sistemas Emssanar E.S.S, por su apoyo y buena disposición para llevar a cabo este trabajo de grado.

A todos ellos, gracias, por su apoyo en el desarrollo de este proyecto.

Diego Alexander Acosta

En primer lugar doy gracias a Dios, por haberme permitido alcanzar este sueño.

Agradezco a mis amados padres, quienes han sabido guiarme por el camino del bien con su cariño y sabiduría.

Un agradecimiento muy especial a mi esposa, por estar conmigo en estas etapas de mi vida brindándome su apoyo y comprensión, muchas gracias.

De igual manera quiero agradecer a nuestro director Ing. Francisco Nicolás Solarte, su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia en un marco de confianza, afecto y amistad, fundamentales para la culminación de este trabajo.

Quiero también dar mi gratitud al Ing. Edgar Enríquez por su asesoría a lo largo del proyecto.

Al ingeniero Harold Caicedo, Jefe del Área de Sistemas de Emssanar E.S.S, por permitirnos realizar nuestro proyecto en la Emssanar E.S.S, por brindarnos su confianza y apoyo.

Al Ing. Diego Bastidas administrador de la red de datos de Emssanar E.S.S un agradecimiento enorme por la confianza depositada en nosotros, por brindarnos toda la información necesaria para el proyecto, por su amabilidad y profesionalismo en todas las etapas del proyecto ya que siempre mantuvo abiertas sus puertas para nosotros.

A todos ellos muchas gracias.

Heider Henry Quetamá Caicedo

DEDICATORIA

A Dios por brindarme la oportunidad de formarme como profesional, por permitirme alcanzar mi sueño de ser ingeniero de sistemas.

A mis padres y familiares cercanos, que me brindaron su apoyo incondicional y confianza, para seguir por este camino hasta llegar a un feliz término, de llegar a ser un excelente Ingeniero de Sistemas.

Diego Alexander Acosta.

Dedico este proyecto en primer lugar a Dios, por enseñarme el camino correcto de la vida, por levantarme en los momentos más difíciles y guiarme con su sabiduría para poder cumplir mis metas en la vida.

También dedico este proyecto, con todo mi amor a los seres más importantes en mi vida, mis padres María Luisa Caicedo y Campo Elias Quetamá, quienes me han brindado su amor y apoyo para alcanzar uno de los retos más importantes, junto a mis dos grandes tesoros y razón de vivir mi hijo Santiago Quetamá y mi esposa Maritza Rodríguez quienes se convirtieron en mis compañeros inseparables.

Heider Henry Quetamá Caicedo

RESUMEN

La auditoría a la entidad de Salud Emssanar E.S.S, en el área de sistemas tiene como objetivo principal evaluar los procesos en la parte del hardware y software de la red de datos que esta organización maneja, identificando las dificultades o falencias de esta, así como también auditar la seguridad física y lógica.

Para el desarrollo de esta auditoría se tomó como marco de referencia el enfoque COBIT (objetivos de control para tecnologías de la información), dentro de este encontramos los procesos y dominios, planear y organizar, adquirir e implantar, entregar y dar soporte, monitorear y evaluar. Posteriormente, se eligieron los procesos con sus respectivos objetivos de control de tal manera que estuvieran acorde con los objetivos de esta investigación.

Junto con lo anterior, se elaboraron fuentes de conocimientos, cuestionarios cuantitativos, entrevistas, plan de pruebas y la matriz de probabilidad e impacto para calificar los diferentes hallazgos encontrados.

Una vez terminado el proceso de auditoría y teniendo en cuenta la misión y visión de la entidad de salud Emssanar E.S.S. se elaboraron las conclusiones, recomendaciones y un plan de mejora respecto a la seguridad física y lógica de la red de datos del área de sistemas.

ABSTRACT

The audit of the entity Health Emssanar E.S.S in the systems area 's main objective is to evaluate the processes on the part of the hardware and software data network that handles this organization, identifying difficulties or shortcomings of this, as well as audit the physical and logical security.

For the development of this audit was taken as the COBIT framework approach (Control Objectives for Information Technology), within this are the processes and domains, plan and organize, acquire and implement, deliver and support, monitor and evaluate. Later processes with their respective control objectives so that they were consistent with the objectives of this research were chosen.

Along with this, sources of knowledge, quantitative questionnaires, interviews, test plan and the probability and impact matrix to describe the different findings were developed.

Once completed the audit process and taking into account the mission and vision of the organization of health Emssanar E.S.S, conclusions, recommendations and a plan of improvement on the physical and logical security of the data network systems area were developed.

CONTENIDO

Pág

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

ANEXOS

Los anexos relacionados a continuación se entregan por medio magnético en CD y se adjuntan al presente informe.

ANEXO 1. Procedimiento planeación de infraestructura y soporte tecnológico.

ANEXO 2. Entrevistas Diego Bastidas.

ANEXO 3. Manual de plataforma Tecnológica.

ANEXO 4. Imágenes cableadas.

ANEXO 5. Falta de señales de seguridad.

ANEXO 6. Diagrama de red.

ANEXO 7. Entrevista seguridad lógica.

ANEXO 8. Imágenes cubículos.

ANEXO 9. Imágenes sin filtro.

ANEXO 10. Inventario de equipos de Emssanar.

ANEXO 11. Lista de chequeo.

ANEXO 12. Listado de Ips e imágenes.

ANEXO 13. Pruebas de intrusión.

ANEXO 14. Entrevistas y checklist.

ANEXO 15. Cobit marco teórico.

ANEXO 16. Manual de Funciones Emssanar E.S.S.

GLOSARIO

ANSI: Instituto Americano de Estándares Nacionales (American Nacional StandardsInstitute).

ANCHO DE BANDA: es la medida de datos y recursos de comunicación disponible oconsumida expresados en bit/s o múltiplos de él (kbit/s, Mbit/s, entre otros).

ATM: El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Administración: El método de etiquetar cables, identificar, documentar y efectuar movimientos, adiciones y cambios al cableado y canalizaciones.

Área de trabajo: Espacio en el edificio, contenedor o taller donde los usuarios interactúan con el equipo terminal**.**

BROADCAST: En castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

BACK BONE: El cable principal en una red.

Cable (cordón) de equipo: Cable o ensamble de cables usado para conectar equipo al cableado horizontal o principal.

Cableado: Conjunto de cables, alambres, cordones y elementos de conexión.

Cable de fibra óptica: Ensamble que consiste en uno o más hilos de fibra óptica.

Cable híbrido: Ensamble de dos o más cables del mismo o de diferente tipo o categoría, cubiertos por un mismo forro o cubierta.

Conmutador de Paquetes: La conmutación de paquetes es el envió de datos en una red de computadoras. Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, en la que está especificado la ruta a seguirá lo largo de la red hasta el destino del paquete. Mil octetos es el límite de longitud superior de los paquetes, y si la longitud es mayor el mensaje se fragmenta en otros paquetes.

Cuarto de equipos: Espacio destinado para alojar el equipo principal, así como las terminaciones de cable y los distribuidores de cableado de piso, Campus y/o edificio.

Dirección IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo(habitualmente una computadora) dentro de una red que utilice el protocolo IP (InternetProtocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar. Esta dirección puede cambiar 2 ó 3 veces al día; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Equipo: Equipo electrónico digital de telecomunicaciones utilizado para proporcionar al usuario los servicios de voz, datos y video. Por ejemplo: conmutadores de redes de área local, conmutadores de tecnología ATM, concentradores de datos, multiplexores ópticos, entre otros muchos más.

ETHERNET: La tecnología de LAN más popular actualmente. La norma IEEE 802.3define las reglas para configurar una red Ethernet. Es una red CSMA/CD de banda base a10 Mbps, que funciona con cableado coaxial fino y grueso, par trenzado y fibra óptica.

EIA: ("Telecommunications Industry Association") Asociación de las industrias de telecomunicaciones.

Fibra óptica: Tipo de cable que se basa en la transmisión de información por técnicas opto eléctricas mediante una combinación de vidrio y materiales plásticos. A diferencia del cable coaxial y del par trenzado no se apoya en los impulsos eléctricos, sino que transmite por medio de impulsos luminosos. Se caracteriza por un elevado ancho de banda con alta velocidad de transmisión y poca pérdida de señal.

FIREWALL: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorpora relementos de privacidad, autentificación, etc.

FRAME RELAY: FrameRelay o (Frame-modeBearerService) es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducido por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite

una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

FAST ETHERNET: Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo). El nombre Ethernet viene del concepto físico de ether. En su momento el prefijo fastse le agregó para diferenciarla de la versión original Ethernet de 10 Mbps.

GATEWAY: Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Gabinete: Conector para alojar accesorios de conexión, cableado y equipo activo.

HOST: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (ssh, FTP, www, email, etc.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

IP: Protocol Internet.

IEEE 802.1D: Es el estándar de IEEE para bridges MAC (puentes MAC), que incluye bridging (técnica de reenvío de paquetes que usan los switches), el protocolo Spaning Treey el funcionamiento de redes 802.11 entre otros.

ISO: Organización de Estándares Internacionales (Internacional Standards Organization).

LAN: Una red de área local, red local o LAN (del inglés local área network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite una conexión entre dos o más equipos.

Multicast: En español significa multidifusión, es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen. En oposición a multicast, los envíos de un punto a otro en una red se denominan unidifusión (inglés unicast), y

los envíos a todos los nodos en una red se denominan difusión amplia (inglés broadcast)

LAN: Red de Área Local (Local Área Network).

MAC: En redes de computadoras la dirección MAC (Media Access Control address o dirección de control de acceso al medio) es un identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

OSI: Open SystemInterconnection es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

PBX: PrivateBranch Exchange se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior.

Puente de red: Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Estén interconectados los segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

Router: En español significa direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red).Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar e lpaquete de datos.

RSTP: Rapid SpanningTreeProtocol (RSTP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. Especificado en IEEE802.1w, es una evolución del Spanningtree Protocol (STP), reemplazándolo en la edición2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

STP: es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC

SISTEMA DE INFORMACIÓN: Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

TIA: ("Electronic Industries Alliance") Asociación de Industrial Electrónicas.

TOPOLOGÍA: La arquitectura o topología de red es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, mediante la combinación de estándares y protocolos.

TOPOLOGÍA DE RED: La arquitectura o topología de red es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, mediante la combinación de estándares y protocolos. Define las reglas de una red y cómo interactúan sus componentes. Estos equipos de red pueden conectarse de muchas y muy variadas maneras.

TCP/IP: Protocolo de Control de Transmisión / Protocolo de Internet (Transmission Control Protocol/Internet Protocol)

UTP: Cable par trenzado sin blindar.

UDP: son las siglas de Protocolo de Datagrama de Usuario (en inglés User Datagram Protocol) un protocolo sin conexión que, como TCP, funciona en redes IP. UDP/IP proporciona muy pocos servicios de recuperación de errores, ofreciendo en su lugar una manera directa de enviar y recibir datagramas a través una red IP

UTP: Par trenzado sin blindar.

VLAN: Las VLAN es una LAN virtual. Un grupo de dispositivos de una LAN que están configurados (con software de administración) de forma que se puedan comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, se encuentran en una serie de segmentos LAN diferentes. Dado que las VLAN se basan en la lógica en vez de sobre conexiones físicas, son extremadamente flexibles.

INTRODUCCIÓN

La Empresa Solidaria de Salud Emssanar E.S.S, actualmente maneja una red informática grande, puesto que tiene una plataforma tecnológica distribuida, en el departamento de Nariño, en el alto Putumayo, en el Cauca y Valle; la sede principal se encuentra en la ciudad de Pasto desde donde se administra y se monitorea a las demás sedes.

Para Emssanar E.S.S las redes de datos, computadoras y comunicaciones, son muy útiles, ya que mediante ellas se proporciona la capacidad y los elementos necesarios para el intercambio de información y/o comunicación, ya sea en forma de voz, datos, video o una mezcla de los anteriores, así como también compartir recursos Hardware, datos y programas, licencias de sitio y aplicaciones para trabajo en grupo de una manera rápida, efectiva y a distancia.

Teniendo en cuenta la importancia de la red de datos en la Empresa de salud Emssanar E.S.S, se hace necesario evaluar el desempeño y seguridad de la misma, para ello se desarrolla una auditoría informática en redes, la cual consiste en una serie de mecanismos que evalúan la red tanto en la parte lógica y física, con el fin de lograr una utilización más eficiente y segura de la información.

Por lo tanto, este proyecto tiene como objetivo realizar una auditoría informática a la red de datos de la empresa solidaria de salud Emssanar E.S.S, con el fin de evaluar cómo están funcionando la seguridad de la infraestructura y seguridad lógica de la red de datos y así identificar posibles fallas, debilidades o fortalezas y realizar un plan de mejora con las recomendaciones a los hallazgos encontrados en la auditoría.

IDENTIFICACIÓN DEL PROBLEMA

TÍTULO DEL PROYECTO

AUDITORÍAA LA SEGURIDAD FÍSICA Y LÓGICA DE LA RED DE DATOS EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. SEDES CORPORATIVA PASTO Y SEDES ALTO PUTUMAYO.

TEMA: auditoría aplicada al área de sistemas, a la parte física y lógica de la red de datos de la Empresa Solidaria de Salud Emssanar E.S.S de Nariño.

MODALIDAD: este trabajo de grado, corresponde a la modalidad de trabajo de aplicación, a realizarse en la EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S, donde permitirá ampliar conocimiento y generar diferentes alternativas de desarrollo empresarial a través de la aplicación de métodos de organización, funcionamiento y aplicación y cumplimiento de políticas, leyes y normas, necesarios para el funcionamiento de una empresa.

LÍNEA DE INVESTIGACIÓN: según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de facultad 045 de octubre 10 de 2002 dado por el honorable consejo de la facultad, el proyecto corresponde a la línea de investigación de Sistemas Computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de auditoría de sistemas

DEFINICION DEL PROBLEMA

Planteamiento del problema. Debido al amplio cubrimiento que presenta la empresa Solidaria de Salud del Régimen Subsidiado, Emssanar E.S.S, existen zonas en las cuales se han presentado fallas de conexión entre las sedes, generando inconvenientes para la entidad tanto en lo referente a la atención de los usuarios como en la demora de los procesos que se llevan a cabo diariamente.

En este sentido, también cabe anotar lo siguiente: no hay antecedentes de auditorías informáticas que se hayan ejecutado en cuanto a la seguridad lógica y de la infraestructura sobre la red de datos en la empresa Emssanar E.S.S.

Por otra parte, la perdida de conexión entre las sedes puede ser causada por diferentes factores como las fallas en la infraestructura de la red o por ataques externos de personas malintencionadas e incluso del mismo personal que trabaja en la entidad, los cuales pretenden conseguir la información con la que cuenta la empresa

Formulación del problema. ¿Cómo la ejecución de una auditoría informática a la parte lógica y física de la red de datos, en la Empresa Solidaria de Salud EMSANAR E.S.S, puede identificar, minimizar los riesgos, vulnerabilidades y amenazas que se presentan en el manejo de la información en esta reconocida entidad de salud?

OBJETIVOS

Objetivo General. Identificar y describir las falencias, riesgos y amenazas que se presentan en el manejo de la información en la Empresa Solidaria de Salud EMSANAR E.S.S. por medio de la aplicación de una auditoría informática a la parte lógica y física de la infraestructura de la red de datos, para minimizar el impacto y probabilidad de ocurrencia de los riesgos encontrados, mediante los controles necesarios.

Objetivos Específicos:

Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la empresa solidaria de salud EMSSANAR E.S.S.

Definir los riesgos, vulnerabilidades y amenazas existentes en cuanto a la seguridad en la parte lógica y física de la red de datos de la empresa solidaria de salud EMSANAR E.S.S. Realizar el proceso de análisis y evaluación de riesgos que permitan valorar la probabilidad e impacto que causaría cada uno de los riesgos y generar la matriz de riesgos.

Ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a seguridad en la parte lógica y física de la red de datos de la empresa solidaria de salud, EMSANAR E.S.S.

Presentar los resultados de las evaluaciones de la auditoría en el informe final, y elaborar el plan de mejora que será sustentado y entregado a la empresa solidaria de salud, EMSSANAR. E.S.S, como resultados de la auditoría.

JUSTIFICACIÓN

Emssanar es una Empresa Solidaria de Salud del Régimen Subsidiado que integra a más de 1’200.000 afiliados en el sur occidente Colombiano cuenta con 270 sedes de las diferentes unidades de negocio (EPS-S, IPS, SF, Fundación Emssanar y Cetem) ubicadas en los departamentos de Nariño, Putumayo, Cauca y Valle. Su sede principal se encuentra en Pasto, donde se administra, monitorea y controla todo el funcionamiento de las demás sedes, para ello cuenta con una red informática que es administrada, monitoreada y evaluada por el área de sistemas de Emssanar E.S.S.

Al observar y estudiar las dimensiones de la Empresa Solidaria de Salud Emssanar E.S.S. se hace necesario auditar la parte de la red de datos que ella maneja puesto que, con la implementación de las nuevas tecnologías en las empresas, el uso de sistemas de información software y la adopción de nuevas plataformas tecnológicas, aparecen también nuevas amenazas en cuanto a la seguridad de la red, por lo que las empresas deben realizar procesos de auditoría de forma frecuente y estar actualizándose para detectar los riesgos y amenazas que se presentan dentro de su organización, en cuanto a la seguridad ya sea física o lógica para proteger su principal activo, como es el de la información y de esta manera cumplir con sus objetivos de forma óptima y eficiente.

Además, en la empresa Solidaria de Salud Emssanar E.S.S no se ha revisado ni evaluado a profundidad la parte de redes en el área de sistemas y comunicaciones, diagnostico que es importante para la empresa y con la cual no cuenta actualmente.

Por lo anterior se llevó a cabo en la Empresa Solidaria de Salud Emssanar E.S.S, el proceso de auditoría informática a la red de datos, con lo cual se logró determinar las fallas en la comunicación de la red, que se presentan en las sedes de la empresa Emassanar E.S.S conjuntamente con el desarrollo de este proyecto de auditoría, se realizó un plan de mejoramiento, en la parte de la red de datos de la empresa solidaria Emssanar E.S.S. que le permitirá identificar y mitigar las fallas encontradas, para lograr la eficiencia y eficacia en el área de sistemas de la red de datos, que es de vital importancia para toda la organización de la empresa.

ALCANCE Y DELIMITACIÓN

Para el desarrollo de este proyecto se trabajó en Pasto-Nariño, en la sede Administrativa Pasto, IPS Lorenzo, IPS Parque Bolívar, sede atención al usuario Cresemillas, sede fundación Emssanar la Aurora, además de esta región se trabajó en las oficinas del alto Putumayo. Se auditó lo referente a la seguridad de

la infraestructura física y seguridad lógica de la red en estas sedes y se elaboró un plan de mejoramiento en sobre las falencias o debilidades detectadas. Durante el desarrollo del proyecto se aplicaron las técnicas y el modelo de auditoría informática enfocadas a área de sistemas de Emssanar E.S.S, revisando y evaluando los procesos mediante el modelo COBIT, de estándares internacionales de calidad, logrando así identificar diferentes vulnerabilidades en el manejo y mantenimiento de la seguridad lógica en cuanto a:

- Firewall.
- Trafico de la red.
- IPS (sistemas de prevención de intrusos).
- Antivirus – Antimalware – Antispyware Antispam.
- Filtros de contenido web.
- Sistemas integrales de administración.

La parte física en cuanto a:

- Servidores de red y puntos de control.
- Consolas para administración centralizada de servidores.
- Intranet clientes de la red.
- Routers y Switches.
- Dispositivos y sistemas de seguridad en redes.
- Accesos a los elementos de red.
- Dispositivos inalámbricos y antenas.
- Cableado estructurado (cables, conectores, paneles, canalizaciones).
- Medios informáticos removibles.
- Unidades de distribución de energía (PDU).
- Sistemas de alimentación ininterrumpida (UPS).

1. MARCO TEÓRICO

En el desarrollo de este proyecto se hacen necesarios tener en claro ciertos conceptos tales como: redes, auditoría de redes, análisis de riesgos, y los estándares del COBIT.

1.1 ANTECEDENTES

La informática está inmersa en la gestión integral de la organización. A finales del siglo XX, los sistemas de TI (tecnologías de la información) se constituyeron como las herramientas más poderosas para cualquier organización, puesto que apoyan la toma de decisiones, generando un alto grado de dependencia, así como una elevada inversión en ellas. Debido a la importancia que tienen en el funcionamiento de una organización, existe la auditoría informática.[1] Es por ello que las tecnologías de información, necesitan ser evaluadas, controladas y administradas, en su funcionamiento, y esto se logra mediante una auditora informática.

Existen diferentes modelos de auditoría, como: Coso (Sponsoring Organizations of theTreadway Commission), ISO **(**Organización Internacional para la Estandarización (International Organization for Standardization), entre otros y actualmente un modelo nuevo es el Cobit, (Objetivos de Control para la Información y la Tecnología relacionada). Cobit brinda un conjunto de buenas prácticas a través de un marco de trabajo de dominios y procesos, presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

[1] FERNÁNDEZ Nubia. Importancia de la auditoría informática en las organizaciones, Disponible en internet: <http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica>. [citado el 5 agosto de 2014]

El modelo COBIT es un modelo muy completo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Existen diferentes auditorías que se han desarrollado por estudiantes de ingeniería de Sistemas de la ciudad de Pasto, en diferentes instituciones o empresas, de la región y por lo cual, se decidió tomar como antecedentes los siguientes trabajos de grado sobre auditorías ya que aportan información sobre la empresa en la cual se lleva a cabo el proceso de auditoría, metodologías y herramientas aplicables al proyecto.

Como primer antecedente se tiene: **Auditoría informática en el área de sistemas e indicadores de funcionamiento del hardware en la Empresa Solidaria de Salud Emssanar E.S.S. del Departamento de Nariño**[2]desarrollado por LAURA YANETH NOGUERA QUENGUAN y EDY YANIRA SANCHEZ PERENGUEZ de la UNIVERSIDAD DE NARIÑO. Este trabajo de grado se realizó en las instalaciones de Emssanar y utilizaron la metodología COBIT. El trabajo arriba citado sirvió de antecedente para este proyecto pues brindó información sobre el hardware de la empresa y aportó información en la construcción del marco teórico sobre la metodología COBIT.

Por otra parte se tiene la **Auditoría de sistemas aplicada al sistema integral de información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto**[3]**,** realizada por OSCAR JULIÁN ESTRADA OBANDO de la UNIVERSIDAD DE NARIÑO. Este trabajo de grado consistió en realizar la evaluación de los controles relacionados con la seguridad de la información, identificar las fallas en cuestión de seguridad, plantear posibles soluciones para mejorarlas condiciones de seguridad físicas y lógicas del Sistema Integral de Información utilizando para ello la metodología COBIT. El proyecto arriba mencionado sirvió de antecedente para este proyecto pues aportó las diferentes técnicas y herramientas para la auditoría.

Otro proyecto es **Auditoría de sistemas aplicada a redes de datos**[4] desarrollado por KAROL JANETH JURADO GARCIA y BYRON ALEXANDER MUÑOZ MUÑOZ de la Institución Universitaria CESMAG .Este trabajo de grado consistió en aplicar la metodología COBIT a la red de datos de la Cámara de Comercio de Pasto. Este trabajo de grado aportó diferentes tipos de cuestionarios y formatos de encuestas

[2] NOGUERA, Laura y SANCHEZ Edy Yanira. Auditoría informática en el área de sistemas e indicadores de funcionamiento del hardware en la Empresa Solidaria de Salud Emssanar E.S.S. del Departamento de Nariño. Universidad de Nariño. 2012

[3] ESTRADA, Oscar. Auditoría de sistemas aplicada al sistema Integral de información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto. Universidad de Nariño.2007

[4] JURADO Karol y MUÑOZ Byron. Auditoría de sistemas aplicada a redes de datos. Institución Universitaria CESMAG.2004

puestos en práctica en la cámara de comercio de Pasto y que fueron tenidos en cuenta en nuestro proyecto de auditoría.

1.2 ASPECTOS GENERALES DE LA AUDITORÍA

En los últimos años, el desarrollo de la tecnología informática avanza rápidamente y con ello la manera como las personas, las empresas y la sociedad se desenvuelven en el mundo de la tecnología, el ámbito competitivo laboral se ha adaptado de forma muy positiva el manejo de la tecnología, teniendo como resultado que la información de una empresa este bien organizada, interconectada mediante un sistema de red de datos que le permita administrar los recursos de la empresa de forma local y remota, para compartir todo tipo de información, en diferentes formatos como por ejemplo: datos, imágenes, telefonía, audio, voz IP, videos, etc. y de la misma manera dar un uso óptimo y confiable a sus activos de tecnología de información.

Las redes de datos que se manejan en una organización o empresa necesitan ser auditadas para de esta manera evaluar la eficiencia y la eficacia de las mismas, tanto en la parte física y lógica como: diseño de la red, instalaciones, cableado estructurado, ups, cuartos de comunicaciones, centros y equipos de cómputo, equipos de comunicación, sistemas de información, conectividad, control de acceso de los usuarios de la red, cuellos de botella, calidad en la transmisión de los datos (ancho de banda), vulnerabilidad de la red (antivirus, firewall), recuperación de hardware, de software, etc. Para así conocer con que herramientas se cuenta y que tan actualizados está y obtener un plan estratégico y corporativo que le permita a la empresa conocer las fortalezas y debilidades que genere a la parte administrativa seguridad, confiabilidad, efectividad y eficacia de su entorno.

1.2.1 Definición de auditoría. Auditoría es un examen crítico y sistemático que se realiza a una empresa, a fin de evaluar el cumplimiento de normas, proyectos, la parte financiera, el cumplimiento de objetivos, en general evalúa la eficiencia y eficacia de todos los procesos que tienen que ver con el mejoramiento y desarrollo empresarial, estableciendo diferentes alternativas de soluciones para garantizar organización y logro de objetivos. La eficiencia, definida como lograr el objetivo en menor tiempo posible y la eficacia definida como lograr el objetivo sin importar el tiempo, se convierte en la clave para obtener una auditoría de calidad.

Un auditor debe ser una persona capaz de observar cada movimiento y comportamiento de los procesos, encaminado siempre al objetivo específico, que es el de evaluar la eficacia y eficiencia de cada proceso tomado como caso de estudio, para que por medio del señalamiento de alternativas de acción, la empresa como tal tome decisiones que permita corregir hallazgos en caso de que

sean encontrados, mejorando las funciones de cada proceso permitiendo así el cumplimiento de los objetivos propuestos por la empresa.

1.2.2 Clasificación de la auditoría. La auditoría se puede clasificar de dos maneras, auditoría externa y auditoría interna.

Auditoría externa. La auditoría externa se caracteriza porque la realiza un profesional totalmente independiente de la empresa, el cual después de examinar y evaluar el área de los sistemas de información genera una opinión veraz y creíble de los casos de estudio tomados, para luego presentarlos como resultados o hallazgos a la empresa u organización.

Auditoría interna. La auditoría interna es la evaluación exhaustiva y detallada de cada uno de los procesos llevados dentro de una empresa, se evalúan sistemas de información como también operaciones contables y financieras, evaluando siempre la eficiencia y eficacia de todos los procesos. Generalmente la empresa es quien asigna a un profesional calificado perteneciente a la misma con el objeto de utilizar diferentes técnicas que permitan realizar un examen, dando como resultado la detección de fallas a tiempo, para corregirlas y mejorar algunos procesos que así el informe de la auditoría final lo sugiera.

1.2.3 Tipos de Auditoría[5]. Entre ellos se encuentran:

- **Auditoría informática,** proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

- **Auditoría de seguridad de sistemas de información**, análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

[5]MORGADO Gastby. Auditoría fiscal y auditoría. Disponible en internet:<http://www.monografias.com/trabajos16/auditoría-fiscal/auditoría-fiscal.shtml>. [Citado 11 de Febrero de 2012]

1.3 AUDITORÍAINFORMÁTICA COMO OBJETO DE ESTUDIO

La auditoría informática es de reciente desarrollo y su aparición se debe a la creciente automatización de la información en todos los niveles de las organizaciones.

La auditoría informática es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

1.4 CLASIFICACIÓN DE LA AUDITORÍA INFORMÁTICA

Auditoría informática de explotación. La explotación informática se encarga de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. Para realizar la explotación informática se dispone de una materia prima, los datos, que sea necesario transformar, y que se sometan previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y finalmente, son distribuidos al cliente.

Auditoría informática de sistemas:[6] se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de las instalaciones informáticas se auditen por separado, aunque formen parte del entorno general de sistemas, por ejemplo auditoría relacionadas con:

Sistemas operativos: engloba los subsistemas de teleproceso entrada/salida etc. Debe verificarse en primer lugar que los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los sistemas operativos permite descubrir las posibles incompatibilidades entre otros productos de software básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software básico: es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto,

[6] CANAVES. Mario. Auditoría informática. Disponible en internet: <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>. [Citado 16 de Enero de 2012]

por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al sistema. Igualmente debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

Investigación y desarrollo: como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las compañías del ramo. La auditoría informática deberá cuidar de que la actividad de investigación y desarrollo no interfiera ni dificulte las tareas fundamentales internas.

Auditoría informática de comunicaciones y redes.[7]Para el informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc. no son sino el soporte físico-lógico del tiempo real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios).

El auditor de comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la des actualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática.

Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras con tarjetas de comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

[7] CANAVES, Mario. Auditoría informática. Disponible en internet: <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>. [Citado 16 de Enero de 2012]

Auditoría a los sistemas de redes.[8]Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.

Auditoría de la seguridad informática. La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

1.5 METODOLOGÍA DE LA AUDITORÍA INFORMÁTICA

Una metodología es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado determinado, de tal manera que una metodología en la auditoría informática consiste en un conjunto de pasos ordenados y lógicos para

[8] BLOG, Clasificación de los tipos de auditoría. <http://myblog-bilky.blogspot.com/>[Citado 13 de Junio de 2012]

llevar a cabo un examen sistemático de la eficiencia y la eficacia de los procesos, activos, recursos de TI que posee una organización o empresa.

La auditoría incluye los siguientes pasos:[9]

- Alcance y objetivos de la auditoría informática
- Estudio inicial del entorno auditable
- Determinación de los recursos necesarios para realizar la auditoría
- Elaboración del plan y de los programas de trabajo
- Actividades propiamente dichas de la auditoría
- Confección y redacción del informe final
- Redacción de la carta de introducción o carta de presentación del Informe final

1.5.1 Alcance de la auditoría[10]. Expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

Tanto los alcances como las excepciones deben figurar al comienzo del informe final.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

1.5.2 Estudio inicial. Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

❖ Organización: Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto un auditor deberá fijarse en:

❖ Organigrama: El organigrama expresa la estructura oficial de la organización a auditar.

❖ Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

---

[9] CATEDRAS INGENIERIA. Metodología de la auditoría informática. Disponible en internet: <http://www.ub.edu.ar/catedras/ingenieria/auditoría/tpmetodo/tpmetodo2.htm#p2-1-1>. Consultado: 5 de Mayo de 2014.

[10] Ibíd., Consultado: 5 de Mayo de 2014.

❖ Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

❖ Relaciones jerárquicas y funcionales entre órganos de la organización: El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

Las de jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinados.

❖ Flujos de información: Además de las corrientes verticales interdepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra departamentales.

Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

❖ Número de puestos de trabajo: El equipo auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

1.5.3. Entorno operacional. El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

❖ Situación geográfica de los sistemas: Se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.

❖ Arquitectura y configuración de hardware y software: Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías.

Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

❖ Inventario de hardware y software: El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware figurarán las CPUS, unidades de control local y remoto, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

❖ Comunicación y redes de comunicación: En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.

❖ Igualmente, poseerán información de las redes locales de la empresa.

1.5.4 Determinación de recursos de la auditoría informática.[11]Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

1.5.5 Recursos materiales. Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas de software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.

Los recursos materiales del auditor son de dos tipos:

❖ Recursos materiales software: programas propios de la auditoría: Son muy potentes y flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de técnica de sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

❖ Recursos materiales hardware: los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Para lo cual habrá de convenir él, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

[11] CATEDRAS INGENIERIA. Metodología de la auditoría informática. Disponible en internet: <http://www.ub.edu.ar/catedras/ingenieria/auditoría/tpmetodo/tpmetodo2.htm#p2-1-1>. Consultado: 5 de Mayo de 2014.

1.5.6 Recursos humanos. La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable.

Es igualmente importante señalar que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

1.5.7 Elaboración del plan y de los programas de trabajo[12]: una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo y así, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

❖ Si la revisión debe realizarse por áreas generales o áreas específicas.

❖ Si la auditoría es global, de toda la informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

❖ En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.

❖ En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.

❖ En el plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.

❖ El plan establece disponibilidad futura de los recursos durante la revisión.

❖ El plan estructura las tareas a realizar por cada integrante del grupo.

❖ En el plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

❖ Una vez elaborado el plan, se procede a la programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

[12] Ibíd., Consultado: 5 de Mayo de 2014.

1.6 ACTIVIDADES PROPIAMENTE DICHAS DE LA AUDITORÍA INFORMÁTICA[13:]

La auditoría informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad. Existen técnicas que hacen que el auditor las aplique de acuerdo a su juicio y al tipo de auditoría a ejecutar y son:

1.6.1 Técnicas de trabajo/ Tipos de pruebas:

- Análisis de la información obtenida del auditado
- Análisis de la información propia
- Cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos
- Inspección
- Confirmación
- Investigación
- Certificación
- Observación

1.6.2 Herramientas

- Cuestionario general inicial
- Cuestionario Checklist
- Estándares
- Monitores
- Simuladores (Generadores de datos)
- Paquetes de auditoría (Generadores de Programas)
- Matrices de riesgo

1.6.3 Confección y redacción del informe final. La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste de

[13] CATEDRAS INGENIERIA, Metodología de la auditoría informática. Disponible en internet: <http://www.ub.edu.ar/catedras/ingenieria/auditoría/tpmetodo/tpmetodo2.htm#p2-1-1>. Consultado: 5 de Mayo de 2014

opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

1.6.4 Redacción de la carta de introducción o carta de presentación del informe final.[14]La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o persona concreta que encargó o contrato la auditoría.

Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no hará copias de la citada carta de introducción. La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios
- Incluirá fecha, naturaleza, objetivos y alcance
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.

En la carta de introducción no se escribirán nunca recomendaciones.

Estructura del informe final: el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Siguiendo los siguientes pasos:

- Definición de objetivos y alcance de la auditoría
- Enumeración de temas considerados
- Cuerpo expositivo

Para cada tema, se seguirá el siguiente orden a saber:

A. Situación actual: Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.

B. Tendencias: Se tratarán de hallar parámetros que permitan establecer tendencias futuras.

C. Puntos débiles y amenazas.

[14] Ibíd., Consultado: 5 de Mayo de 2014.

D. Recomendaciones y planes de acción: Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.

E. Redacción posterior de la carta de introducción o presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo: El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.

- Las ventajas del cambio deben superar los inconvenientes derivados de mantenerla situación.

- No deben existir alternativas viables que superen al cambio propuesto.

- La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación. La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

- Flujo del hecho o debilidad: Hecho encontrado.

Ha de ser relevante para el auditor y pera el cliente, ha de ser exacto, y además convincente, No deben existir hechos repetidos.

Consecuencias del hecho: las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho: se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho: no deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

Recomendación del auditor informático:

- Deberá entenderse por sí sola, por simple lectura.

- Deberá estar suficientemente soportada en el propio texto.

- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.

- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.7 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍAINFORMÁTICA[15]

1.7.1 Las entrevistas. Le proporcionan al auditor el conocimiento del personal auditado y como se están llevando a cabo las funciones en la organización, aunado a esto las entrevistas conllevan a lo siguiente:

- El auditor comienza a continuación las relaciones personales con el auditado.

- La entrevista es una de las actividades personales más importante del auditor; recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

- Interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

1.7.2 Cuestionarios.[16]Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser habitual comenzar solicitando la cumplimentación de cuestionarios pre-impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

---

[15] CANAVES, Mario .Auditoría informática. Disponible en internet: <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>. Consultado 16 de Enero de 2012

[16] Ibíd., Consultado: 16 de Enero 2012.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

1.7.3 Checklist. El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas normales", que en realidad servirán para la cumplimentación sistemática de sus cuestionarios, de sus checklist.
Hay opiniones que descalifican el uso de las checklist, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar checklist, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes.

Según la claridad de las preguntas y el talento del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula.

Las empresas externas de auditoría informática guardan sus checklist, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y concisamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Los cuestionarios o checklist responden fundamentalmente a dos tipos de filosofía" de calificación o evaluación:

a. Checklist de rango: contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo: Se supone que se está realizando

una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados, de acuerdo a la siguiente escala:

1: Muy deficiente.
2: Deficiente.
3: Mejorable.
4: Aceptable.
5: Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guion. La cumplimentación de la checklist no debe realizarse en presencia del auditado

Las checklist de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las checklist binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo.

No existen checklist estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

1.7.4 Trazas y/o huellas. Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan Exactamente las funciones previstas, y no otras. Para ello se apoya en productos de software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo. Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnicas de sistemas a cada uno de los parámetros

variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

1.7.5 Observación.[17]La observación es una de las técnicas más utilizadas en la recolección de información para aplicación de una auditoría, ya que a través de diferentes técnicas y métodos de observación permite recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas. Existen diferentes tipos de observación, entre las cuales están:

- Observación directa
- Observación indirecta
- Observación oculta
- Observación participativa
- Observación no participativa
- Introspección
- Retrospección
- Observación histórica
- Observación controlada
- Observación natural

1.7.6 Inventarios.[18]Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas.

Los principales tipos de inventarios aplicables en el ambiente de sistemas Computacionales, son:

- Inventario de software

[17] CANAVES, Mario. Auditoría informática. Disponible en internet: <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>. Consultado 16 de Enero de 2012

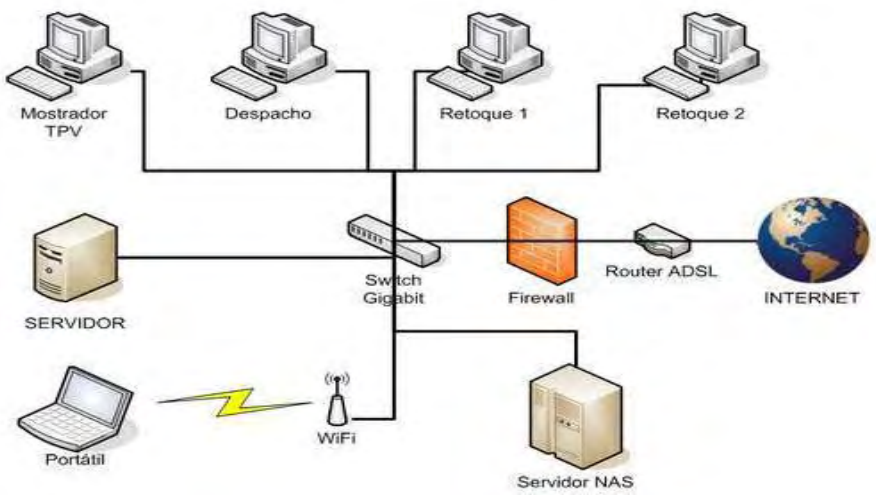
[18] Ibíd., Consultado: 16 de Enero 2012.

- Inventario de hardware
- Inventario de documentos
- Inventario de documentos administrativos
- Inventario de documentos técnicos para el sistema
- Manuales e instructivos técnico del hardware, periféricos y componentes del sistema
- Manuales de la organización
- Manuales de procedimientos administrativos
- Manuales de perfil de puestos
- Otros manuales administrativos
- Manuales e instructivos de mantenimiento físico del sistema (hardware), entre otros.

1.8 REVISION CONCEPTOS DE REDES

1.8.1 Definición de red. Una red informática, es un conjunto de computadoras conectadas por medio de cables, señales, ondas con el objetivo de compartir información o recursos, los mismos que pueden ser medios magnéticos, impresoras, programas, y también servicios como acceso a internet, e-mail, chat, juegos, etc., además da la posibilidad de creación de grupos de trabajo, gestión centralizada, acceso a otros sistemas operativos. [19]

Figura 1. Red informática.



[19] GALLEGOS, Alex. Red de computadoras. Monografías. disponible en internet: http://www.monografias.com/trabajos72/red-computadoras/red-computadoras.shtml Consultado marzo de 2014.

Fuente: SIMONELLI, Andreina. Redes Fundamentos de la informática. Redes. Disponible en internet: http://fundamentosinformaticaunerg.blogspot.com/p/redes.html Consultado: marzo 2014.

1.8.2 Clasificación de las redes[20]

- ✓ **Clasificaciones por extensión**. La clasificación más común para referirse a los distintos tipos de redes es la referente a su extensión Las redes LAN (Red de Área Local), WAN (Red de Área Amplia) y MAN, Metropolitan Área Network pertenecen a esta clasificación. Entre ellas se encuentra:

  - **Redes de área local (LAN)**. Una red de área local (LAN, Local Área Network) suele ser una red de propiedad privada y conectar enlaces de una única oficina, edificio o campus. Dependiendo de las necesidades de la organización donde se instale y del tipo de tecnología utilizada, una LAN puede ser tan sencilla como dos PC y una impresora situadas en la oficina de la casa de alguien; o se puede extender por toda una empresa e incluir periféricos de voz, sonido y vídeo. Actualmente, el tamaño de las LAN está limitado a unos pocos kilómetros.

    Las LAN están diseñadas para permitir compartir recursos entre computadoras personales o estaciones de trabajo. Los recursos a compartir pueden incluir hardware (por ejemplo, una impresora), software (por ejemplo, un programa de aplicación) o datos. Un ejemplo frecuente de LAN, que se encuentra en muchos entornos de negocios, enlaza un grupo de trabajo de computadoras relacionadas con una cierta tarea, como, por ejemplo, estaciones de trabajo de ingeniería o PC de contabilidad. Una de las computadoras puede tener un disco de gran capacidad y convertirse en servidora de los otros clientes. El software se puede almacenar en este servidor central para que sea usado por todo el grupo según las necesidades de cada miembro. En este ejemplo, el tamaño de la LAN puede estar determinado por restricciones en el número de licencias, por el número de usuarios, por copia de software o por restricciones en el número de usuarios con licencia para acceder al sistema operativo.

  - **Redes de área extensa (WAN)**.[21]Una red de área amplia (WAN, Wide Área Network) proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de vídeo sobre grandes áreas geográficas que

[20] SIMONELLI, Andreina. Fundamentos de la informática. Redes. Disponible en internet: http://fundamentosinformaticaunerg.blogspot.com/p/redes.html Consultado: marzo 2014.
[21] Ibíd., Consultado: 16 de Marzo 2014.

pueden extenderse a un país, un continente o incluso al mundo entero. Una WAN puede ser tan compleja como las troncales que conectan Internet o tan simple como la línea telefónica que conecta una computadora casera a Internet.

Normalmente se denomina a la primera WAN conmutada y a la segunda WAN punto a punto.

La WAN conmutada conecta los sistemas terminales, que habitualmente incluyen un enrutador (dispositivo de conexión entre redes) que conecta a otra LAN o WAN.

La WAN punto a punto es normalmente una línea alquilada a un proveedor de telefonía o TV por cable que conecta una computadora casera a una LAN pequeña o a un proveedor de servicios de Internet (ISP, Internet Service Provider). Este tipo de WAN se usa a menudo para proporcionar acceso a Internet.

- **Redes de área metropolitana (MAN)**.[22]La red de área metropolitana (MAN, Metropolitan Área Network) tiene un tamaño intermedio entre una LAN y una WAN. Normalmente cubre el área de una ciudad. Está diseñada para clientes que necesitan una conectividad de alta velocidad, normalmente a Internet, y tiene puntos de conexión extendidos por la ciudad o parte de ella. Un buen ejemplo de MAN es la parte de red de una compañía telefónica que puede producir una línea DSL a los clientes. Otro ejemplo es la red de TV por cable, diseñada originalmente para la TV por cable, pero usada actualmente para proporcionar conexiones de alta velocidad a Internet.

✓ **Clasificaciones por propiedad**.[23]Según su nivel de acceso o privacidad, las redes pueden ser: Redes públicas y Redes privadas.

- **Redes públicas:** son aquellas redes cuyo acceso es público y global, de modo que permiten a sus usuarios comunicarse y compartir información y servicios dentro del área pública que abarcan. El ejemplo más claro de red pública y de ámbito mundial es Internet.

[22] Ibíd., Consultado: 16 de Marzo 2014
[23] GOMESZ, Sebastián. Redes corporativas. Clasificación de las redes según su propiedad. Disponible en internet: http://sebastiangomezm.blogspot.com/2011/09/clasificacion-de-las-redes-segun-su_7508.html consultado marzo 2014.

- **Redes privadas**. Son redes restringidas al propietario o a los usuarios que las utilizan (son redes LAN en su mayoría). Cuando en este tipo de redes se utilizan herramientas típicas de la red pública Internet (web, correo electrónico, FTP, etc.) se denominan intranets.

✓ **Clasificaciones por método de conexión.**[24]En esta clasificación podemos distinguir dos grupos de redes: Por medios guiados y por medios no guiados (inalámbricas).

- **Por medios guiados**. En ellas, la información viaja en forma de ondas encapsuladas dentro de un cable. Dicho cable puede ser de par trenzado (el más utilizado en redes LAN), coaxial o de fibra óptica.

- **Por medios no guiados (inalámbricas)**. En ellas la transmisión de la señal se realiza mediante antenas. En este grupo se utilizan tecnologías de radiofrecuencia (redes Wi-Fi y Bluetooth).

  En este tipo de medios tanto la transmisión como la recepción se lleva a cabo mediante antenas. La antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

✓ **Clasificaciones por topología**.[25]Topología Es el arreglo físico o lógico de un sistema de telecomunicaciones.

Topologías físicas

- **Topología en anillo.**[26]En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor. Cuando un dispositivo recibe una señal para otro dispositivo, su repetidor regenera los bits y los

[24] REDES LOCALES. clasificación de las redes por método de conexión. Disponible en internet: https://sites.google.com/site/redeslocalesmaria/2-clasificacion-de-las-redes/por-metodo-de-conexion Consultado marzo 2014.

[25] GÜIM. Redes de comunicación. Tipos de redes. Disponible en internet: http://guimi.net/monograficos/GRedes_de_comunicaciones/G-RCnode4.html Consultado marzo 2014.

[26] PBC Tecnologías. Electrónica fácil. Tipos de redes. Disponible en internet: http://electronicafacillord.blogspot.com/2014/06/tipos-de-redes.html Consultado marzo 2014.

retransmite al anillo. Un anillo es relativamente fácil de instalar y reconfigurar. Cada dispositivo está enlazado solamente a sus vecinos inmediatos (bien físicos o lógicos). Para añadir o quitar dispositivos, solamente hay que mover dos conexiones. Las únicas restricciones están relacionadas con aspectos del medio físico y el tráfico (máxima longitud del anillo y número de dispositivos). Además, los fallos se pueden aislar de forma sencilla. Generalmente, en un anillo hay una señal en circulación continuamente. Si un dispositivo no recibe una señal en un período de tiempo especificado, puede emitir una alarma. La alarma alerta al operador de red de la existencia del problema y de su localización. Sin embargo, el tráfico unidireccional puede ser una desventaja. En anillos sencillos, una rotura del anillo (como por ejemplo una estación inactiva) puede inhabilitar toda la red. Esta debilidad se puede resolver usando un anillo dual o un conmutador capaz de puentear la rotura.

- **Topología en anillo doble**.[27]Una topología de anillo doble consta de dos anillos concéntricos. La topología de anillo doble es igual a la topología de anillo, con la diferencia de que hay un segundo anillo redundante que conecta los mismos dispositivos, aunque solamente trabaja un anillo a la vez.

- **Topología en bus**.[28]Una topología de bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos. Los nodos se conectan al bus mediante cables de conexión (latiguillos) y sondas. Un cable de conexión es una conexión que va desde el dispositivo al cable principal. Una sonda es un conector que, o bien se conecta al cable principal, o se pincha en el cable para crear un contacto con el núcleo metálico. Cuando las señales viajan a través de la red troncal, parte de su energía se transforma en calor, por lo que la señal se debilita a medida que viaja por el cable. Por esta razón, hay un límite en el número de conexiones que un bus puede soportar y en la distancia entre estas conexiones.

- **Topología en estrella**.[29]Cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí. A

[27] Ibíd., Consultado: 16 de Marzo 2014.

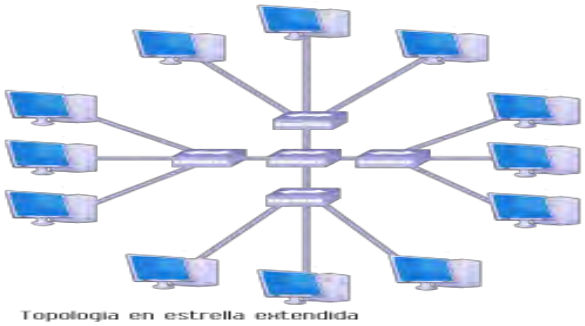
[28] PEREZ, Rafael. Redes e instalaciones. Clasificación de las redes. Disponible en internet: http://conocimientosdehoy.blogspot.com/2014/10/clasificacion-de-las-redes.html Consultado marzo 2014.

[29] PEREZ, Rafael. Redes e instalaciones. Clasificación de las redes. Disponible en internet: http://conocimientosdehoy.blogspot.com/2014/10/clasificacion-de-las-redes.html Consultado marzo 2014.

diferencia de la topología en malla, la topología en estrella no permite el tráfico directo de dispositivos. El controlador actúa como un intercambiador: si un dispositivo quiere enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final. Una topología en estrella es más barata que una topología en malla. En una estrella, cada dispositivo necesita solamente un enlace y un puerto de entrada/salida para conectarse a cualquier número de dispositivos. Este factor hace que también sea más fácil de instalar y reconfigurar. Además es necesario instalar menos cables y la conexión, desconexión y traslado de dispositivos afecta solamente a una conexión; la que existe entre el dispositivo y el concentrador. Otra ventaja de esta red es su robustez. Si falla un enlace, solamente este enlace se verá afectado. Todos los demás enlaces permanecen activos. Este factor permite también identificar y aislar los fallos de una forma muy sencilla. Mientras funcione el concentrador, se puede usar como monitor para controlar los posibles problemas de los enlaces y para puentear los enlaces con defectos. Una gran desventaja de la topología en estrella es la dependencia que toda la topología tiene de un punto único, el concentrador. Si el concentrador falla, toda la red muere.

- **Topología en estrella extendida**.[30]La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella, la ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

Figura 2. Topología en estrella extendida



Fuente: Redes e instalaciones. Clasificación de las redes. Disponible en internet: http://conocimientosdehoy.blogspot.com/2014/10/clasificacion-de-las-redes.html Consultado marzo 2014**.**

[30] Ibíd. . Consultado marzo 2014.

- **Topología en malla completa**.[31]Cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.

  Las ventajas de una malla es el uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos.

  Otra ventaja es que esta topología es robusta. Si un enlace falla, no inhabilita todo el sistema. En tercer lugar, está la ventaja de la privacidad o la seguridad.
  Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes. Finalmente, los enlaces punto a punto hacen que se puedan identificar y aislar los fallos más fácilmente. El tráfico se puede encaminar para evitar los enlaces de los que se sospecha que tienen problemas.

  Esta facilidad permite que el gestor de red pueda descubrir la localización precisa del fallo y ayudar a buscar sus causas y posibles soluciones.

  Entre las desventajas de la malla se relacionan con la cantidad de cable y el número de puertos de entrada/salida necesarios. En primer lugar, la instalación y reconfiguración de la red es difícil, debido a que cada dispositivo debe estar conectado a cualquier otro.

  En segundo lugar, la masa de cables puede ser mayor que el espacio disponible para acomodarla (en paredes, techos o suelos). Y, finalmente, el hardware necesario para conectar cada enlace (puertos de E/S y cables) puede ser prohibitivamente caro. Por estas razones, las topologías en malla se suelen instalar habitualmente en entornos reducidos por ejemplo, en una red troncal que conecte las computadoras principales de una red híbrida que puede incluir varias topologías más.

[31] PEREZ, Rafael. Redes e instalaciones. Clasificación de las redes. Disponible en internet: http://conocimientosdehoy.blogspot.com/2014/10/clasificacion-de-las-redes.html Consultado marzo 2014.

Topologías lógicas [32]

- **La topología Broadcast**. Se refiere cuando un host envía sus datos a todos los equipos conectados al medio, la transmisión no es controlada. No existe una orden que las estaciones deban seguir para utilizar la red un ejemplo de esta topología es Ethernet.

- **Topología de transmisión de Token**. Se refiere que para controlar las transmisiones, mediante él envió de un token, un host puede transmitir solo cuando han aceptado la señal del token un ejemplo de red que utiliza la transmisión de token es Token Ring.

- **Las redes TOKEN RING están implementadas en una topología en anillo**. La topología física de una red Token Ring es la topología en estrella, en la que todos los equipos de la red están físicamente conectados a un concentrador o elemento central.

  El ANILLO FÍSICO está cableado mediante un concentrador o switch denominado unidad de acceso multiestación (multistationaccessunit, MSAU). La topología lógica representa la ruta del testigo entre equipos, que es similar a un anillo.

  Sencillamente, Token Ring es la tecnología de red en la cual el acceso al medio está determinado por el paso del testigo o Token:

1.8.3 Dispositivos de red[33]

Cableado. Una red está compuesta por un sistema de cableado, que conecta las estaciones de trabajo con los servidores de archivos y otros periféricos. Existen varios tipos de cableados, cada uno con sus propias características en cuanto al costo, velocidad y capacidad.

Cable de par trenzado. Un cable de par trenzado consta de dos hilos de cobre aislados y entrelazados. Hay dos tipos de cables: cable de par trenzado sin apantallar (UTP) y par trenzado apantallado (STP).

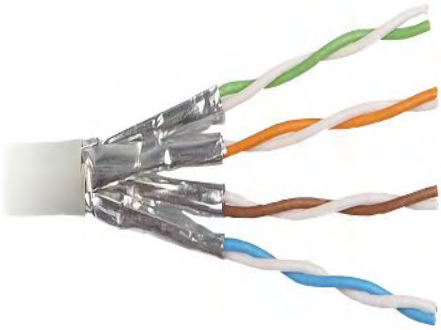
---

[32] ANONIMO. Topología y redes. Topologías físicas y lógicas. Disponible en internet: http://topologiayredes.wordpress.com/tag/broadcast/ Consultado marzo 2014.

[33] ANONIMO. Redes de computadoras. Monografías. Disponible en internet: http://www.monografias.com/trabajos5/redes/redes.shtml Consultado marzo 2014.

Figura 3. Cable UTP sin apantallar

Figura 4. Cable STP o par trenzado apantallado



Fuente: GONZALES, Ricardo. Cable par trenzado. Disponible en internet: http://appnext.blogspot.com/2011/04/cable-de-par-trenzado.html Consultado marzo 2014.

Cable coaxial.[34] Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas.

Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas. A inicios fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive; Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos.

[34]ANONIMO. Redes de computadoras. Monografías. Disponible en internet: http://www.monografias.com/trabajos5/redes/redes.shtml Consultado marzo 2014.

Este cable se puede utilizar en diferentes aplicaciones como: Entre la antena y el televisor, en las redes urbanas de televisión por cable e Internet, en las redes de transmisión de datos como Ethernet, en las redes telefónicas interurbanas y en los cables submarinos.

Cable de fibra óptica.[35]El cable de fibra óptica es habitualmente utilizado en redes de datos, el cual está compuesto de un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Las fibras son utilizadas en su mayoría en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia siendo inmune a la interferencia de frecuencias de radio; además las fibras son utilizadas para redes locales, en donde se necesite una alta confiabilidad y fiabilidad, teniendo así un costo mayor que los cables de transmisión anteriormente mencionadas.

1.8.4 Tarjetas de red.[36]Este es el dispositivo más utilizado en la actualidad para conectar un equipo a la red, es de tamaño estándar que puede venir de forma integrada en las placas base o individualmente, se coloca en ranuras de ampliación de las PC, a diferencia en las computadoras portátiles ya vienen incorporadas. Las tarjetas de red actúan como la interfaz entre un ordenador y el cable de red. La función de la tarjeta de red es la de preparar, enviar y controlar los datos en la red.

1.8.5 Modem.[37]El modem es usado para la transmisión de datos vía telefónica, el cual convierte señales o pulsaciones en información, comunicándose con el ISP64 mediante una línea telefónica, con un modem se puede descargar información, enviar y recibir datos, también existen algunos módems que pueden enviar y recibir faxes y llamadas telefónicas , etc.

1.8.6 Switch.[38] Este es un dispositivo de interconexión de redes de computadoras, opera en la capa 2 del modelo OSI es decir el nivel de enlace de datos, estos

---

[35] ANONIMO. Redes de computadoras. Monografías. Disponible en internet: http://www.monografias.com/trabajos5/redes/redes.shtml Consultado marzo 2014.

[36] Ibíd., Consultado marzo 2014.

[37] Ibíd., Consultado marzo 2014.

[38] PEÑA, Katherine. Enrutadores inalámbricos. Monografías. Disponible en internet: http://www.monografias.com/trabajos72/enrutadores-inalambricos/enrutadores-inalambricos2.shtml Consultado marzo 2014.

tienen la particularidad de aprender y almacenar las direcciones de dicho nivel, por lo que siempre irán desde el puerto de origen directamente al de llegada.

La función de este dispositivo además de interconectar computadoras, sirve para expandir la red conectando múltiples dispositivos dentro de un edificio o campus, por ejemplo puede conectar los ordenadores, impresoras y servidores, creando una red de recursos compartidos. Cabe recalcar que este dispositivo permite ahorrar dinero y aumentar la productividad.

Existen dos tipos básicos de switch los cuales son los gestionados y no gestionados.

Los switch gestionados: Permiten acceder a ellos para programarlos, se puede monitorizar y ajustar local o remotamente, para proporcionarle al switch el control de cómo transmite el tráfico en su red y quien tiene acceso a su red.

Los switch no gestionados: Funcionan de forma automática y no permiten realizar cambios. Un ejemplo de quienes utilizan estos tipos de switch son los equipos de redes domésticas. Además el switch se encarga de encaminar la conexión hacia el puerto requerido por una única dirección y de esta manera reduce el tráfico y disminuye las colisiones notablemente.

1.8.7 Router.[39]El router es un dispositivo que sirve para la interconexión de redes informáticas que opera en la capa tres perteneciente al nivel de red, trabajan con direcciones IP, el cual nos permitirá el enrutamiento de paquetes de datos entre redes, lee cada paquete y lo envía atreves del camino más eficiente al destino, toma en cuenta factores como líneas más rápidas, líneas menos saturadas, etc.

A continuación se dará una explicación de lo que anteriormente llamamos paquete de datos.

Es la unidad fundamental de transporte de información en todas las redes de computadoras, el mismo que está compuesto por tres elementos:

Una cabecera: Contiene la información necesaria para transportar el paquete desde el emisor hasta el receptor.

Área de datos: Contiene los datos que se trasladarán.

Cola: Comúnmente incluye código de detección de errores.

---

[39] Ibíd., Consultado marzo 2014.

Router ADSL.[40]Es un dispositivo que permite conectar uno o varios equipos o incluso una LAN, este router trata de varios componentes en uno solo, el cual realiza las funciones de puerta de enlace: Es decir proporciona salida hacia el exterior a una red local.

Router: Dirige el paquete procedente de internet hacia el destino por medio. Del camino correspondiente, es decir es capaz de encaminar paquetes IP.

Módem ADSL: Este es el que modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos.

Punto de acceso wireless: Esto es lo más común que se utiliza ya que algunos router ADSL permiten la comunicación vía Wireless es decir sin cables con los equipos de la red local.

En la actualidad los avances tecnológicos son muy interesantes, ya que han conseguido introducir la funcionalidad de cuatro equipos en uno solo como se explicó anteriormente.

Figura 5. Router compuesto.

Fuente: COMPRAWIFI.Compra router.Belkinrouter ADSL Disponible en internet: http://www.comprawifi.com/descatalogados/belkin-router-adsl-802-11g-54mbps-4-puertos-rj45/prod_1430.html Consultado marzo 2014.

[40] PEÑA, Katherine. Enrutadores inalámbricos. Monografías. Disponible en internet: http://www.monografias.com/trabajos72/enrutadores-inalambricos/enrutadores-inalambricos2.shtml Consultado marzo 2014.

1.8.8 Microonda.[41]Es un tipo de red inalámbrica que utiliza microondas como medio de transmisión, generalmente transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps

Funcionamiento. El servicio utiliza una antena que se coloca en un área despejada sin obstáculos que pudieran entorpecer una buena recepción en el edificio o la casa del receptor y se coloca un módem que interconecta la antena con la computadora. La comunicación entre el módem y la computadora se realiza a través de una tarjeta de red, que deberá estar instalada en la computadora. La tecnología inalámbrica trabaja bien en ambientes de ciudades congestionadas, ambientes suburbanos y ambientes rurales.

1.8.9 Red satelital.[42]Son redes que utilizan como medios de transmisión satélites artificiales localizados en órbita alrededor de la tierra.

1.8.10 servidores y terminales.

Servidor. Los servidores forman parte de una red y se lo visualiza desde dos puntos diferentes, de tipo software y hardware pero a la final ambos proveen servicios a otras aplicaciones llamados clientes. Algunos servicios habituales son, los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final, es decir el propósito de estos servidores es proveer datos que otras máquinas puedan utilizar.

Tipos de servidores.[43]

Servidor web: es un ordenador que usa el protocolo http para enviar páginas web cuando el usuario lo solicita.

Servidor de archivo: este servidor es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.

---

[41] PEÑA, Katherine. Enrutadores inalámbricos. Monografías. Disponible en internet: http://www.monografias.com/trabajos72/enrutadores-inalambricos/enrutadores-inalambricos2.shtml Consultado marzo 2014.

[42] HERNANDEZ, Jorge. Redes satelitales. Monografías. Disponible en internet: http://www.monografias.com/trabajos29/redes-satelitales/redes-satelitales.shtml Consultado Marzo 2014.

[43] PORTAL EDUCATIVO, TiposDe.org. Tipos de servidores. Disponible en internet: http://www.tiposde.org/informatica/131-tipos-de-servidores/ Consultado marzo 2014.

Servidor de correo: este servidor almacena, envía, recibe, selecciona la ruta y realiza otras operaciones relacionadas con email para los clientes de la red.

Servidor de fax: este servidor almacena, envía, recibe, selecciona la ruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiada de fax.

Servidor de base de datos: este servidor provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. Los servidores web, servidores de correo y servidores de bases de datos son a lo que tiene acceso la mayoría de la gente al usar Internet.

1.8.11 Vlan.[44]Una VLAN es un agrupamiento lógico de usuarios o dispositivos independiente de su ubicación física en un segmento. La configuración de las VLAN se hace en los switchs mediante software y es considerada como un dominio de Broadcast.

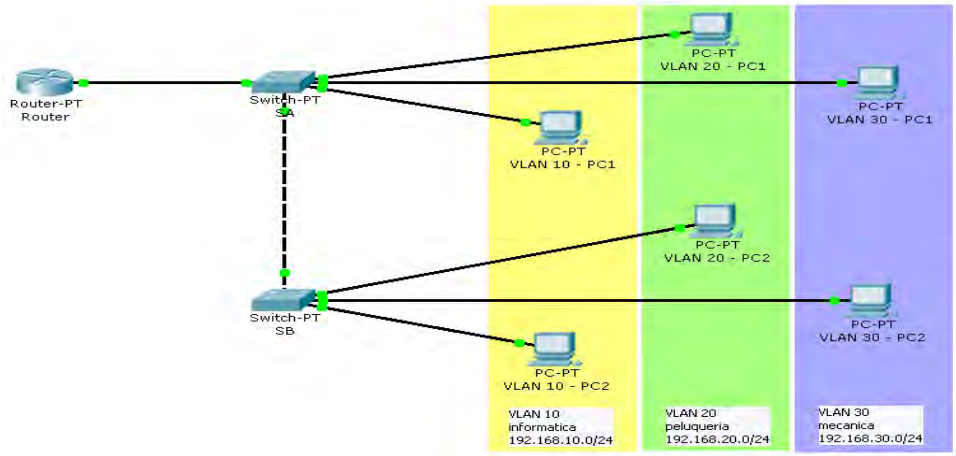
Las VLAN son útiles para reducir el dominio de emisión y ayudan en la administración de la red separando segmentos lógicos de una red de área local, como departamentos de una empresa, institución etc. que no deberían intercambiar datos usando la red local. Las VLAN funcionan en las Capas 2 y 3 del modelo de referencia OSI.

Tipos de VLAN:

La VLAN de nivel 1 o VLAN basada en puerto. Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN, el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla, el servidor estará en la VLAN amarilla.

[44] UAZUAY, Estudios. Vlans. Disponible en internet: http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf consultado marzo 2014.

Figura 6. LAN de nivel 1 o basada en puerto.



Fuente: APRENDE WEBWIKI. Configuración de redes virtuales. Disponible en internet: http://wiki.aprendeweb.org/index.php?title=Configuraci%C3%B3n_de_redes_virtuales#Nivel_2_-_VLAN_basadas_en_MAC Consultado marzo 2014.

Ventajas:

Facilidad de movimientos y cambios.

Micro segmentación y reducción del dominio de Broadcast.

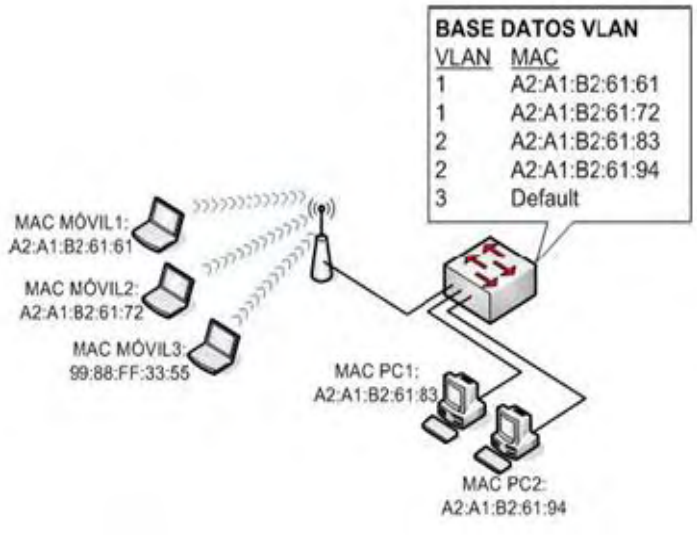
Multiprotocolo: la definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

Administración: un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

La VLAN de nivel 2 o VLAN basada en la dirección MAC Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación.

Figura 7. VLAN basada en mac.



Fuente: APRENDEWEB. Configuración de redes virtuales. Disponible en internet: http://wiki.aprendeweb.org/index.php?title=Configuraci%C3%B3n_de_redes_virtuales#Nivel_2_-_VLAN_basadas_en_MAC Consultado marzo 2014.

Ventajas:

Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambia de lugar la reconfiguración del switch.

Multiprotocolo.
Se pueden tener miembros en múltiples VLANs.

Desventajas:

Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.

Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

La VLAN de nivel 3 o VLAN basada en protocolo[45], permite crear una red virtual por tipo de protocolo por ejemplo, TCP/IP, IPX, AppleTalk. Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Tener configurado VLANs significa tener los siguientes beneficios en la red:

Una computadora puede ser trasladada físicamente y seguirá permaneciendo a la misma VLAN sin ningún tipo de reconfiguración, ya están configurados como dominios lógicos.

Control y conservación del ancho de banda, ya que las redes virtuales tienen la posibilidad de restringir los broadcast a los dominios lógicos que se desee.

Conectividad, porque se puede conectar diferentes switch y expandir las redes virtuales atreves de los mimos, aunque este situados en lugares geográficamente distintos.

Aumento de la seguridad en la red, ya que los accesos desde y hacia los dominios lógicos pueden ser restringidos de acuerdo a las necesidades de cada red.

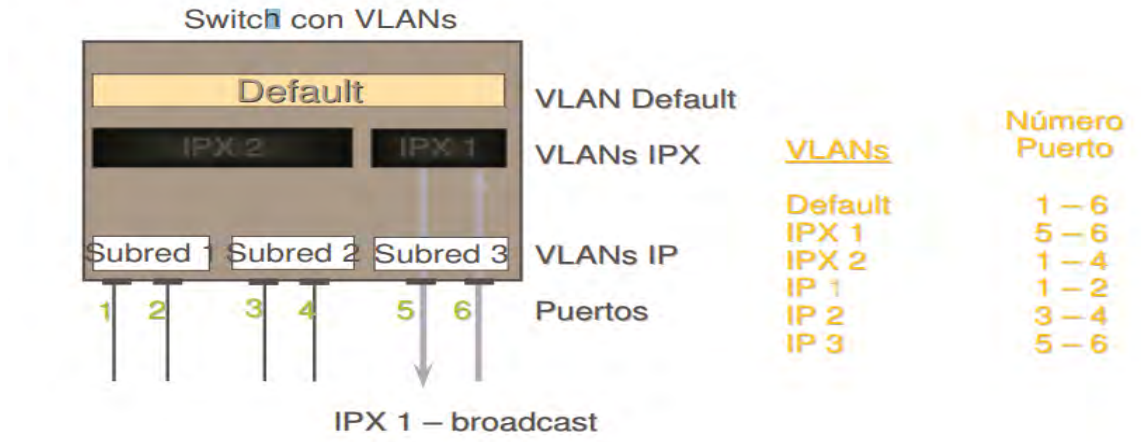
Disminución de tráfico en la red.

Ahorro de dinero, al utilizar conmutadores existentes**.**

Grupos de Trabajo Virtuales.

[45] UAZUAY, Estudios. Vlans. Disponible en internet: http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf consultado marzo 2014.

Figura 8. VLAN basadas en protocolo



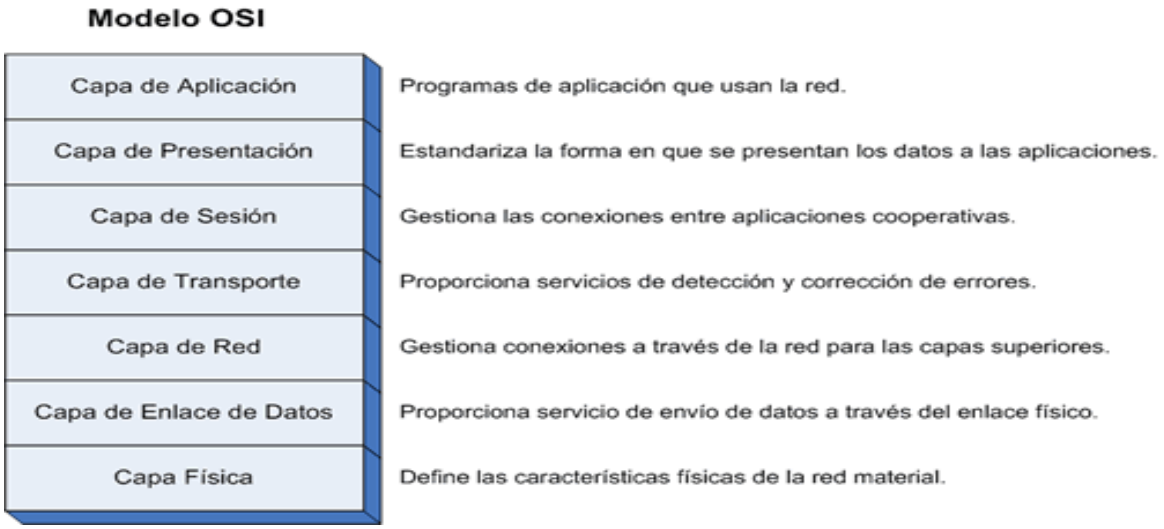
Fuente: APRENDEWEB. Configuración de redes virtuales. Disponible en internet: http://wiki.aprendeweb.org/index.php?title=Configuraci%C3%B3n_de_redes_virtuales#Nivel_2_-_VLAN_basadas_en_MAC Consultado marzo 2014.

1.8.12 Modelo de referencia OSI.[46]El modelo OSI fue creado por la ISO con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes, así todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado a este modelo con características muy precisas en cada nivel.

Este modelo es considerado una arquitectura de redes, ya que especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes, el mismo modelo que está dividido en siete capas como se muestra en la figura.

[46] UNICEN, Cátedras. El modelo osi. Disponible en internet: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf Consultado marzo 2014.

Figura 9. Capas del modelo OSI.



Fuente: TEXTOS CIENTIFICOS. Tcp/ip y el modelo OSI. Disponible en internet:http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi Consultado marzo 2014.

El nivel físico (capa1). Corresponde a la primera capa del modelo de referencia OSI y básicamente es la que se encarga de las conexiones físicas de la computadora hacia la red, pudiendo ser:

Medios guiados: Cable coaxial, cable de par trenzado, fibra óptica, etc.

Medios no guiados: Radio, infrarrojos, microondas, láser y otras redes inalámbricas.

Funciones de la capa física.[47]Esta capa se encarga de las siguientes funciones:

- Son los que transmiten el flujo de bits a través del medio.
- Son los que manejan las señales eléctricas y electromagnéticas.
- Define si la trasmisión es uni o bidireccional (simplex, dúplex o full-dúplex).
- Características del medio físico de trasmisión, es decir tipo de cable o calidad del mismo, tipo de conectores normalizados o a su vez tipo de antena.
- Definen las características de los materiales como componentes, conectores mecánicos y eléctricas, de este ultimo los niveles de tensión que se van a usar en la transmisión de los datos por los medios físicos.

[47] TEXTOS CIENTIFICOS. Tcp/ip y el modelo osi. Disponible en internet: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi Consultado marzo 2014.

- Definen las características funcionales de la interfaz, el establecimiento, mantenimiento y liberación del enlace físico.
- Son los que garantizan la conexión, aunque no la fiabilidad de ésta.

Capa de enlace de datos (capa 2).[48]El nivel de la capa de enlace de datos corresponde al segundo nivel del modelo de referencia OSI y es una capa lógica adicional sobre el nivel físico para controlar y gestionar el intercambio de información. El objetivo del nivel de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente.

Funciones de la capa física de enlace[49]

- Direccionamiento en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que el ordenador debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Distribución ordenada de tramas las mismas que son pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

Capa de red (capa 3).[50]La capa de red, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

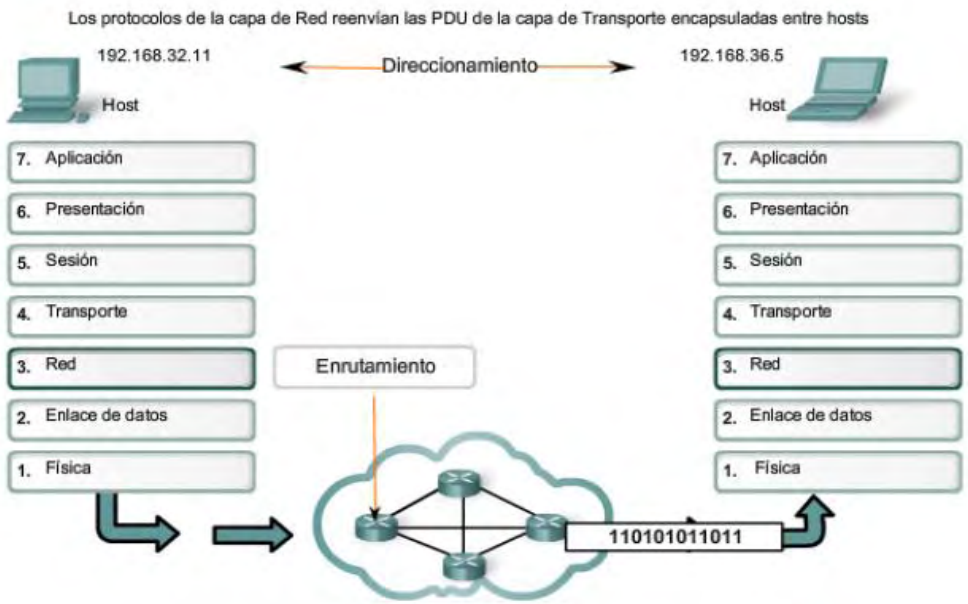
Para realizar la transferencia de archivos de extremo a extremo la Capa 3 utiliza cuatro procesos básicos: direccionamiento, encapsulamiento, enrutamiento y desencapsulamiento.

[48] Ibíd., Consultado marzo 2014.

[49] Ibíd., Consultado marzo 2014.

[50] Ibíd., Consultado marzo 2014.

Figura 10. Funcionamiento de la capa de red



Fuente: DITUYI. Capa de red. Disponible en internet: http://www.dituyi.net/capa-de-red/ Consultado marzo 2014.

Direccionamiento.[51]La Capa de red debe proveer un mecanismo para direccionar los dispositivos finales, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación.[52]El encapsulamiento trata de un proceso que envuelve los datos con la información de protocolo necesaria antes de transitar por la red, la información se mueve hacia abajo por las capas del modelo OSI, para que cada capa añada un encabezado, antes de pasarla a una capa inferior. Los encabezados contienen información de control para los dispositivos de red y receptores para asegurar la apropiada entrega de los datos y que el receptor interprete correctamente lo que recibe.

Enrutamiento.[53]El proceso de enrutamiento consiste en proveer los servicios para que a lo largo de la ruta, cada paquete pueda ser guiado a través de la red para

[51] DITUYI. Capa de red. Disponible en internet: http://www.dituyi.net/capa-de-red/ Consultado marzo 2014.

[52] Ibíd., Consultado marzo 2014.
[53] Ibíd., Consultado marzo 2014.

que llegue a su destino final, los mismos que no siempre están conectados a la misma red, esto se logra mediante los dispositivos intermediarios que conectan las redes, es decir los routers, cuya función es seleccionar las rutas y dirigir paquetes hacia su destino.

Desencapsulamiento.[54] Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de red, para luego pasar al servicio adecuado en la capa de Transporte.

El propósito de esta capa es el de formar una interface entre los usuarios de una máquina y la red, ya que la red es controlada por esta capa y las 2 primeras.

Direcciones de la capa de red[55]Las direcciones de la capa de red, también se las conoce como direcciones virtuales, las mismas que son de tipo jerárquico.

Una dirección de red virtual está conformada por dos partes: La primera corresponde a cada una de las redes de internet, y la otra parte corresponde a los hosts en cada una de las redes.

La parte de la red, identifica cada red dentro de la estructura de la internet, permitiendo que los routers identifiquen las rutas de conexión ya que el router utiliza esta dirección para determinar el host destino de los paquetes de red la parte del host identifica los dispositivos o un puerto de ese dispositivo.

Estructura de una dirección IP. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo que utilice el protocolo IP y está dividida en cuatro secciones de 8 bits llamados octetos, los mismos q identifican una red específica y un host en particular dentro de la red.

[54] Ibíd., Consultado marzo 2014.

[55] DIYUTI. Capa de red. Disponible en internet: http://www.dituyi.net/capa-de-red/ Consultado marzo 2014.

Tabla 1. Clases de direcciones IP.

Clase	Cantidad de redes posibles	Cantidad máxima de equipos en cada una
A	126	16777214
B	16384	65534
C	2097152	254

Fuente: USUARIO DEBIAN. Calculadora de direcciones ip. Disponible en internet: http://usuariodebian.blogspot.com/2012/02/gip-calculadora-de-direcciones-ip.html Consultado marzo 2014.

Direcciones IP reservadas. ICANN. [93] ha reservado una cantidad de direcciones, para evitar conflictos de direcciones IP en la red de redes estas direcciones son las siguientes:

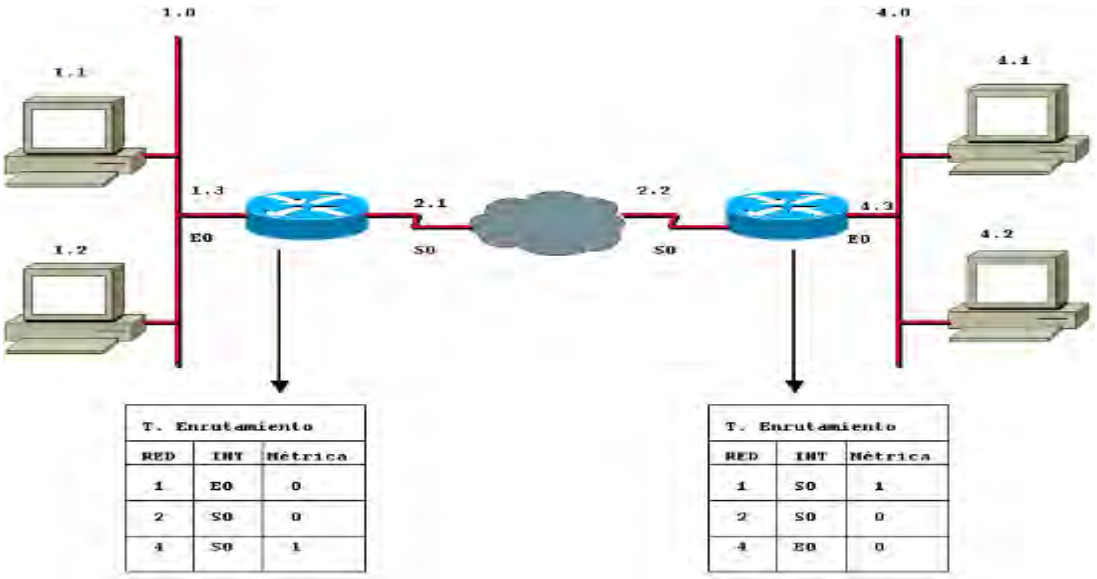
Direcciones IP privadas de clase A: 10.0.0.1 a 10.255.255.254; hacen posible la creación de grandes redes privadas que incluyen miles de equipos.

Direcciones IP privadas de clase B: 172.16.0.1 a 172.31.255.254; hacen posible la creación de redes privadas de tamaño medio.

Direcciones IP privadas de clase C: 192.168.0.1 a 192.168.0.254; para establecer pequeñas redes privadas.

Operativa del router en la capa de red. Los routers operan en la capa de red registrando y grabando las diferentes redes y eligiendo la mejor ruta para las mismas.

Figura 11. Routers capa de red



Fuentes: UNIVERSIDAD CESAR VALLEJO. Router y switch. Disponible en internet: http://es.slideshare.net/mcwilmermary/ucv-sesion-13-router1 Consultado marzo 2014.

La operativa del Router en la capa de Red. Los routers colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos:

Dirección de red[56]. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

Interfaz. Se refiere a la interfaz usada por el router para llegar a una red dada esta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

Métrica. [57]Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita al router la elección de la mejor ruta, para llegar al host destino. Esta métrica cambia en función de la forma en que el router elige las rutas.

Entre las métricas más habituales están las siguientes:

[56] UNIVERSIDAD CESAR VALLEJO. Router y switch. Disponible en internet: http://es.slideshare.net/mcwilmermary/ucv-sesion-13-router1 Consultado marzo 2014.
[57]Ibíd., Consultado marzo 2014.

- El número de redes que han de ser cruzadas para llegar al destino (conocido también como saltos).
- El tiempo que se tarda en atravesar todas las interfaces hasta una red dada (conocido también como retraso).

- Valor asociado con la velocidad de un enlace (conocido también como ancho de banda).

Para que los routers puedan operar en una red, es necesario que cada tarjeta esté configurada en la red. El router utiliza la información de configuración de la tarjeta para determinar la parte de la dirección correspondiente a la red, a fin de construir una tabla de enrutamiento.

Además de identificar redes y proporcionar conectividad, los router deben proporcionar las siguientes funciones:

- Los routers separan las tramas de Capa 2 y envían paquetes basados en direcciones de destino Capa 3.
- Los routers asignan una dirección lógica de capa 3 individual a cada dispositivo de red por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete ya que pueden incluir o sacar paquetes.

- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.

- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.

- Los routers soportan una gran variedad de estándares de conectividad al nivel de la capa física, lo cual ofrece la posibilidad de construir WAN.

- Además, pueden proporcionar controles de acceso y seguridad, que son elementos necesarios cuando se conectan ubicaciones remotas.

Capa de transporte (capa 4).[58]La capa transporte es el cuarto nivel del modelo OSI, encargado del transporte de paquetes confiable y eficiente de la máquina origen a la destino, independientemente del tipo de red física que se esté utilizando.

Para lograr este objetivo, la capa de Transporte, hace uso de los servicios proporcionados por la capa de red. El hardware o software que se encarga del trabajo se llama entidad de transporte que puede estar:

[58] TEXTOS CIENTIFICOS. Tcp/ip y el modelo osi. Disponible en internet: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi Consultado marzo 2014.

- En la Tarjeta de interfaz de red
- En el núcleo del sistema operativo
- En un proceso de usuario independiente
- En un paquete de biblioteca que forma parte de las aplicaciones de la red.

La capa de sesión (capa 5).[59]La capa de sesión es el quinto nivel del modelo de referencia OSI, la misma que organiza y sincroniza el diálogo y controla el intercambio de datos, además de controlar el diálogo entre las aplicaciones de los sistemas finales.

Permite a los usuarios de máquinas diferentes establecer sesiones entre ellos, permitiendo el transporte ordinario de datos, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

La capa de sesión tiene las siguientes funciones.

- **Control del diálogo**: Quién habla, cuándo, cuánto tiempo, este puede ser simultáneo en los dos sentidos (full-dúplex) o alternado en ambos sentidos (half-duplex).

- **Agrupamiento**: El flujo de datos se puede marcar para definir grupos de datos.

- **Recuperación**: La capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación y no desde el principio.

- **Establecer sesión:** Permite a usuarios en diferentes máquinas establecer una sesión la cual puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas.

Capa de presentación (capa 6).[60]La capa de presentación es el sexto nivel del modelo de referencia OSI, se podría definir como un protocolo de paso de la información desde las capas adyacentes , a diferencia de todas las capas inferiores que se interesan solo en mover bits de manera confiable de la maquina origen a la maquina destino, la capa de presentación se ocupa de la sintaxis y la

[59] Ibíd., Consultado marzo 2014.
[60] TEXTOS CIENTIFICOS. Tcp/ip y el modelo osi. Disponible en internet: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi Consultado marzo 2014.

semántica de la información que se transmite, además de ser necesario esta capa puede traducir entre distintos formatos de datos, ordenar y organizar los datos antes de su transferencia.

Función de la capa de presentación.[61]Está a cargo de la presentación de los datos en una forma que el dispositivo receptor pueda comprender.

Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta una de sus funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión.

Para comprender esto mejor maneja dos sistemas:

- El primer sistema utiliza el código de caracteres decimales codificados en binario (EBCDIC) para representar los caracteres en la pantalla.

- El segundo sistema utiliza el Código (ASCII) para el intercambio de la información, la capa de presentación opera como traductor entre estos dos tipos diferentes de códigos.

Comprimir los datos si es necesario.

Aplicar a los datos procesos criptográficos.

Cifrado y compresión de datos. La capa de presentación, protege la información durante la transmisión, ya que utiliza una clave de cifrado para cifrar los datos en el lugar origen y luego descifrarlos en el lugar destino, la capa de presentación también se ocupa de la compresión de los archivos, es decir reducir el tamaño de los archivos, esto se realiza mediante el uso de algoritmos.

Capa de aplicación (capa 7).[62]La capa de aplicación es el séptimo nivel del modelo de referencia OSI, ofrece la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros.

Cabe aclarar que el usuario no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, un ejemplo claro es, cuando chateamos con el messenger no es necesario que codifiquemos la información y los datos del destinatario para

[61]Ibíd.
[62] Ibíd., Consultado marzo 2014.

entregarla a la capa de presentación para que esta a su vez realice él envió del paquete.

Tabla 2. Protocolos que intervienen en esta capa de aplicación.

Protocolo	Uso
HTTP (HyperText Transfer Protocol)	Para acceso a páginas web
FTP (File Transfer Protocol)	Transferencia de archivos.
SMTP (Simple Mail Transfer Protocol)	Envío y distribución de correo electrónico.
POP (Post Office Protocol)	Correo electrónico.
SSH (Secure Shell)	Cifra casi cualquier tipo de transmisión.
Telnet	Para acceder a equipos remotos.
DNS (Domain Name Service)	Servicio de nombres de dominio.

Fuente: Capa de aplicación. Disponible en internet: http://es.wikipedia.org/wiki/Capa_de_aplicaci%C3%B3n Consultado marzo 2014.

Función de la capa de aplicación.

- La capa de aplicación es responsable de lo siguiente:
- Identifica y establece la disponibilidad de los socios de comunicación deseados.
- Sincroniza las aplicaciones que cooperan.
- Establece acuerdos con respecto a los procedimientos para la recuperación de errores.
- Controla la integridad de los datos.

1.9 SEGURIDAD INFORMÁTICA[63]

La seguridad puede dividirse, a grandes rasgos, en dos grandes bloques: seguridad física y seguridad lógica. Para salvaguardar los activos de la empresa no puede existir una sin la otra, ambas son complementarias.

De nada sirve controlar los accesos físicos a las instalaciones para no sufrir percances y mantener a salvo los bienes, si un individuo puede acceder a la

[63] CATARINA. Seguridad informática. Conceptos básicos. Disponible en internet: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf Consultado marzo 2014.

información confidencial de la compañía cómodamente desde el ordenador de su casa.

1.9.1 La seguridad física. Cuyo término hace referencia a la protección de la organización frente a accesos no autorizados y ataques físicos a los ordenadores, instalaciones, personal, documentación, etc.

1.9.2 La seguridad lógica.[64] La cual garantiza la seguridad a nivel de los datos, permitiendo el acceso lógico a la información sólo a personas autorizadas. La seguridad lógica aplica mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio.

Algunos de los controles utilizados en la seguridad lógica son:

- Se limita el acceso a determinados aplicaciones, programas o archivos mediante claves o a través de la criptografía.
- Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.
- Cerciorarse de los archivos, las aplicaciones y programas que se utilizan en la compañía se adaptan a las necesidades y se usan de manera adecuada por los empleados.
- Controlar que la información que entra o sale de la empresa es íntegra y sólo está disponible para los usuarios autorizados.

1.9.3. Autenticación.[65]Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

---

[64] RIOS, Julio. Seguridad informática. Disponible en internet: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml Consultado marzo 2014.

[65] Ibíd., Consultado marzo 2014.

Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.

- Algo que la persona posee: por ejemplo una tarjeta magnética.

- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.

- Algo que el individuo es capaz de hacer**:** por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación.

1.9.4. Integridad.[66]La integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la huella digital es uno de los pilares fundamentales de la seguridad de la información.

1.9.5. Confidencialidad.[67]La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte

---

[66] RIOS, Julio. Seguridad informática. Disponible en internet: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml Consultado marzo 2014.

[67] RIOS, Julio. Seguridad informática. Disponible en internet: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml Consultado marzo 2014.

no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

1.9.6 Amenazas lógicas.[68]Para evitar posibles amenazas lógicas en la red de datos, es importante que todos los empleados, especialmente los administradores de los equipos, tomen conciencia del cuidado que deben poner para que no se materialicen posibles daños. Además, es fundamental implementar mecanismos de prevención, detección y recuperación ante posibles amenazas lógicas como virus, gusanos, bombas lógicas y otros códigos maliciosos.

La expansión de la cultura de la seguridad entre los empleados puede ahorrar muchos disgustos a la entidad, muchas veces implementando medidas tan sencillas como, por ejemplo:

- No ejecutar programas de los que se desconozcan su procedencia.
- No utilizar programas no autorizados por la dirección.
- No abrir correos personales desde los equipos de la compañía.
- No visitar páginas web que no sean propósito de la empresa.
- Instalar y actualizar habitualmente un software dedicado detectar y eliminar códigos maliciosos que puedan albergar los ordenadores.
- Realizar chequeos de los correos electrónicos recibidos para comprobar que no suponen una amenaza para la entidad.

A continuación, se detallan las amenazas lógicas más frecuentes que pueden dañar los bienes de la empresa y las posibles formas de evitar o disminuir la probabilidad de ocurrencia y el impacto que causaría en la entidad.

Malware.[69]Un malware es todo software diseñado para realizar acciones maliciosas sobre el sistema. La palabra malware proviene del inglés “malicious software”, es decir software malicioso o también llamado badware. Existen gran cantidad de malware y seguramente aparecerán nuevos tipos, según evolucionen

[68] BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

[69] BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

las nuevas tecnologías. En los sucesivos apartados se detallarán los badware más relevantes:

- Virus
- Gusanos
- Troyanos
- Bombas lógicas
- Adware
- Spyware
- Puertas traseras
- Spam

Virus.[70]Un virus es una secuencia de código que se aloja en un fichero ejecutable denominado host (huésped) de manera que al ejecutar el programa también se ejecuta el virus. Llevan a cabo diversas acciones que interfieren en el correcto funcionamiento del ordenador sin conocimiento del usuario. Los virus informáticos son muy habituales en la red y pueden provocar daños irreparables.

En algunas ocasiones, borran información necesaria para el correcto funcionamiento del sistema, y esto provoca que el disco duro tenga que ser formateado para reparar el daño. Ocupan poco espacio en disco, característica importante para que el virus pueda pasar inadvertido el máximo tiempo posible. Se auto-replican, es decir, se realizan copias de sí mismo para expandirse rápidamente.

El ciclo de vida de un virus es el siguiente:

- El virus es programado.
- Se expande.
- Realiza la función maliciosa para la que está programado.

Finalmente, pueden ocurrir dos cosas: se produce su extinción o se produce una mutación. En este último caso, se repite el ciclo.

Los virus se pueden agrupar en dos tipos:

- **Virus benignos:** estos virus están programados para molestar al usuario pero no dañan al sistema.

- **Virus malignos:** causan algún tipo de daño en el sistema.

[70] Ibíd., Consultado Marzo 2014.

Es posible distinguir tres módulos en los virus informáticos:

- Módulo de reproducción: Maneja las rutinas para infectar a las entidades ejecutables procurando que el virus pase desapercibido a los ojos del usuario y, de esta forma, infectar otras entidades que cuando se ejecutan en otros ordenadores se consigue que el virus se propagarse rápidamente.

- Módulo de ataque: Contiene las rutinas de daño adicional. Este módulo, se activa con determinados eventos en el sistema como, por ejemplo, una fecha, una hora, si se encuentra un archivo determinado o lo que el programador del virus decidiera atacar.
- Módulo de defensa: Las rutinas de este módulo se encargan de proteger al virus e intentar que pase desapercibido el mayor tiempo posible.

Gusanos.[71]En inglés, el término que se utiliza es "worm". Los gusanos son programas capaces de ejecutarse por sí mismos (a diferencia de los virus que necesitan de la existencia de un fichero ejecutable) y propagarse por la red. A día de hoy, constituyen una amenaza habitual en Internet y las consecuencias que conllevan pueden ser fatales y se consideran como una subclase de virus informático.

Residen en memoria y tiene gran capacidad para replicarse pudiendo incluso, enviar copias de sí mismo a otros equipos por medio de correos electrónicos. Es frecuente detectar que nuestro ordenador está infectado con un gusano cuando los recursos del sistema se consumen y detectamos que la máquina desempeña su actividad muy lentamente. Esto es debido a que el gusano se auto-replica y envía copias a otros ordenadores a través de las redes de comunicación sin intervención de ningún usuario.

Troyanos.[72]Un caballo de Troya o troyano es un programa que bajo una apariencia inofensiva y útil para el usuario se inserta en un ordenador, y permite que usuarios externos accedan a la información contenida o controlen de forma remota el equipo. Los troyanos son creados para obtener información privilegiada de la máquina anfitriona. No necesariamente provocan daños en la computadora infectada y, a diferencia de los virus y los gusanos, los troyanos no se reproducen.

Generalmente los caballos de Troya son utilizados para espiar, instalando en la máquina anfitriona un software de acceso remoto para observar las actividades

[71]BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

[72]Ibíd., Consultado Marzo 2014.

que realiza el usuario del ordenador. Estos troyanos reciben el nombre de programa espía o spyware. Si lo que se pretende es capturar secuencias insertadas en el teclado para conseguir contraseñas reciben el nombre de key logger.

También existen troyanos que pueden abrir puertas traseras al ordenador para que un tercero realice las acciones maliciosas que persiga.

Para evitar que nuestros ordenadores se infecten de troyanos, no debemos ejecutar ningún programa ni fichero ejecutable del que se desconozca el origen, además de contar con un antivirus actualizado y un software anti-troyanos.

Bombas lógicas.[73]Las bombas lógicas son programas que se activan después de cierto tiempo causando daños en el sistema. Es muy común en empleados descontentos que abandonan una empresa (por ejemplo, porque han sido despedidos o han decidido trabajar para la competencia) e introducen una bomba lógica en los ordenadores de la organización con el fin de que cuando se cumplan unas condiciones que el individuo haya establecido, la bomba lógica se active y cause algún tipo de daño en el sistema.

De esta manera, no levantaría sospechas. Las bombas lógicas se activan porque se cumplen algunas de las siguientes condiciones:

- En una fecha concreta.
- En una hora determinada.
- Si un contador interno llega a un número concreto.
- Se alcanza cierto número de ejecuciones del programa que contiene la bomba lógica.
- Si se cumplen otras características establecidas por el atacante.

Por lo tanto, una bomba lógica puede permanecer inactiva durante un largo periodo de tiempo, de manera que nadie nota ningún comportamiento extraño en el sistema hasta que la bomba se activa. En esta característica, radica el poder dañino de las bombas lógicas. Pueden realizar diversas acciones, desde mostrar un simple mensaje hasta borrar información importante del disco duro.
Debido a que es muy común este tipo de sabotaje por parte de empleados a punto de abandonar la organización, es vital inhabilitarles el acceso a los sistemas para que no puedan acceder desde el momento en el que se les informe de su despido.

[73] BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

Adware.[74]Los adware son aplicaciones que muestran publicidad o la descarga al equipo del usuario cuando éste instala un programa. “Ad” es el diminutivo de advertisement que en castellano significa anuncio. Muchos programas de descarga gratuita contienen adware de esta forma, los creadores del programa consiguen un beneficio económico.

El usuario, al instalar el programa, no es consciente de la descarga del adware. En ocasiones, pueden remplazar la página de inicio del navegador, aparecer ventanas pop-ups con publicidad o instalarse aplicaciones no deseadas.
Por ejemplo, al instalar un programa, en las opciones que vienen marcadas “por defecto”, aceptamos la instalación de una barra de herramientas en nuestro navegador. Hoy en día, los antivirus incluyen herramientas de detección de adware. Sin embargo, toda precaución es poca y los usuarios deben asegurarse que el programa que instalan no contiene adware leyendo cuidadosamente el contrato de licencia. Además, se debería instalar alguna herramienta que bloquee las ventanas emergentes y evitar así, las ventanas de adware.

Spyware.[75]El spyware o software espía envía información personal del usuario a terceros sin que éste tenga conocimiento sobre lo sucedido. Vulneran la privacidad de los usuarios. La información enviada puede ser las páginas web que se visitan o algo más comprometido como contraseñas o números de tarjetas de crédito.

Habitualmente las empresas utilizan esa información para enviar publicidad a los usuarios. Al igual que los adware, se pueden instalar al descargar un programa y aceptar las condiciones de uso. Para evitar instalar este software malicioso en los equipos de la compañía, lo más adecuado es poner en práctica las medidas comentadas en el apartado de adware. Además de los antivirus que los detectan, existen diversos programas anti-spyware.

Spam.[76]Un spam o correo basura es un mensaje publicitario enviado al correo electrónico de un gran número de usuarios sin que éstos lo hubiesen solicitado. Sobrecargan los servidores de correo y los usuarios tienen que invertir tiempo en eliminarlos.

[74] BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

[75] Ibíd., Consultado Marzo 2014.

[76] BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

Ingeniería social.[77]La ingeniería social consiste en la manipulación de las personas para que de manera voluntaria, lleven a cabo actos que de otro modo no realizarían. Es una técnica muy sencilla y desafortunadamente, muy efectiva.

Por ejemplo, se utiliza la ingeniería social cuando se descarga un programa de Internet pensado que es un antivirus para el ordenador y, de esta forma, estar a salvo de posibles amenazas. Al ejecutar el programa la computadora es infectada por un troyano. Si al descargar el software para su equipo, en lugar de llamarse "Antivirus X" se denominara "Troyano", nadie lo descargaría.

Nunca debemos ejecutar programas de los que se desconozca el origen. Los atacantes se aprovechan de los usuarios confiados y de su falta de cultura en medidas de seguridad.

Sniffing.[78]El sniffing consiste en capturar cualquier paquete que circulan por la red. Se puede realizar sniffing por software o por hardware. En este último caso, se conecta un dispositivo a un cable de red para capturar los paquetes que viajen a través del cable (esta práctica recibe el nombre de wiretapping).
Generalmente el sniffing se realiza por software. Un programa captura la información de la red almacenándola, habitualmente, en un fichero al que accede el atacante.

Las tramas que circulan por delante de la máquina en la que se encuentra instalado el sniffer son captadas aunque la información no vaya dirigida a dicha máquina.

Redes sociales.[79]Las redes sociales han surgido en los últimos años para revolucionar la manera de comunicarnos vía Internet. Estas redes, nos permiten mostrar y compartir fotos, videos, comentarios, etc. Sin embargo, en ocasiones, suponen una amenaza en nuestra seguridad tanto física como lógica. A través de los mensajes publicados, los vídeos y las fotos, es fácil que los demás usuarios conozcan dónde nos encontramos, quiénes son nuestros amigos y familia y qué hacemos en cada momento.

Relativo a la seguridad lógica, un intruso podría crearse un perfil con el nombre y apellidos de un tercero conocido por la víctima. De esta manera, la víctima

[77]Ibíd., Consultado Marzo 2014.

[78]Ibíd., Consultado Marzo 2014.
[79]BORGHELLO, Cristian. Amenazas lógica. Tipos de ataques. Disponible en internet: http://www.segu-info.com.ar/ataques/ataques.htm Consultado marzo 2014.

aceptaría a su supuesto amigo para que ambos pudieran comunicarse a través de la red social. El intruso, haciendo uso de la ingeniería social, podría solicitarle información personal para hacer uso ilícito de ella.

Otra amenaza de la seguridad lógica radica en que estas redes sociales se han convertido en un medio para propagar **malware**. En varias redes como Facebook, es posible el intercambio de pequeñas aplicaciones realizadas por terceros que no han sido desarrolladas por los informáticos de la propia red. Algunas de estas aplicaciones con aspecto inofensivo contienen código malicioso. Las aplicaciones pueden ser recomendadas por sus amigos o familiares, lo que dificulta que estos usuarios desconfíen.
.

Métodos de protección

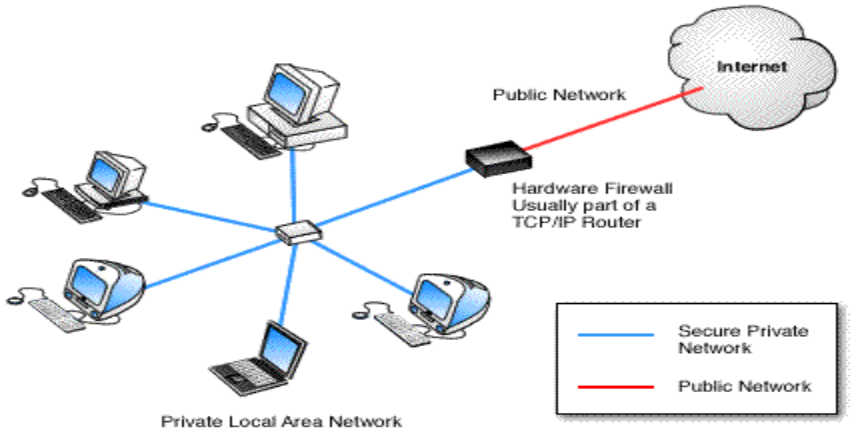
Firewall (Cortafuegos).[80]Un firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).
Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.

- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

[80]BORGHELLO, Cristian. Firewall. Tipos de firewall. Disponible en internet: http://www.segu-info.com.ar/fisica/seguridadfisica.htm .Consultado marzo 2014.

Figura 12. Firewall



Fuente: BORGHELLO, Cristian. Firewall. Tipos de firewall. Disponible en internet: http://www.segu-info.com.ar/fisica/seguridadfisica.htm .Consultado marzo 2014.

Como puede observarse en la figura el muro cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa. Algunos firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para establecer la comunicación.

Tipos de firewall[81]

Filtrado de paquetes (capa de transporte y red).Se utilizan routers con filtros y reglas basadas en políticas de control de acceso.

El router es el encargado de filtrar los paquetes basados en cualquiera de los siguientes criterios:

- Protocolos utilizados.
- Dirección IP de origen y de destino.
- Puerto TCP-UDP de origen y de destino.

[81] BORGHELLO, Cristian. Firewall. Tipos de firewall. Disponible en internet: http://www.segu-info.com.ar/fisica/seguridadfisica.htm .Consultado marzo 2014.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico.

Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de firewalls trabajan en los niveles de transporte y de red del modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

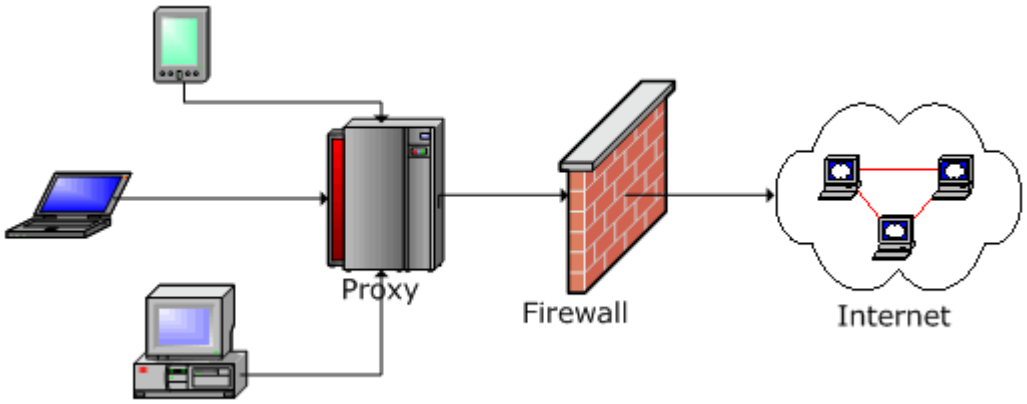
- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior. Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

Proxy-Gateway de aplicaciones.[82]Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como servidores proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastión Host.

El proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes. Cuando un usuario desea un servicio, lo hace a través del proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

[82]ORICODE. Firewalls and Proxies Explained. Disponible en internet: http://www.postcastserver.com/help/Firewalls_and_Proxies_Explained.aspx Consultado marzo 2014.

Figura 13. Firewall por proxy



Fuente: ORICODE. Firewalls and Proxies Explained. Disponible en internet: http://www.postcastserver.com/help/Firewalls_and_Proxies_Explained.aspx Consultado marzo 2014.

Inspección de paquetes.[83]Este tipo de firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de red hasta la de aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

Restricciones de un firewall.[84]Los cortafuegos no pueden proteger contra los ataques que no pasan a través del cortafuego. Muchas empresas que se conectan a Internet están muy preocupados por los datos de propiedad se escapan fuera de la empresa a través de esa ruta. Por desgracia para los interesados, una cinta magnética, disco compacto, DVD o unidades flash USB se puede con la misma eficacia puede utilizar para exportar datos.

Otra cosa que un firewall no puede realmente proteger es contra es espías informáticos dentro de su red. Mientras que un espía industrial podría exportar la información a través de su servidor de seguridad, que es igual de probable que exportarlo a través de teléfono, fax, o disco compacto. Los CD son un medio mucho más probable que los medios de información a fugas de una organización que de un firewall.

[83]ORICODE Firewalls and Proxies Explained. Disponible en internet: http://www.postcastserver.com/help/Firewalls_and_Proxies_Explained.aspx Consultado marzo 2014.
[84]Ibid. Consultado Marzo 2014.

Los firewalls tampoco puede proteger la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Otra cosa que el firewall no puede hacer es que el firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del firewall y difunde esta información, el firewall no se dará cuenta.

Finalmente se puede concluir que un firewall trabaja mejor si se complementa con una defensa interna y un manejo apropiado de la información por parte de los usuarios.

Ventajas de un firewall.[85]Los firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el firewall.

Los firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

[85]ORICODE Firewalls and Proxies Explained. Disponible en internet: http://www.postcastserver.com/help/Firewalls_and_Proxies_Explained.aspx Consultado marzo 2014.

Copia de seguridad. [86]Las copias de seguridad se utilizan con el fin de recuperar la información del sistema en el caso de que se produzca la pérdida de la misma. La información se almacena en dispositivos de almacenamiento que se depositan en un lugar seguro. De esta manera, se consigue restaurar el sistema en el caso de que se produzca un fallo. Los fallos en el sistema pueden ser:

- Físicos: se originan fallos en el hardware.
- De diseño: se producen fallos en los programas.
- De operación: causados por la intervención humana.
- De entorno: producidos por desastres naturales o del entorno.

Realizar copias de seguridad o backups es vital para la continuidad del negocio. La fiabilidad de los datos almacenados en las copias de seguridad dependerá de la frecuencia con la que se realicen tales copias y de la frecuencia con la que actualice la información de la compañía. La periodicidad con la que se realicen backups dependerá de la empresa, del grado de criticidad de la información y del nivel de actualización de ésta.

Por ejemplo, un banco necesita realizar copias de seguridad constantemente ya que a cada momento, se están actualizando datos en las cuentas bancarias de los clientes.

Existen varios tipos de backups:

Copias de seguridad integral o completa: se realizan copias del fichero completo sin tener en cuenta que la información ya hubiera sido copiada. Generalmente se realizan semanalmente.
Copias de seguridad incrementales: copia los archivos que tienen activado el atributo de modificado, es decir, sólo se copia la información actualizada. Cuando se realiza la copia de seguridad el atributo de modificado se desactiva. Se realiza una copia completa del fichero únicamente la primera vez que se copia. Ahorra espacio pero para recuperar un fichero es necesario recurrir a la última copia completa y a todas las copias incrementales realizadas hasta el momento.

Copias de seguridad diferencial: es muy similar a los backups incrementales. La diferencia reside en que el atributo de modificado no se desactiva hasta que no se realiza un backup completo o incremental. Para recuperar un fichero se utiliza la última copia completa y la última diferencial. Por este motivo, la recuperación de archivos es más rápida que con copias incrementales aunque necesitan más dispositivos de almacenamiento.

[86]FELLOWS, Russ. Copia de seguridad completa, incremental o diferencial: cómo elegir el tipo adecuado .Disponible en internet: http://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado Consultado marzo 2014.

Los dispositivos que se utilizan para llevar a cabo los backups son diversos, desde cintas magnéticas, CD, DVD, pendrive hasta centros de respaldos remotos propios o vía Internet. Las copias de seguridad se suelen realizar de forma automática cuando se trata de grandes sistemas, utilizando aplicaciones software específica para ese fin. Los backups deben almacenarse en lugares seguros y lo más alejados posibles de la información respaldada. De nada sirve tener copias de seguridad actualizadas en un armario de las instalaciones donde se encuentra la información si un incendio puede destruir el edificio y acabar con ellas.

Es importante conocer el tiempo con el que se dispone para realizar el backup. Mientras se efectúa la copia, es oportuno no realizar modificaciones sobre los ficheros que se estén respaldando. Por este motivo, es necesario planificar el tiempo del que se dispone para realizar las copias que dependerá, en gran medida, de la cantidad de información que haya que respaldar, el tipo de copia y el dispositivo utilizado, y así, evitar que afecte al funcionamiento normal del sistema.

1.10 SISTEMAS DE CABLEADO ESTRUCTURADO[87]

1.10.1. Reglas del cableado estructurado. El cableado estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, administradores de red y cualquier otro técnico que trabaje con cables.

Hay tres reglas que ayudan a garantizar la efectividad y eficiencia en los proyectos de diseño del cableado estructurado.

- Buscar una solución completa de conectividad. Una solución óptima para lograr la conectividad de redes abarca todos los sistemas que han sido diseñados para conectar, tender, administrar e identificar los cables en los sistemas de cableado estructurado. La implementación basada en estándares está diseñada para admitir tecnologías actuales y futuras. El cumplimiento de los estándares servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo.

- Planificar teniendo en cuenta el crecimiento futuro. La cantidad de cables instalados debe satisfacer necesidades futuras. Se deben tener en cuenta las soluciones de categoría 5e, categoría 6 y de fibra óptica para garantizar que se satisfagan futuras necesidades. La instalación de la capa física debe poder funcionar durante diez años o más.

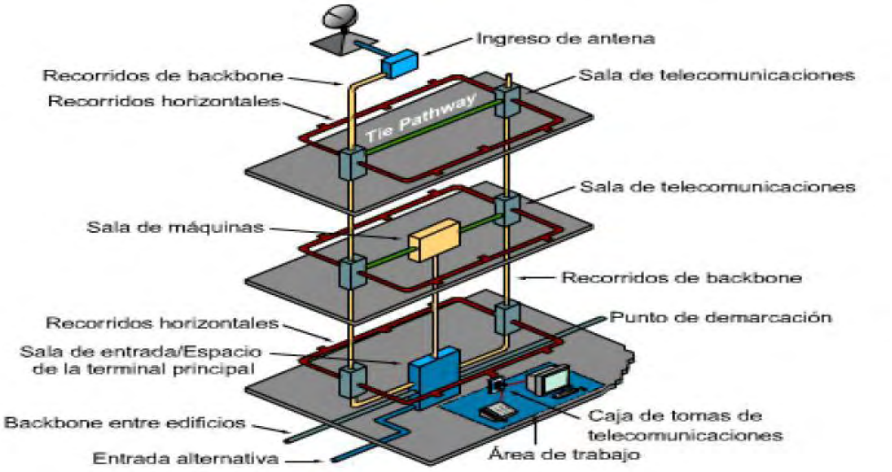
[87]CARABAJO SIMBAÑA, Grace Paola. Análisis, diseño del cableado estructurado y propuesta de implementación en la ilustre municipalidad del cantón sucúa. Cuenca, Noviembre de 2010. 196 p. Tesis previa a la obtención del título de ingeniero de sistemas. Facultad de ingeniería. Carrera: ingeniería de sistemas.

▪ Conservar la libertad de elección de proveedores. Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones.

1.10.2. Subsistemas de cableado estructurado.[88]Existen siete subsistemas relacionados con el sistema de cableado estructurado, cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables:

- Punto de demarcación (demarc) dentro de las instalaciones de entrada (EF) en la sala de equipamiento.
- Sala de equipamiento.
- Sala de telecomunicaciones.
- Cableado backbone, también conocido como cableado vertical.
- Cableado de distribución, también conocido como cableado horizontal.
- Área de trabajo.
- Administración.

Figura 14. Subsistemas de Cableado Estructurado



Fuente: PÉREZ, Diego. Cableado estructurado. Disponible en internet: http://cableadoestructuradodiego.blogspot.com/2011/07/reglas-para-cableado-estructurado-de.html. Consultado marzo 2014

[88] PEREZ, Diego. Cableado estructurado. Disponible en internet: http://cableadoestructuradodiego.blogspot.com/2011/07/reglas-para-cableado-estructurado-de.html. Consultado marzo 2014

El demarc es donde los cables del proveedor externo de servicios se conectan a los cables del cliente en su edificio.

El cableado backbone está compuesto por cables de alimentación que van desde el demarc hasta la salas de equipamiento y luego a la salas de telecomunicaciones en todo el edificio.

El cableado horizontal distribuye los cables desde las salas de telecomunicaciones hasta las áreas de trabajo.

Las salas de telecomunicaciones es donde se producen las conexiones que proporcionan una transición entre el cableado backbone y el horizontal.

Estos subsistemas convierten al cableado estructurado en una arquitectura distribuida con capacidades de administración que están limitadas al equipo activo, como por ejemplo los PC, switches, hubs, etc. El diseño de una infraestructura de cableado estructurado que enrute, proteja, identifique y termine los medios de cobre o fibra de manera apropiada, es esencial para el funcionamiento de la red y sus futuras actualizaciones.

1.10.3. Escalabilidad.[89]En telecomunicaciones y en ingeniería informática, la escalabilidad es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

En una LAN que es capaz de adaptarse a un crecimiento posterior se denomina red escalable. Es importante planear con anterioridad la cantidad de tendidos y de derivaciones de cableado en el área de trabajo. Es preferible instalar cables de más que no tener los suficientes.

Además de tender cables adicionales en el área de backbone para permitir posteriores ampliaciones, por lo general se tiende un cable adicional hacia cada estación de trabajo o escritorio, esto ofrece protección contra pares que puedan fallar en cables de voz durante la instalación, y también permite la expansión. Por otro lado, es una buena idea colocar una cuerda de tracción cuando se instalan los

[89] PEREZ, Diego. Cableado estructurado. Disponible en internet: http://cableadoestructuradodiego.blogspot.com/2011/07/reglas-para-cableado-estructurado-de.html. Consultado marzo 2014

cables para facilitar el agregado de cables adicionales en el futuro. Cada vez que se agregan nuevos cables, se debe también agregar otra cuerda de tracción.

Escalabilidad del backbone.[90]Al decidir qué cantidad de cable de cobre adicional debe tender, primero determine la cantidad de tendidos que se necesitan en ese momento y luego agregue aproximadamente un 20 por ciento más. Una forma distinta de obtener capacidad de reserva es mediante el uso de cableado y equipamiento de fibra óptica y en el edificio del backbone. Por ejemplo, el equipo de terminación puede ser actualizado insertando láser y controladores más veloces que se adapten al aumento de la cantidad de fibras.

Escalabilidad del área de trabajo. Cada área de trabajo necesita un cable para la voz y otro para los datos. Sin embargo, es posible que otros equipos necesiten una conexión al sistema de voz o de datos. Las impresoras de la red, las máquinas de FAX, los computadores portátiles, y otros usuarios del área de trabajo pueden requerir sus propias derivaciones de cableado de red. Una vez que los cables estén en su lugar, use placas de pared multipuerto sobre los jacks.

Punto de demarcación.[91]El punto de demarcación (demarc) es el punto en el que el cableado externo del proveedor de servicios se conecta con el cableado backbone dentro del edificio. Representa el límite entre la responsabilidad del proveedor de servicios y la responsabilidad del cliente.

En muchos edificios, el demarc está cerca del punto de presencia (POP) de otros servicios tales como electricidad y agua corriente.

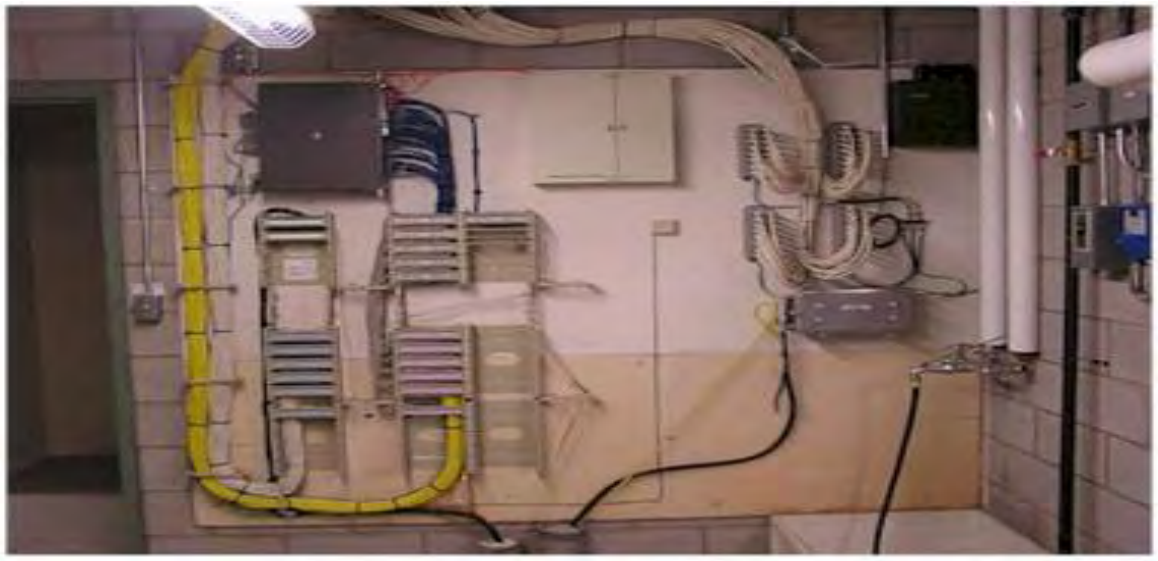
El proveedor de servicios es responsable de todo lo que ocurre desde el demarc hasta la instalación del proveedor de servicios. Todo lo que ocurre desde el demarc hacia dentro del edificio es responsabilidad del cliente, el proveedor de telefonía local normalmente debe terminar el cableado dentro de los 15 m (49,2 pies) del punto de penetración del edificio y proveer protección primaria de voltaje. Por lo general, el proveedor de servicios instala esto.

El estándar TIA/EIA-569-A especifica los requisitos para el espacio del demarc. Los estándares sobre el tamaño y estructura del espacio del demarc se relacionan con el tamaño del edificio. Para edificios de más de 2000 metros cuadrados (21.528 pies cuadrados), se recomienda contar con una habitación dentro del edificio que sea designada para este fin y que tenga llave.

[90] Ibíd. . Consultado marzo 2014.

[91]Ibíd., Consultado marzo 2014.

Figura 15. Punto de demarcación



Fuente: IDTECHNOLOGY .Sistema de transporte de información. Disponible en internet: https://idtechnology.wordpress.com/category/curso-cableado-estructurado/ Consultado marzo 2014.

1.10.5. Salas de equipamiento y telecomunicaciones.[92]La sala de equipamiento es el centro de la red de voz y datos. La sala de equipamiento es esencialmente una gran sala de telecomunicaciones que puede albergar el marco de distribución, servidores de red, routers, switches, PBX telefónico, protección secundaria de voltaje, receptores satelitales, moduladores y equipos de Internet de alta velocidad, entre otros.

Los aspectos de diseño de la sala de equipamiento se describen en los estándares TIA/EIA- 569-A.En edificios grandes, la sala de equipamiento puede alimentar una o más salas de telecomunicaciones (TR) distribuidas en todo el edificio. Las TR albergan el equipo del sistema de cableado de telecomunicaciones para un área particular de la LAN, como por ejemplo, un piso o parte de un piso.

Los routers, hubs y switches de departamentos y grupos de trabajo se encuentran comúnmente en la TR.

[92] PEREZ, Diego. Cableado estructurado. Disponible en internet: http://cableadoestructuradodiego.blogspot.com/2011/07/reglas-para-cableado-estructuradode.html. Consultado marzo 2014

El switch de cableado y un panel de conexión de una TR pueden estar montados contra una pared con una consola de pared con bisagra, un gabinete para equipamiento completo, o un bastidor de distribución.

La consola de pared con bisagra debe ser colocada sobre un panel de madera terciada que cubra la superficie de pared subyacente. La bisagra permite que la unidad pueda girar hacia afuera de modo que los técnicos tengan fácil acceso a la parte posterior de la pared. Es importante dejar 48 cm (19 pulgadas) para que el panel se pueda separar de la pared.

El bastidor de distribución debe tener un mínimo de 1 metro (3 pies) de espacio libre para poder trabajar en la parte delantera y trasera del bastidor. Para montar el bastidor de distribución, se utiliza una placa de piso de 55,9 cm (22 pulgadas). La placa de piso brinda estabilidad y determina la distancia mínima para la posición final del bastidor de distribución.

Un gabinete para equipamiento completo requiere por lo menos 76,2 cm (30 pulgadas) de espacio libre delante de la puerta para que ésta se pueda abrir. Los gabinetes para equipamiento tienen por lo general 1,8 m (5,9 pies) de alto, 0,74 m (2,4 pies) de ancho y 0,66 m (2.16 pies) de profundidad.

Cuando coloque el equipamiento dentro de los bastidores de equipos, tenga en cuenta si el equipo utiliza electricidad o no.

Otras consideraciones a tener en cuenta son el tendido y administración de los cables y la facilidad de uso. Por ejemplo, un panel de conexión no debe colocarse en la parte de arriba de un bastidor si se van a realizar modificaciones significativas después de la instalación. Los equipos pesados como switches y servidores deben ser colocados cerca de la base del bastidor por razones de estabilidad.

La escalabilidad que permite el crecimiento futuro es otro aspecto a tener en cuenta en la configuración del equipamiento.

La configuración inicial debe incluir espacio adicional en el bastidor para así poder agregar otros paneles de conexión o espacio adicional en el piso para instalar bastidores adicionales en el futuro.

La instalación adecuada de bastidores de equipos y paneles de conexión en la TR permitirá, en el futuro, realizar fácilmente modificaciones a la instalación del cableado.

1.10.6. Áreas de trabajo. El área de trabajo es un término que se usa para describir el área que obtiene los servicios de una determinada sala de telecomunicaciones. El tamaño y la calidad de áreas de trabajo se pueden planificar con un plano de piso aproximado y una brújula.

Un área de trabajo es el área a la que una TR en particular presta servicios. Esta área de trabajo por lo general ocupa un piso o una parte de un piso de un edificio, como se ve en la figura.

Figura 16. Área de trabajo

Fuente: XDEXTECNOLOGIA. Cableado estructurado. Disponible en internet: blog2009/06/cableado-estructurado.html://xdextecnologia.blogspot.com/ Consultado marzo 2014.

El área de trabajo es un término que se usa para describir el área que obtiene los servicios de una determinada sala de telecomunicaciones. El tamaño y la calidad de áreas de trabajo se pueden planificar con un plano de piso aproximado y una brújula.

Un área de trabajo es el área a la que una TR en particular presta servicios. Esta área de trabajo por lo general ocupa un piso o una parte de un piso de un edificio, como se ve en la figura.

La distancia máxima de cable desde el punto de terminación en la TR hasta la terminación en la toma del área de trabajo no puede superar los 90 metros (295 pies).

La distancia de cableado horizontal máxima de 90 metros se denomina enlace permanente.
Cada área de trabajo debe tener por lo menos dos cables uno para datos y otro para voz.

Como se mencionó anteriormente, se debe tener en cuenta la reserva de espacio para otros servicios y futuras expansiones.

Debido a que la mayoría de los cables no pueden extenderse sobre el suelo, por lo general éstos se colocan en dispositivos de administración de cables tales como bandejas, canastos, escaleras y canaletas. Muchos de estos dispositivos seguirán los recorridos de los cables en las áreas sobre techos suspendidos. Se debe multiplicar la altura del techo por dos y se resta el resultado al radio máximo del área de trabajo para permitir el cableado desde y hacia el dispositivo de administración de cables.

La ANSI/TIA/EIA-568-B establece que puede haber 5 m (16,4 pies) de cable de conexión para interconectar los paneles de conexión del equipamiento, y 5 m (16,4 pies) de cable desde el punto de terminación del cableado en la pared hasta el teléfono o el computador. Este máximo adicional de 10 metros (33 pies) de cables de conexión agregados al enlace permanente se denomina canal horizontal. La distancia máxima para un canal es de 100 metros (328 pies): el máximo enlace permanente, de 90 metros (295 pies) más 10 metros (33 pies) como máximo de cable de conexión.

Existen otros factores que pueden disminuir el radio del área de trabajo. Por ejemplo, es posible que las vías de cable propuestas no lleven directamente al destino. La ubicación de los equipos de calefacción, ventilación y aire acondicionado, los transformadores y el equipo de iluminación pueden determinar tendidos factibles que sean más largos.

Después de tomar todos los factores en consideración, el radio máximo de 100 m (328 pies) puede estar más cercano a los 60 m (197 pies). Por razones de diseño, en general se usa un radio de área de trabajo de 50 m (164 pies).

1.10.7. Tipos de cable de conexión[93]

Cable de conexión UTP

Los cables de conexión vienen en varios esquemas de cableado. El cable de conexión directa es el más común de los cables de conexión. Tiene el mismo

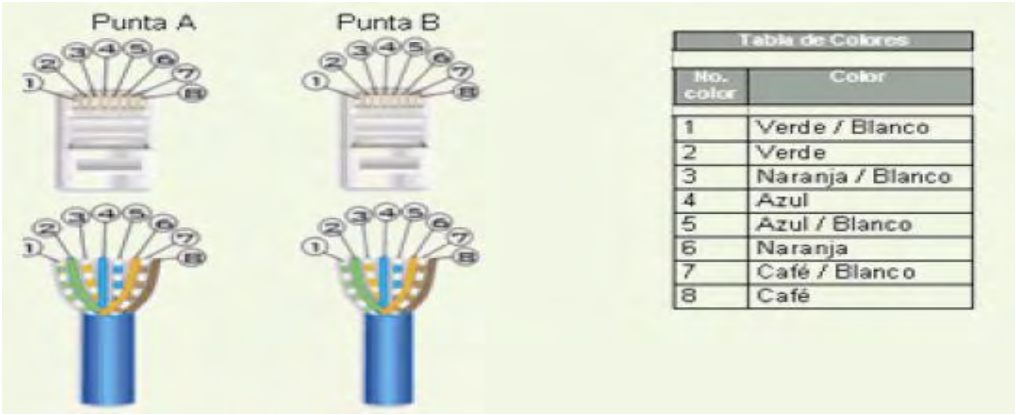
[93] XDEXTECNOLOGIA. Cableado estructurado. Disponible en internet: blog2009/06/cableado-estructurado.htmlxdextecnologia.blogspot.com/ Consultado marzo 2014.

esquema de cableado en los dos extremos del cable. Por lo tanto, el pin de un extremo se conecta al número de pin correspondiente en el otro extremo.

Estos tipos de cables se usan para conectar los PC a la red, al hub o al switch. Cuando se conecta un dispositivo de comunicaciones como un hub o switch a un hub o switch adyacente, por lo general se utiliza un cable de interconexión cruzada. Los cables de interconexión cruzada utilizan el plan de cableado T568-A en un extremo y el T568-B en el otro.

En el interior del cable categoría 5 se encuentran 4 pares de hilos, este tipo de cables se encuentran identificados por colores que porta cada una de las puntas de cobre, cada color tiene un número de identificación y por lo tanto se crean configuraciones dependiendo del orden de números que tenga cada color. Esta configuración también es llamada Uno a Uno ya que los números de los colores son consecutivos, del 1 al 8. Con esto decimos que el orden que tenga la punta A del cable debe ser idéntica a la punta B.

Figura 17. Configuración uno a uno



Fuente: TELCOPLUSEC .Esquema de colores estándar para cables UTP cat 5. Disponible en internet: http://telcoplusec.blogspot.com/2011/10/esquema-de-colores-estandar-para-cables.html Consultado marzo 2014.

1.10.8 Administración de cables.[94]Los dispositivos de administración de cables son utilizados para tender cables a lo largo de un trayecto ordenado e impecable y para garantizar que se mantenga un radio mínimo de acodamiento. La administración de cables también simplifica el agregado de cables y las modificaciones al sistema de cableado.

[94]XDEXTECNOLOGIA. Cableado estructurado. Disponible en internet: blog2009/06/cableado-estructurado.htmlxdextecnologia.blogspot.com/ Consultado marzo 2014.

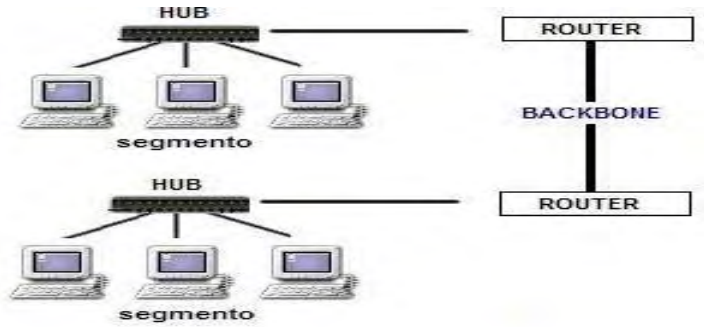
Hay muchas opciones para la administración de cables dentro de la TR. Los canastos de cables se pueden utilizar para instalaciones fáciles y livianas. Los bastidores en escalera se usan con frecuencia para sostener grandes cargas de grupos de cables. Se pueden utilizar distintos tipos de conductos para tender los cables dentro de las paredes, techos, pisos o para protegerlos de las condiciones externas. Los sistemas de administración de cables se utilizan de forma vertical y horizontal en bastidores de telecomunicaciones para distribuir los cables de forma impecable.

1.10.9 MC, IC, HC.[95]La TR primaria se llama conexión cruzada principal (MC) La MC es el centro de la red.

Es allí donde se origina todo el cableado y donde se encuentra la mayor parte del equipamiento. La conexión cruzada intermedia (IC) se conecta a la MC y puede albergar el equipamiento de un edificio en el campus. La conexión cruzada horizontal (HC) brinda la conexión cruzada entre los cables backbone y horizontales en un solo piso del edificio.

1.10.10. Cableado backbone[96]

Figura 18. Cableado backbone



Fuente: XDEXTECNOLOGIA. Tecnología de internet Backbone. Disponible en internet: blog2009/06/cableado-estructurado.htmlxdextecnologia.blogspot.com/ Consultado marzo 2014.

Cualquier cableado instalado entre la MC y otra TR se conoce como cableado backbone los estándares establecen con claridad la diferencia entre el cableado horizontal y backbone. El cableado backbone también se denomina cableado

[95] Ibíd., Consultado marzo 2014.
[96]Unitel. Normas sobre el cableado estructurado. Disponible en internet: http://unitel-tc.com/normas-sobre-cableado-estructurado/ Consultado marzo 2014

vertical. Está formado por cables backbone, conexiones cruzadas principales e intermedias, terminaciones mecánicas y cables de conexión o jumpers usados para conexiones cruzadas de backbone a backbone.

El cableado de backbone incluye lo siguiente:

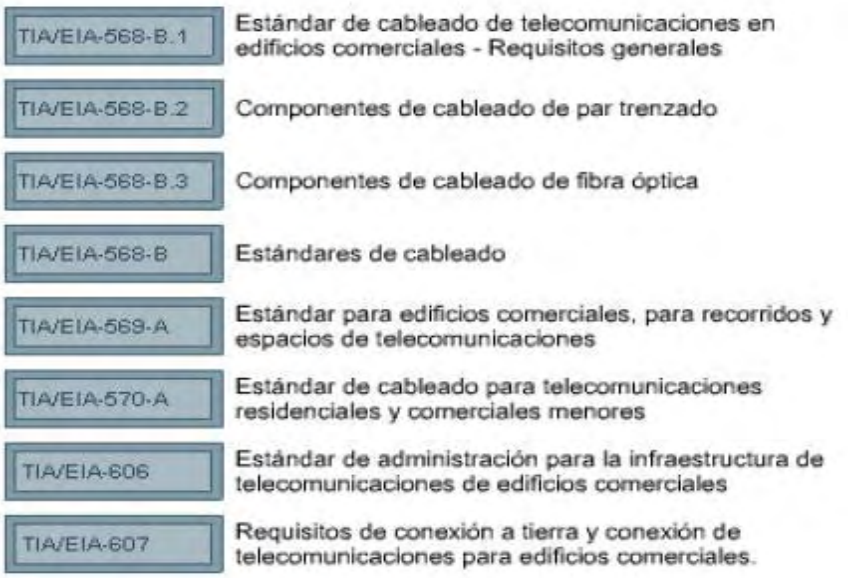
- TR en el mismo piso, MC a IC e IC a HC.
- Conexiones verticales o conductos verticales entre TR en distintos pisos, tales como cableados MC a IC.
- Cables entre las TR y los puntos de demarcación.
- Cables entre edificios, o cables dentro del mismo edificio, en un campus compuesto por varios edificios.

La distancia máxima de los tendidos de cable depende del tipo de cable instalado. Para el cableado backbone, el uso que se le dará al cableado también puede afectar la distancia máxima. Por ejemplo, si un cable de fibra óptica monomodo se utiliza para conectar la HC a la MC, entonces la distancia máxima de tendido de cableado backbone será de 3000 m (9842,5 pies).

Algunas veces la distancia máxima de 3000 m (9842,5 pies) se debe dividir en dos secciones. Por ejemplo, en caso de que el cableado backbone conecte la HC a la IC y la IC a la MC. Cuando esto sucede, la distancia máxima de tendido de cableado backbone entre la HC y la IC es de 300 m (984 pies). La distancia máxima de tendido de cableado backbone entre la IC y la MC es de 2700 m (8858 pies).

1.10.11. Estándares TIA/EIA. La asociación de la industria de las telecomunicaciones (TIA) y la asociación de industrias de electrónica (EIA) son asociaciones industriales que desarrollan y publican una serie de estándares sobre el cableado estructurado para voz y datos para las LAN. La figura muestra estos estándares.

Figura 19. Estándar TIA/EIA para cableado estructurado



Fuente: UNITEL. Normas sobre el cableado estructurado. Disponible en internet: http://unitel-tc.com/normas-sobre-cableado-estructurado/ Consultado marzo 2014

Tanto la TIA como la EIA están acreditadas por el Instituto Nacional Americano de Normalización (ANSI) para desarrollar estándares voluntarios para la industria de las telecomunicaciones. Muchos de los estándares están clasificados ANSI/TIA/EIA. Los distintos comités y subcomités de TIA/EIA desarrollan estándares para fibra óptica, equipo terminal del usuario, equipo de red, comunicaciones inalámbricas y satelitales.

Estándares TIA/EIA. Aunque hay muchos estándares y suplementos, los que se enumeran en la figura de arriba, son los que los instaladores de cableado utilizan con más frecuencia.

TIA/EIA-568-A: Este antiguo estándar para cableado de telecomunicaciones en edificios comerciales especificaba los requisitos mínimos de cableado para telecomunicaciones, la topología recomendada y los límites de distancia, las especificaciones sobre el rendimiento de los aparatos de conexión y medios, y los conectores y asignaciones de pin.

TIA/EIA-568-B: El actual estándar de cableado especifica los requisitos sobre componentes y transmisión para los medios de telecomunicaciones. El estándar TIA/EIA-568-B se divide en tres secciones diferentes: 568-B.1, 568-B.2 y 568-B.3.

TIA/EIA-568-B.1 especifica un sistema genérico de cableado para telecomunicaciones para edificios comerciales que admite un entorno de múltiple proveedores y productos.

TIA/EIA-568-B.1.1 es una enmienda que se aplica al radio de curvatura del cable de conexión UTP de 4 pares y par trenzado apantallado (ScTP) de 4 pares.

TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas y los procedimientos de medición necesarios para la verificación del cableado de par trenzado.

TIA/EIA-568-B.2.1 es una enmienda que especifica los requisitos para el cableado de Categoría 6.

TIA/EIA-568-B.3 especifica los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica.

TIA/EIA-569-A: El estándar para recorridos y espacios de telecomunicaciones en edificios comerciales especifica las prácticas de diseño y construcción dentro de los edificios y entre los mismos, que admiten equipos y medios de telecomunicaciones.

TIA/EIA-606-A: El Estándar de administración para la infraestructura de telecomunicaciones de edificios comerciales incluye estándares para la rotulación del cableado. Los estándares especifican que cada unidad de terminación de hardware debe tener una identificación exclusiva. También describe los requisitos de registro y mantenimiento de la documentación para la administración de la red.

TIA/EIA-607-A: Los estándares sobre requisitos de conexión a tierra y conexión de telecomunicaciones para edificios comerciales admiten un entorno de varios proveedores y productos diferentes, así como las prácticas de conexión a tierra para varios sistemas que pueden instalarse en las instalaciones del cliente.

El estándar especifica los puntos exactos de interfaz entre los sistemas de conexión a tierra y la configuración de la conexión a tierra para los equipos de telecomunicaciones. El estándar también especifica las configuraciones de la conexión a tierra y de las conexiones necesarias para el funcionamiento de estos equipos.

1.11 TIPOS DE PRUEBAS DE AUDITORÍA INFORMATICA[97]

Pruebas de penetración (pentesting) es el proceso utilizado para realizar una evaluación o auditoría de seguridad de un alto nivel. Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos que se siguen e implementan, durante la realización de cualquier programa de auditoría en seguridad de la información. Una metodología de pruebas de penetración define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas con cuidado para poder evaluar correctamente los sistemas de seguridad.

1.11.1 Tipos de pruebas de penetración:[98]Existen diferentes tipos de pruebas de penetración, las más comunes y aceptadas son las pruebas de penetración de caja negra (Black-Box), las pruebas de penetración de caja blanca (White-Box) y las pruebas de penetración de caja gris (Grey-Box).

• **Prueba de caja negra.** No se tienen ningún tipo de conocimiento anticipado sobre la red de la organización. Un ejemplo de este escenario, es cuando se realiza una prueba externa a nivel web, y está es realizada solo con el detalle de una URL o dirección IP, el cual es proporcionado al equipo de pruebas. Esto simula el rol de intentar irrumpir en el sitio web o red de la organización. Así mismo simula un ataque externo realizado por un atacante malicioso.

• **Prueba de caja blanca.** El equipo de pruebas cuenta con acceso para evaluar las redes y ha sido dotado de diagramas de la red y detalles de hardware, sistemas operativos, aplicaciones, entre otra información, antes de que la prueba sea realizada. Esto no iguala a una prueba sin conocimiento pero puede acelerar el proceso en gran medida y obtener resultados más precisos. La cantidad de conocimiento previo conduce a realizar las pruebas a sistemas operativos específicos, aplicaciones y dispositivos de red que residen en la red en lugar de invertir tiempo enumerando lo que podría posiblemente estar en la red. Este tipo de prueba equipara una situación donde el atacante puede tener conocimiento completo de la red interna.

• **Prueba de caja gris.** El equipo de pruebas simula un ataque que puede ser realizado por un miembro de la organización inconforme o descontento. El equipo

[97] KALI LINUX. Disponible en internet: http://docs.kali.org/pdf/kali-book-en.pdf Consultado marzo 2014.
[98] Ibíd., Consultado marzo 2014.

de pruebas debe ser dotado con los privilegios adecuados a nivel de usuario y una cuenta de usuario, además de permitirle acceso a la red interna.

1.12 SOFTWARE PARA PRUEBAS EN SEGURIDAD DE REDES

Kali Linux.[99]Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar auditorías de seguridad y pruebas de penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

La selección de kali Linux se debe a su característica principal que es la inclusión de más de 300 herramientas de intrusión, monitoreo y escaneo de software de redes.

Características de Kali Linux[100]

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el VCS.

- Más de 300 herramientas de pruebas de penetración
- Es libre y siempre lo será
- ÁrbolGit Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro
- Paquetes y repositorios firmados con GPG
- Varios lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF

[99] KALI LINUX. Seguridad ofensiva limitada. Documentación Oficial kali Linux. Disponible en internet: http://www.kali.org/official-documentation/. Consultado: 20 de Enero de 2014.
[100] Ibíd., Consultado marzo 2014.

Figura 20. KALI LINUX

Fuente: KALI LINUX. Disponible en internet: http://docs.kali.org/pdf/kali-book-en.pdf consultado marzo 2014.

1.13 EVALUACIÓN DE VULNERABILIDADES

Una evaluación de vulnerabilidades es el proceso de evaluar los controles de seguridad interna y externa para identificar las amenazas que planteen una seria exposición para los activos de la organización.

La evaluación de vulnerabilidades proporciona una amplia visión de las fallas existentes en los sistemas sin medir el impacto real de estas fallas para los sistemas en consideración.

1.13.1 Captura de datos. En esta fase se intenta recolectar toda la información que sea posible sobre el objetivo, por ejemplo posibles nombres de usuarios, direcciones IP, servidores de nombre, y otra información. Durante esta fase cada pieza de información obtenida es importante y no debe ser subestimada.

El proceso donde se captura la información puede ser dividido de dos maneras. La captura de información activa y la captura de información pasiva. En el primera forma, se recolecta información enviando tráfico a la red objetivo, como por ejemplo hacer ping ICMP, y escaneos de puertos TCP/UDP. Para el segundo caso, se obtiene información sobre la red objetivo utilizando servicios o fuentes de terceros, como por ejemplo Google, Bing, o redes sociales.

Software utilizado para la captura de datos Nmap.

Nmap[101]: es una herramienta (GNU) libre multiplataforma, para la exploración de redes y, de forma idónea, la realización de auditorías de seguridad. Se trata de un software desarrollado para escanear redes completas, aunque funciona sin problemas contra un servidor concreto. Nmap rastrea los puertos de la máquina o máquinas en cuestión y establece si un puerto está abierto, cerrado o protegido por un cortafuego. Así, es capaz de identificar máquinas dentro de una red, determinar qué servicios utiliza dicha máquina, definir cuál es su sistema operativo e incluso devolver cierta información sobre el hardware de la máquina.

1.13.2 Descubrir objetivos. Encontrar cuales son las máquinas que están disponibles en la red objetivo, pues si la máquina no está disponible, no se puede continuar con el proceso, y se debe continuar con la siguiente máquina. También se deben obtener indicios sobre el sistema operativo utilizado por la máquina objetivo. Toda esta información con el fin de continuar el proceso después de mapear las vulnerabilidades.

1.13.3 Enumerar el objetivo. La enumeración del objetivo es un proceso utilizado para encontrar y recolectar información de los puertos y servicios disponibles en el objetivo. Usualmente este proceso se realiza luego de haber descubierto el entorno objetivo mediante el escaneo para obtener los hosts en funcionamiento. Este proceso se realiza usualmente al mismo tiempo que el proceso de descubrimiento.

1.13.4 Explotar el objetivo. Luego de haber descubierto las vulnerabilidades en el host o red objetivo, es momento de intentar explotarlas. La fase de explotación algunas veces finaliza el proceso de la Prueba de Penetración, pero esto depende del contrato, pues existen situaciones donde se debe ingresar de manera más profunda en la red objetivo para expandir el ataque por toda la red y ganar los todos los privilegios posibles.

Software utilizado para la prueba de explotación del objetivo **metasploit.**

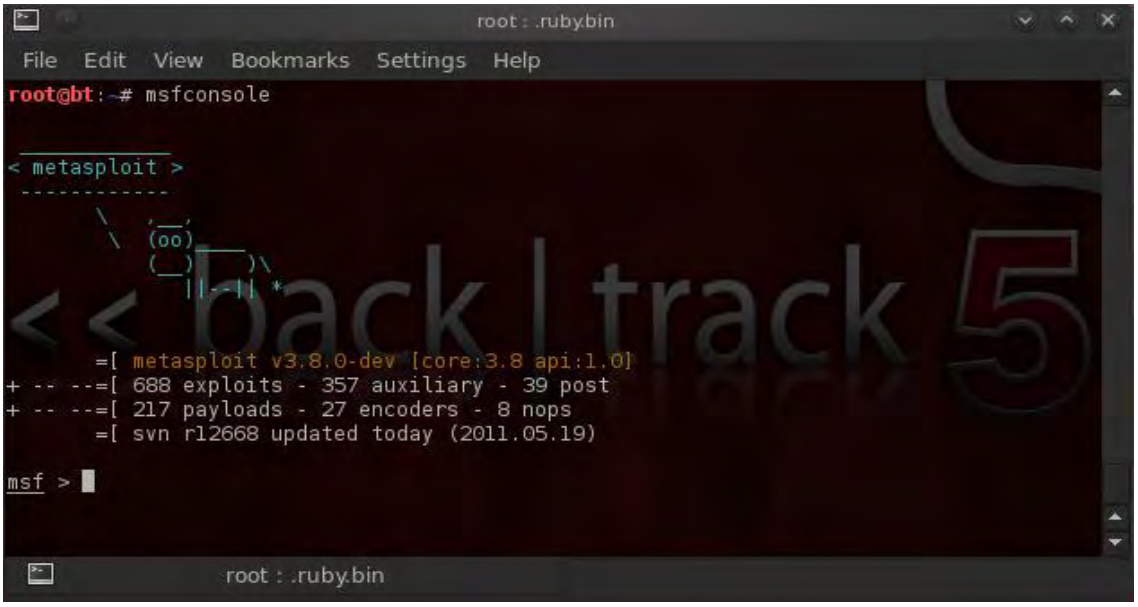
[101] DEBIANHACKERS. Nmap: Escáner de puertos. Disponible en: http://www.debianhackers.net/nmap-escaner-de-puertos, Consultado marzo 2014.

Metasploit (msf)[102]

Metasploit es una de las herramientas de auditoría más útil a libre disposición de los profesionales de la seguridad hoy en día disponible dentro del paquete de herramientas de kalilinux. **Metasploit** es un proyecto de código abierto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para sistemas de detección de intrusos.

Metasploit Framework proporciona un entorno de trabajo realmente impresionante. El MSF es mucho más que una colección de exploits, es una infraestructura que puede aprovechar y utilizar para sus necesidades personalizadas una gran cantidad de exploits guardados en una gigantesca base de datos.

Figura 21. Metasploit en kali Linux



Fuente: METASPLOIT. Tutorial básico. Disponible en internet:http://metasploited.blogspot.com. Consultado 19 Junio de 2011.

[102] AHARON Matil, COPPOLA William, Tutorial de Metasploit Framework de offensive-security, http://ns2.elhacker.net/timofonica/manuales/Manual_de_Metasploit_Unleashed.pdf. Consultado Marzo 2014.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

Pruebas sustantivas: verifican el grado de confiabilidad del SI, sistema de información del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

Pruebas de cumplimiento: verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Para la realización de estas pruebas no se utilizara software, se comprobara directamente los siguientes ítems de seguridad.

- Que los computadores tengan contraseñas de acceso
- Que se registren las actividades de los usuarios en la red.
- Que se evite la importación y exportación de datos
- Que el sistema pida el nombre de usuario y la contraseña para cada sesión:
- Que en cada sesión de usuario no acceda a ningún sistema sin autorización.
- Que las contraseñas no se han mostradas en pantalla tras digitarla.
- Que se encuentre Inhabilitado el software o hardware con acceso libre.
- Que el firewall se encuentre activo en todos los equipos de la red.
- Que el antivirus se encuentre correctamente instalado y actualizado.
- Que no existan programas instalados fuera de los establecidos por la organización.
- Que la conexión a internet este restringida, que no exista el acceso a páginas impropias que no estén permitidas por la organización.

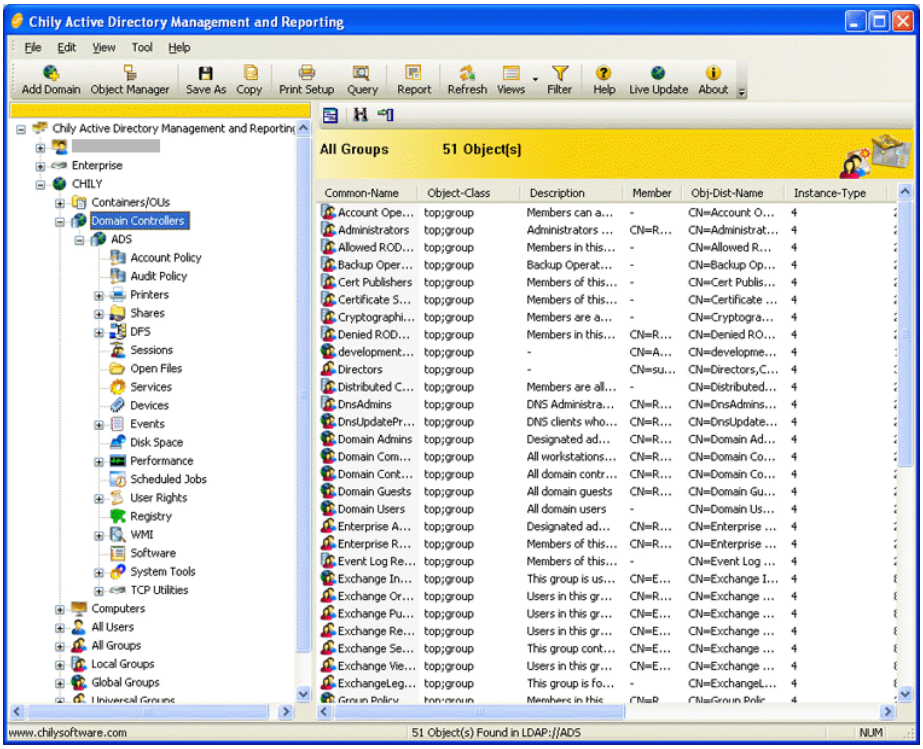
MICROSOFT ACTIVE DIRECTORY[103]: es la implementación más reciente de servicios de directorio para Windows 2000. Las cuestiones básicas relacionadas con un centro de servicios de directorio giran alrededor de la información que se puede almacenar en la base de datos, cómo se almacena, cómo se puede consultar información específica y qué se puede hacer con los resultados. Active Directory se compone del propio servicio de directorio junto con un servicio secundario que permite el acceso a la base de datos y admite las convenciones de denominación X.500.

[103] MICROSOFT SOPORTE, Introducción a ActivityDirectory. Disponible en Internet: http://support.microsoft.com/kb/196464/es. Consultado:18 de Octubre de 2012

Puede consultar el directorio con un nombre de usuario para obtener información como el número de teléfono o la dirección de correo electrónico de ese usuario. Los servicios de directorio también son lo suficientemente flexibles como para permitir la realización de consultas generalizadas (" ¿dónde están las impresoras? “) o bien " ¿cuáles son los nombres de servidores? ") Para ver una lista resumida de las impresoras o servidores disponibles.

Los servicios de directorio también ofrecen la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa. Los usuarios pueden buscar y usar recursos en la red sin conocer el nombre o la ubicación exactos del recurso. Igualmente, puede administrar toda la red con una vista lógica y unificada de la organización de la red y de sus recursos.

Figura 22. ActivityDirectory.



Fuente: FREE 64 BIT. Gestor De Active Directory. Disponible en internet: http://www.64bitprogramlar.com/tags/la-gestion-dactive-directory.

1.14 ANALISIS DE RIESGOS AUDITORÍA

1.14.1 Análisis de riesgos de la auditoría. Los procesos de auditoría y análisis de riesgos son un componente clave en la definición de seguridad de la información y seguridad informática. El principal objetivo de un análisis de riesgo y programa de auditoría es identificar los activos involucrados en la organización, sus metodologías y procesos de estimar el riesgo asociado. Un análisis de riesgo o de auditoría es un proceso que debe ser mirado desde el punto de vista de la administración de la organización y no sólo en el área de tecnologías de la información, porque su alcance es mucho más amplio.[104]El análisis de riesgo o el proceso de auditoría buscan identificar y evaluar el riesgo y recomendar medidas de mitigación para reducir el riesgo a niveles aceptables para la organización. A través de un análisis de riesgo o de auditoría, las organizaciones pueden obtener los siguientes beneficios:

• Mejoras significativas en la seguridad de sistemas de información, almacenan, procesan y transmiten la información de la organización;

• Optimización en la aplicación y los procesos de gestión;

• Mayor y mejor control sobre los activos de la empresa;

• Posibilita una mejor gestión de riesgo organizacional;

• Permite la administración de una organización de hacer mejores decisiones de inversión en seguridad de la información.

Los pasos para realizar un análisis de riesgos o auditoría son las siguientes:

1. Definición del alcance y el contexto organizacional.
2. Identificación.
3. Cálculo de las estimaciones de riesgo.
4. Riesgos.
5. Riesgo de controles comunicación y mitigación.
6. Aplicación de los controles.
7. Aceptación del riesgo.

Una forma de analizar los riesgos es mediante una matriz de riesgos.

[104] DATA RECOVER CENTER. Seguridad de la información. Disponible en internet: http://www.datarecovercenter.com/esl/Servicios/Seguridad-de-la-Informacion/Auditoría-y-Analisis-de-Riesgo. Consultado 3 de Noviembre de 2008.

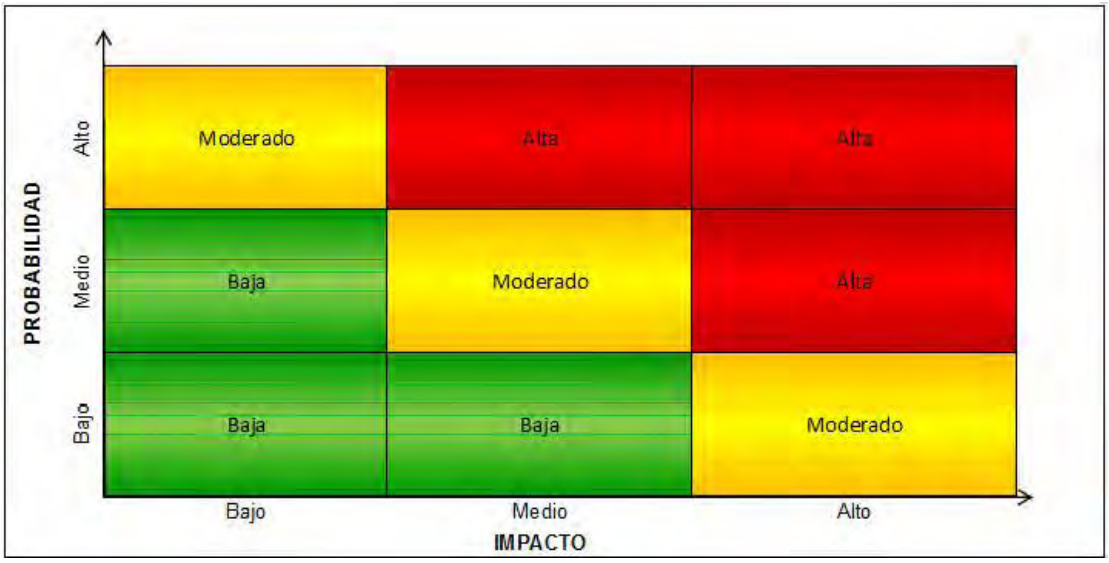
1.14.2 Matriz de probabilidad de impacto. Es una forma usual de establecer o clasificar si un riesgo es bajo, medio o alto, a través de la combinación de dos dimensiones de un riesgo: su probabilidad de que suceda y el impacto que esta genere en los objetivos de la empresa si este llegara a ocurrir.

La matriz de probabilidad e impacto, es el punto clave en clasificar los riesgos, obteniendo así:

Eje X: el impacto que el riesgo genera en los objetivos del proyecto, puede ser de impacto bajo, medio o alto.
Eje Y: la probabilidad de ocurrencia del riesgo puede ser probabilidad de ocurrencia baja, media y alta de que suceda.

La siguiente figura representa la matriz de probabilidad e Impacto.

Figura 23. Matriz de probabilidad e impacto



Fuente: RICARDO SANCHEZ, Seguridad de los sistemas de información. Disponible en internet: http://mismamente-yo.blogspot.com/2012/05/seguridad-de-los-sistemas-de.html. Consultado: 8 de mayo de 2012.

Dónde:

Riesgos bajos (verde), que quizá necesitan monitorización, planes de actuación detectivos.

Riesgos moderados (Amarillo), riesgos que necesitan investigación, planes de actuación preventivos.

Riesgos altos (Rojo), que necesitan mitigación, planes de actuación correctivos.

1.15 ESTANDARES DE AUDITORÍA

Para la realización y ejecución de una auditoría se hace necesario aplicar normas o estándares bajo los cuales las empresas deben regirse, de allí la importancia identificar los estándares internacionales que en este caso, son:

Directrices gerenciales de COBIT, desarrollado por la Information Systems Audit and Control Association (ISACA) Asociación de auditoría y control de los sistemas de información: las directrices gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información.

1.15.1 COBIT (Objetivos de Control para Tecnología de la Información y Relacionada).En una era donde hay una creciente tendencia a los negocios electrónicos, y de dependencia a la tecnología, las organizaciones tendrán que alcanzar crecientes niveles de seguridad y de control. Toda organización debe conocer su propio desempeño y medir su progreso. La metodología COBIT, proporcionan a la administración una guía programática que permita determinar el nivel correcto de control para la TI y que esta soporte los objetivos de la empresa.

COBIT, es un estándar de administración, control y auditoría de información en el mundo de los negocios, desarrollado y promovido por el instituto de gobierno de la tecnología de la información ISACA (Información System Audit and control Assosiation Inc.) asociación mundial de control de información. Se publicó por primera vez en el año de 1996 y en el año 2000 se produjo la tercera versión revisada y aumentada. COBIT es el acrónimo de control objetives for information and related technology. (Objetivos de control para la información y tecnología relacionada.)[105]

COBIT es reconocido en el mundo como un estándar generalmente aplicable y aceptado por las buenas prácticas de control y seguridad en tecnología de información (TI). Permite llenar vacios que existen entre los modelos de control de negocios y los modelos de control enfocados a los aspectos puramente técnicos de sistemas de información.

[105] LEONARDO, Camelo. Seguridad de la información en Colombia. Disponible en internet: http://seguridadinformacioncolombia.blogspot.com/2010/07/que-es-cobit.html. Consultado: 28 de Julio de 2010.

Independiente de la realidad tecnológica de cada caso en particular, COBIT determina, con el respaldo de las normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para coordinar la TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

Proporciona a gerentes, inventores, y usuarios TI un conjunto de medidas generalmente aceptadas, indicadores, procesos y las mejores prácticas para ayudar a ellos a maximizar las ventajas con el empleo de la tecnología de la información, y desarrollo de la gobernación apropiada TI y el control en una empresa.

Metodología COBIT orientada a riesgo. La realización de auditorías por procesos, al igual que las auditorías de sistemas de Información, son actividades que requieren de la precisión de conceptos y definiciones para apoyar su planeación y desarrollo. El hecho de ser relativamente jóvenes y el estar sujetas al cambio de la tecnología de información y de las telecomunicaciones, hace que la comunidad de la auditoría necesite apoyo y guías que faciliten la transición entre el “qué hacer” y el “cómo hacerlo”.

Después de evaluar los objetivos de control determinados por COBIT para mitigar dichos riesgos se efectúan las pruebas (verificaciones) necesarias y aplicables a las circunstancias, con lo cual la auditoría estará en capacidad de concluir si la empresa, el proceso o el sistema auditado está asumiendo riesgos secundarios que son aceptables o que están por encima del nivel máximo aceptable.

Esta metodología de auditoría de sistemas, se efectúa por fases y de la siguiente manera:

La fase de planeación de la auditoría, la cual define el alcance de la auditoría en un cubo o mapa de riesgos representado por tres elementos del proceso o sistema sujeto a auditoría: a) riesgos potenciales críticos, b) los subprocesos o escenarios de riesgo y c) las dependencias (de la empresa o terceras partes) que intervienen en el manejo de las operaciones.

Los pasos para determinar el alcance de la auditoría contemplan: la elaboración de tres matrices de riesgo y definir los objetivos de control COBIT, que deberán ser satisfechos con los controles establecidos en el proceso o sistema sujeto a auditoría.

Para poder identificar estos riesgos y controles, es necesario conocer el negocio a auditar, es decir tener un conocimiento exacto y profundo de los diferentes

procesos, los materiales, las normas, la organización administrativa y los responsables de cada uno de ellos. Se debe llevar un registro en memorias de auditorías como las siguientes: esquemas, diagramas de proceso, diagramas de flujo, organigramas, resúmenes normativos, conclusiones, actas, memoria de entrevista, registro fotográfico, grabaciones, etc.

Una vez se hayan identificado los riesgos se evaluaran los que tienen característica de “riesgo potencial”; para ello se aplican dos métodos de análisis y valoración de categorías de riesgos potenciales típicos, estos contienen procedimientos para medir en formas cuantitativa y cualitativa, la exposición de un proceso o sistema a categorías de riesgos típicos, utilizando los métodos DELPHY y cuestionarios con factores de riesgo.

Una vez establecido el alcance, se evalúan los controles existentes, bajo criterios novedosos para medir en formas numérica y cuantitativa la capacidad que tienen los controles establecidos en los procesos o sistemas para prevenir, detectar o corregir las amenazas o causas de riesgos críticos. La aplicación de tres criterios de evaluación conduce a determinar una escala de 5 rangos de protección.

Sobre estos elementos se proyecta la fase de ejecución de la auditoría, en la que se procederá a planear, diseñar y ejecutar las pruebas de auditoría; cuyos resultados deben analizarse a fin de generar los hallazgos o no conformidades, que forman la materia prima para generar las recomendaciones de la auditoría.

1.16 MODELO DE MADUREZ COBIT

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la

aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud.[106]

Escalas de nivel de madurez COBIT:

0. No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1. Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2. Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3. Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4. Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5. Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.[107]

[106] MAYANS, Gregorio. Modelo de madurez. Disponible en internet: http://www.network-sec.com/gobierno-TI/auditoría-CMM, Consultado: 10 de Noviembre de 2010
[107] Ibíd., Consultado: 10 de Noviembre de 2010

2. DESARROLLO DE LA AUDITORÍA

2.1 ARCHIVO PERMANENTE

Se incluye en este punto información permanente que sirve de consulta guía para la evaluación de políticas y procedimientos de la empresa, en este caso de Emssanar ESS.

2.1.1 Ambiente general de la empresa

Información general y ubicación: La empresa solidaria de salud Emssanar ESS, es una institución prestadora de servicios de salud de primer y segundo nivel de complejidad con cobertura geográfica en Nariño, Putumayo, Cauca y Valle, siendo una empresa de carácter social del Estado.

La auditoría se ejecutó en la regional Nariño, ubicada en la ciudad de Pasto. Sede principal situada en:

- Dirección: B/San Ignacio
- Teléfono: 7336030 ext. 103318
- Página web: www.emssanar.org.co
- e-mail: corporativa@emssanar.org.co

En cuanto a la relación con los entes territoriales, es excelente porque mantiene buena comunicación, de tal manera que las respuestas frente a la problemática que se genera dentro del aseguramiento, han sido concertadas. Y, con los hospitales, tiene una relación de confianza, a pesar de que muchas veces el flujo de recursos no es el ideal. Sin embargo, ellos permiten que las negociaciones sean las más adecuadas y que participe también en algunas de sus actividades en salud, sociales o deportivas. Emssanar es una empresa promotora de salud del régimen subsidiado que integra a más de 1.200.000 mil afiliados en el sur occidente colombiano; cuenta con una red de 270IPS en los departamentos de Nariño, Putumayo, Cauca y Valle, integradas a través de un innovador centro de contactos que permite mejorar la atención al usuario.

Historia de Emssanar ESS[108]

Desde una Empresa Solidaria de Salud a un grupo empresarial y comunitario en el sur occidente Colombiano.

1990, Colombia en el sistema nacional de salud, un escenario donde se encontraban criticas alusivas a: “el sistema actual convierte a los individuos y comunidades en sujetos pasivos de sus actividades y no permite que esas comunidades ejerzan el derecho a cuidar de su salud y a recibir y exigir del sistema servicios oportunos y de buena calidad”.

Frente a este escenario el gobierno Nacional propuso el programa de empresas solidarias de salud como respuesta a las necesidades del sector, como lo describe Iván Jaramillo “Las Empresas Solidarias de Salud se crearon antes de la ley 100 de 1993 y según el Ministro de Salud, Juan Luis Londoño, la experiencia que sirvió de base fue la de los hogares comunitarios del ICBF, los cuales con el mismo dinero lograron multiplicar más la cobertura”.

Así EMSSANAR E.S.S, nace en la segunda fase del programa denominada gestión empresarial, donde se identificaron líderes que representaban a grupos familiares de base, cada uno constituido por veinte grupos en el que el representante o delegado se integraba a procesos organizativos comunitarios para conformar las Empresas solidarias de salud, en función, principalmente de los siguientes propósitos: El adquirir servicios de salud con la financiación del subsidio directo otorgado por el Estado y la articulación con el sistema general de seguridad social en salud, que inicia la labor de administración de los recursos con un enfoque de riesgo.

El proceso de fortalecimiento y participación, que como resultado quedó la organización y constitución de las Empresas Solidarias de Salud, el cuidado del medio ambiente, donde se conformaron los grupos extramurales de apoyo a las familias en su territorio y realidad; bajo esta idea se desarrollaron diferentes experiencias en Colombia, donde comunidades organizadas accedían a servicios de salud básica, mediante un paquete financiado con los aportes del Ministerio de Salud, los departamentos, los municipios y la población vinculada a dichos procesos.

De esta manera Emssanar se ha posicionado como organización comunitaria y empresa solidaria en la región, asegurando la salud de más de un millón de afiliados en ochenta y nueve municipios de los departamentos de: Valle, Cauca,

[108] EMSSANAR E.S.S. Código de buen gobierno y ética de Emssanar, Colombia, 1991. 18.p. Disponible en internet:http://www.emssanar.org.co/contenidos/EPSEmssanar/RENDICION_DE_CUENTAS/CODIGO_DE_BUEN_GOBIERNO_Y_ETICA.pdf.

Nariño y Putumayo, con redes de IPS y de farmacias que actúan en diferentes municipios de la región, contando cuatro mil quinientos asociados y setecientos trabajadores en sus empresas.

2.1.2 Misión.[109]Emssanar E.S.S es una organización empresarial de la economía solidaria, con proyección nacional e internacional, que desde el sur occidente colombiano presta servicios en las áreas de: salud, educación técnica, comercialización de alimentos, asistencia técnica socio-empresarial y micro crédito. A través de tecnologías flexibles, el eficiente manejo de los recursos y un talento humano competente y motivado, comprometido con el liderazgo, la solidaridad, la responsabilidad social y en la contribución al mejoramiento de las condiciones de vida de su comunidad para el desarrollo del país.

2.1.3 Visión.[110]Emssanar E.S.S en el 2019 será un grupo empresarial de la economía solidaria reconocido por su aporte en la generación de capital social y desarrollo sostenible del país.

2.1.4 Valores.[111] Liderazgo, solidaridad, responsabilidad social.

2.1.5 Servicios que ofrece. Emssanar como grupo empresarial, es una organización comunitaria que hace parte del sector de la economía solidaria, se encuentra al servicio de la comunidad y contribuye a la construcción de la región sur occidental colombiana a través del desarrollo empresarial y la redistribución social.

Conformada por diferentes servicios como son:

Emssanar EPS-S: Empresa Promotora de Salud del régimen subsidiado que integra más de un millón de afiliados en el sur occidente colombiano, cuenta con una red de 270 IPS en los departamentos de: Nariño, Putumayo, Cauca y Valle, integradas a través de un innovador centro de contactos que permite mejorar la atención al usuario.

---

[109] COOPERATIVA EMSSANAR I.P.S. Portafolio de servicios. Disponible en internet:http://www.emssanar.org.co/contenidos/cooemssanarips/portafolio/PORTAFOLIO_IPS.pdf. Consultado: 10 de Noviembre de 2014.

[110] Ibíd., .2014.

[111] COOPERATIVA EMSSANAR I.P.S. Portafolio de servicios. Disponible en internet:http://www.emssanar.org.co/contenidos/cooemssanarips/portafolio/PORTAFOLIO_IPS.pdf. Consultado: 10 de Noviembre de 2014.

CooEmssanar IPS: presta servicios de salud bajo el enfoque de mejoramiento continuo y con énfasis en el paciente y su familia, garantizando la calidad en la atención caracterizada por la accesibilidad, oportunidad, seguridad, pertinencia y continuidad, mediante un modelo de salud preventivo y seguro. La política de calidad y seguridad define que el paciente recibirá cuidados en salud sin ser lesionado durante el proceso de atención de las personas que prestan los servicios.

CooEmssanar SF: presta servicios dedicados al suministro de medicamentos, material médico-quirúrgico, productos cosméticos y de uso personal, en el sur occidente colombiano, garantizando su calidad son responsabilidad, actitud de servicio y liderazgo, mediante un talento humano calificado y acreditado, generando confianza en nuestros clientes.

Fundación Emssanar: creada como organización solidaria de desarrollo, tiene diferentes líneas de acción: acompañamiento socio empresarial, educación, investigación y comercialización social de alimentos; en cuyo marco se han ejecutado proyectos que posibilitan la proyección de la organización en la atención a población pobre y vulnerable de los departamentos de Nariño, Putumayo, Cauca y Valle.

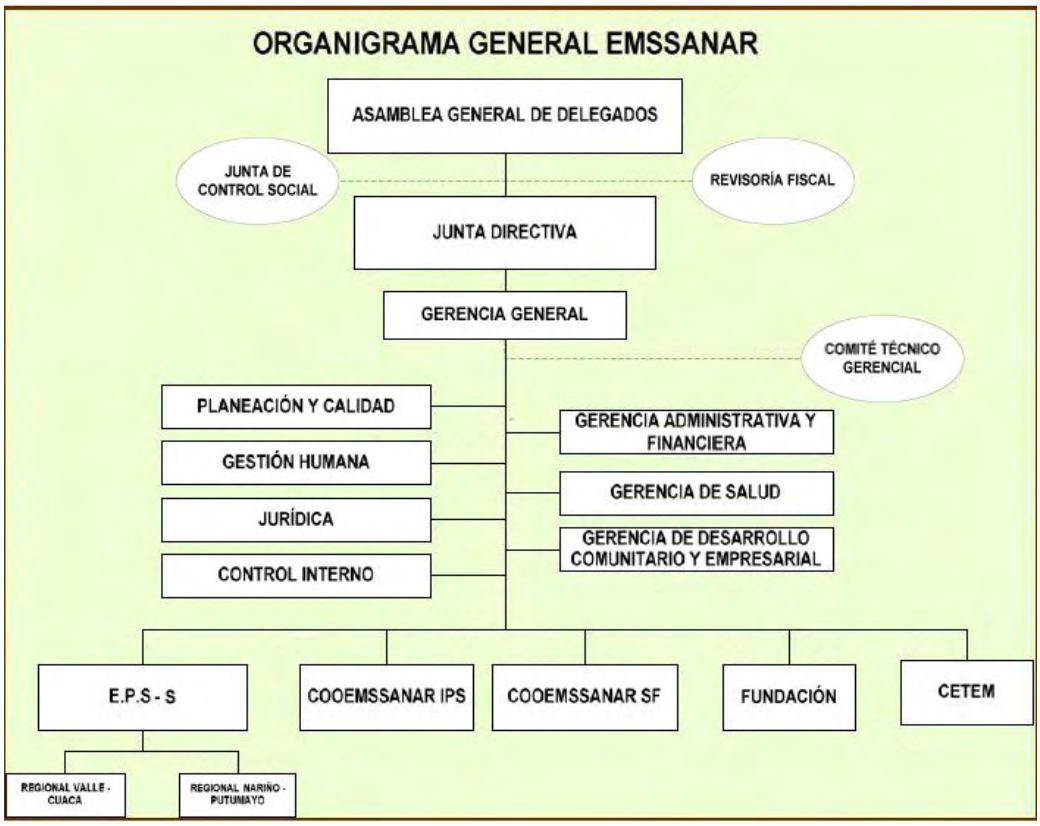
Fundación de servicios educativos de Emssanar (CETEM): entidad sin ánimo de lucro que busca contribuir al mejoramiento de las condiciones y calidad de vida de la población beneficiaria con programas, planes y proyectos de formación, capacitación y educación.[112]

[112] COOPERATIVA EMSSANAR I.P.S. Portafolio de servicios. Disponible en internet:http://www.emssanar.org.co/contenidos/cooemssanarips/portafolio/PORTAFOLIO_IPS.pdf. Consultado: 10 de Noviembre de 2014.

2.1.6 Organigrama general de Emssanar.

Figura 24. Organigrama general Emssanar

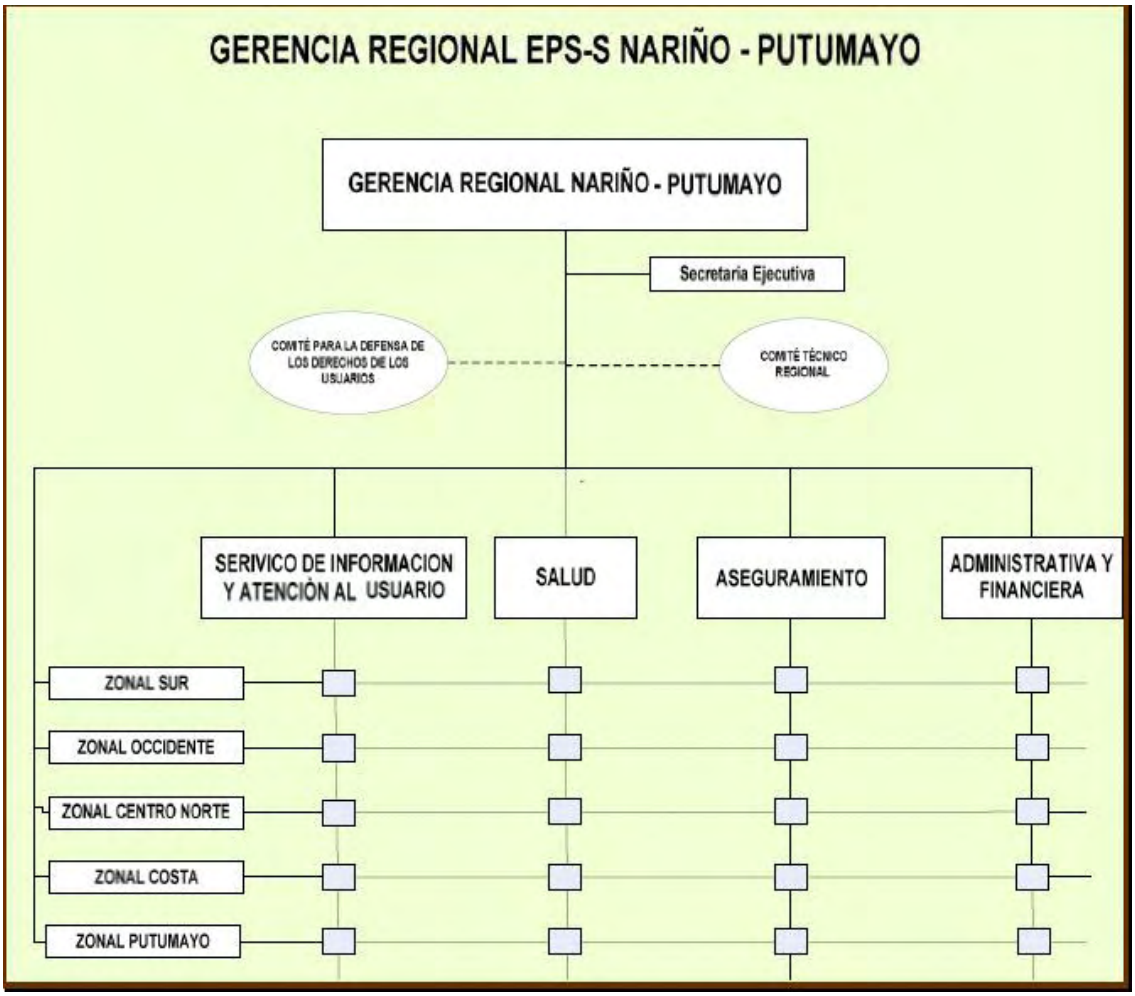
Aprobación**:** según resolución de gerencia general 009 De 2.009.



Fuente: Empresa Solidaria de Salud Emssanar E.S.S.

Organigrama gerencial EPS-S Nariño-Putumayo: aprobación: según resolución de gerencia general 009 De 2.009.

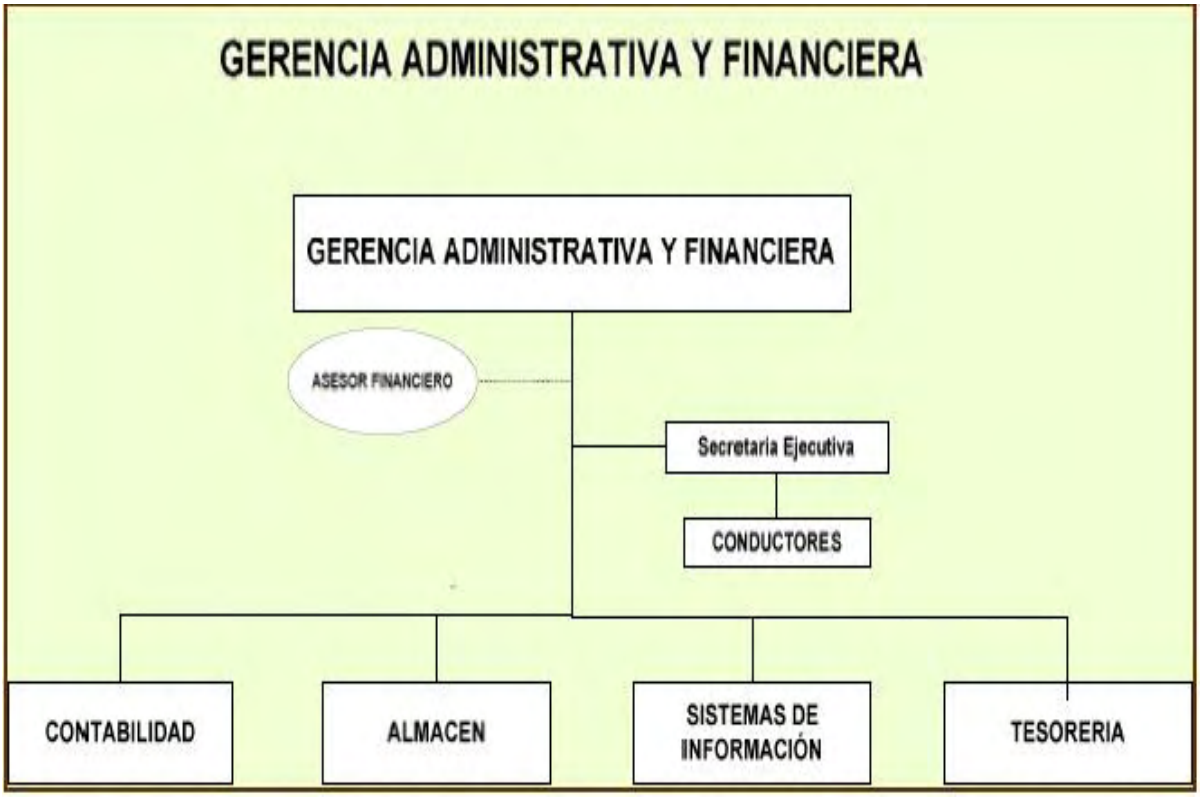
Figura 25. Gerencia regional Nariño- Putumayo



Fuente: Empresa Solidaria de Salud Emssanar E.S.S.

Organigrama gerencia administrativa y financiera: según resolución de gerencia general 0011 de 2.009

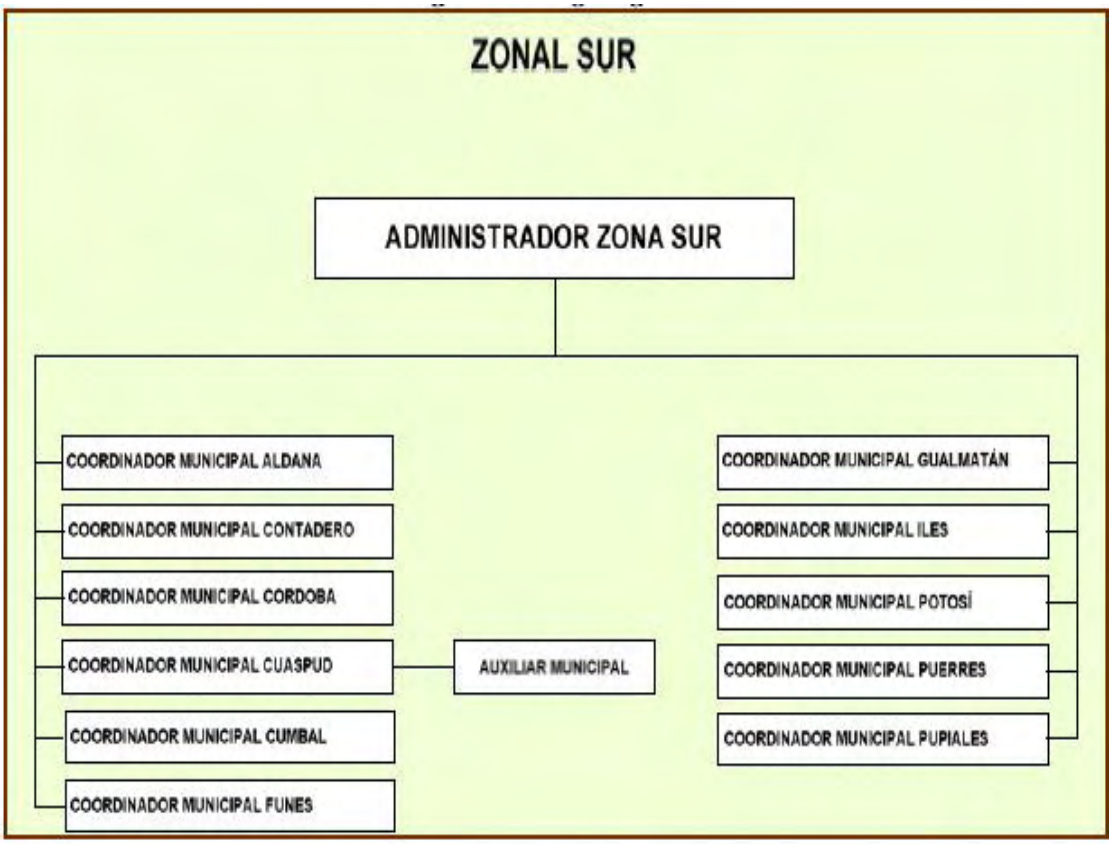
Figura 26. Gerencia administrativa y financiera



Fuente: Empresa Solidaria de Salud Emssanar E.S.S.

Organigrama zonal sur: el municipio de Ipiales, tomado como central de los municipios aledaños, trabaja como zonal de 11 municipios ubicados al sur de Nariño (Figura 60), así:

Figura 27. Zonal Sur



Fuente: Empresa Solidaria de Salud Emssanar E.S.S.

Organigrama del área de sistemas. Aprobación**:** según resolución de gerencia general009 de 2009

Figura 28. Área de sistemas

Fuente: Empresa Solidaria de Salud Emssanar E.S.S.

2.1.7 Área de sistemas. El área de sistemas de Emssanar es un organismo que depende de la gerencia administrativa y financiera, constituido como un espacio encargado de la administración de los sistemas y soporte centralizados, el objetivo de esta área es la organización, control y automatización de la información corporativa.

Dentro de las actividades que se desarrollan en el área de sistemas corresponde a la administración de los sistemas operativos con el objetivo de garantizar la continuidad del funcionamiento de las máquinas y del software al máximo rendimiento y facilitar su utilización a todas las dependencias de la empresa en general. Dentro de lo que concierne a las funciones de la coordinación de sistemas y comunicaciones lo que tiene que ver con el diseño, la implementación y el mantenimiento de los elementos que constituyen la infraestructura informática de la empresa, entendiendo como tal los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la empresa en general los servicios informáticos necesarios para desarrollar sus actividades

Dentro de las actividades se desarrollan tareas que sirven de control para el funcionamiento de los sistemas, están:

- Mantenimiento de los equipos, detección y resolución de averías.
- Sintonía del sistema operativo y optimización del rendimiento.
- Gestión de cuentas de usuario y asignación de recursos a las mismas.
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.

2.1.8 Auditoría de comunicaciones

Consideraciones:

- **Gestión de red: los equipos y su conectividad.**

En principio se definirá a lo que hace referencia gestión de red, para posteriormente dar a conocer cómo se gestiona la red en la Empresa de solidaria de Salud Emssanar E.S.S.

La gestión de red se refiere a todo el conjunto de actividades dedicadas al control y vigilancia de los recursos de la red, esto se logra empleando una variedad de herramientas, aplicaciones o dispositivos. [113]

Cuyo principal objetivo es garantizar un buen nivel de servicio en los recursos gestionados.

Las funciones de gestión de red se basan en dos procedimientos:

Monitoreo. El monitoreo es un proceso pasivo, el mismo que se encarga de observar y obtener datos acerca del estado y del comportamiento de configuración de los recursos de la red, analizando las seguridades, fallos en el sistema de la red, con la ayuda de herramientas o equipos.

Control. A diferencia del monitoreo, el control es un proceso activo, el cual se basa en obtener información del monitoreo y actuar sobre el comportamiento de

[113]ARCE Norma y TACURI Andrés, Auditoría física y lógica a las redes de comunicaciones de computadores de la fábrica pasamanería s.a. Cuenca Ecuador, 2010, 364 p. Trabajo de grado (Ing. De Sistemas).Universidad Politécnica Salesiana. Facultad De Ingenierías. Departamento de Sistemas.

los recursos de la red administrada. Además abarca la configuración y seguridad de la red.

La gestión de la red en la Empresa de Salud Emssanar E.S.S, está administrada de la siguiente manera:

Se centraliza en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados a la red de la fábrica.

Dispone de dos tipos de recursos:

Recursos humanos. El Personal encargado del correcto funcionamiento del centro de gestión de red, corresponde al, Ing. Diego Bastidas.

- **Herramientas de apoyo**. Las herramientas que facilitan las tareas de gestión a los operadores humanos, corresponde a las siguientes.

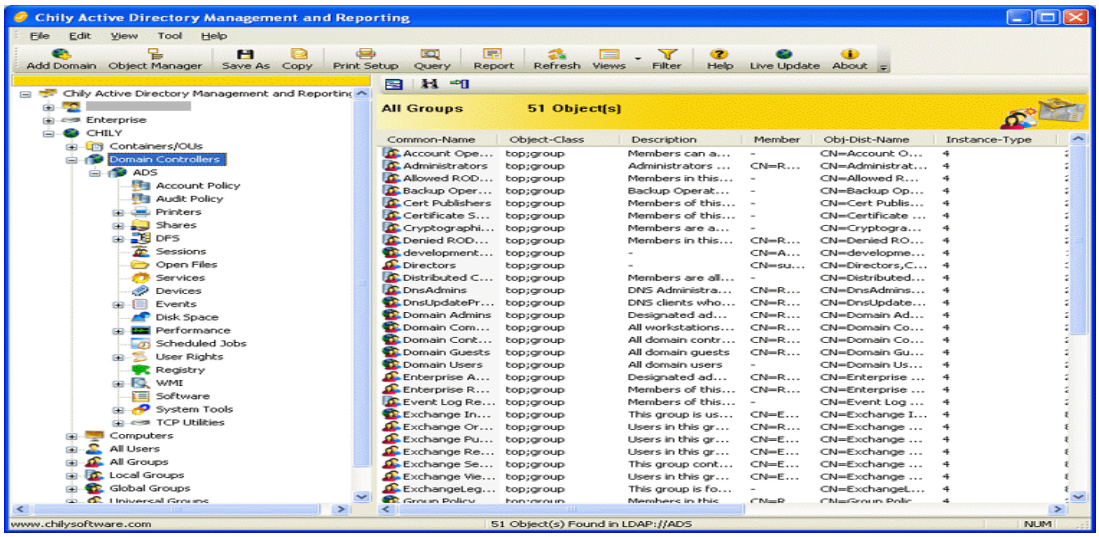
MICROSOFT ACTIVE DIRECTORY[114]: es la implementación más reciente de servicios de directorio para Windows 2000. Las cuestiones básicas relacionadas con un centro de servicios de directorio giran alrededor de la información que se puede almacenar en la base de datos, cómo se almacena, cómo se puede consultar información específica y qué se puede hacer con los resultados. Active Directory se compone del propio servicio de directorio junto con un servicio secundario que permite el acceso a la base de datos y admite las convenciones de denominación X.500.

Puede consultar el directorio con un nombre de usuario para obtener información como el número de teléfono o la dirección de correo electrónico de ese usuario. Los servicios de directorio también son lo suficientemente flexibles como para permitir la realización de consultas generalizadas (" ¿dónde están las impresoras? “) o bien " ¿cuáles son los nombres de servidores? ").Para así ver una lista resumida de las impresoras o servidores disponibles.

Los servicios de directorio también ofrecen la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa. Los usuarios pueden buscar y usar recursos en la red sin conocer el nombre o la ubicación exactos del recurso. Igualmente, puede administrar toda la red con una vista lógica y unificada de la organización de la red y de sus recursos.

[114]MICROSOFT SOPORTE, Introducción a ActivityDirectory. Disponible en Internet: http://support.microsoft.com/kb/196464/es. Consultado:18 de Octubre de 2000

Figura 29. ActivityDirectory.



Fuente: MICROSOFT SOPORTE, Introducción a ActivityDirectory. Disponible en Internet: http://support.microsoft.com/kb/196464/es. Consultado: 18 de Octubre de 2000

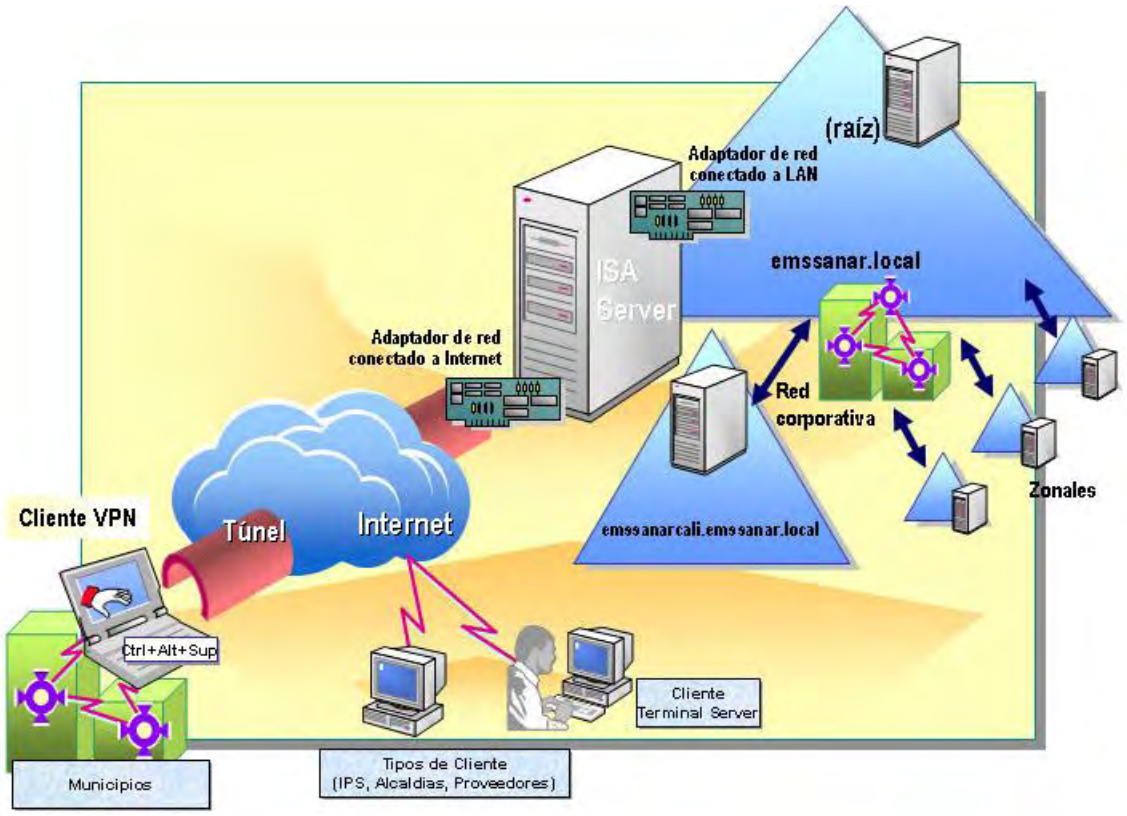
- **Equipos y su conectividad**

Equipos. En la actualidad EMSSANAR E.S.S, su topología de red es de estrella jerárquica. Cuenta con dos (2) centros principales y ocho (8) zonales, cuatro oficinas especiales o de referencia:[115]

[115] EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. Manual plataforma tecnológica. Colombia 2011. 29 p.

SISTEMA DE INTERCONEXION Y PLATAFORMA TECNOLOGICA EMSSANAR

Figura 30 Plataforma tecnológica



Fuente: Empresa Solidaria de Salud Emssanar E.S.S

CENTROS PRINCIPALES

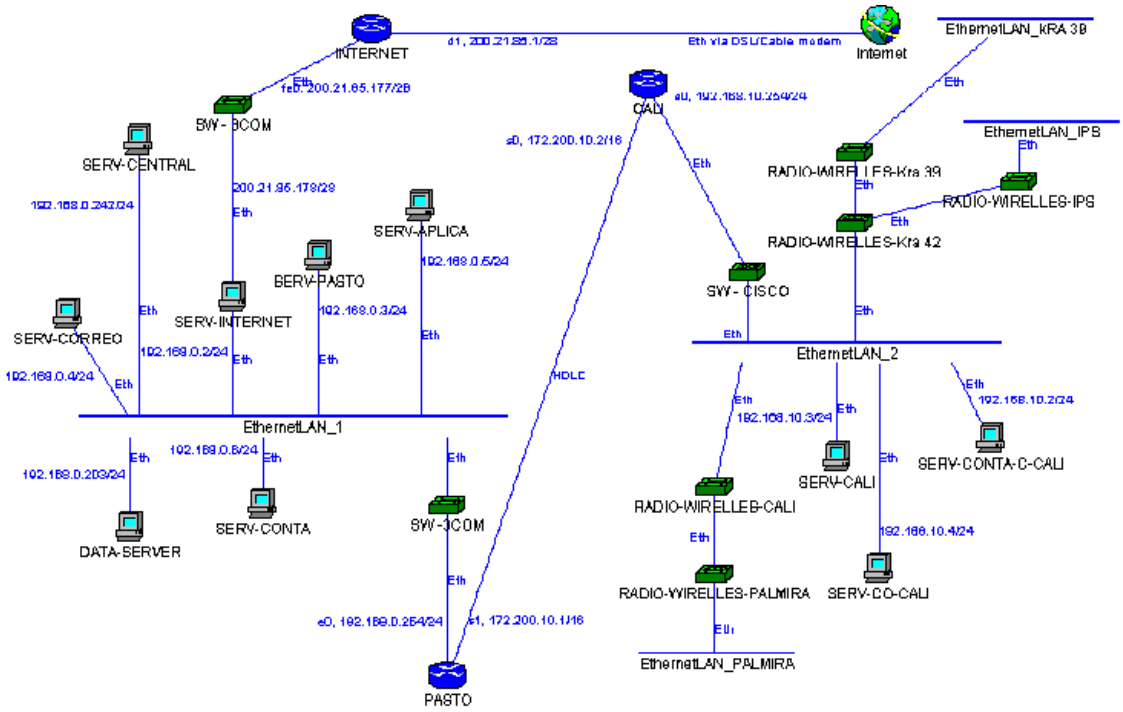
El primero: Ubicado en la ciudad de Pasto que para efectos administrativos se denomina Oficina Corporativa y Regional Nariño – Putumayo. Distribuido en tres sedes que son la A (sede IPS), B (centro de capacitación Emssanar) C (sede Administrativa), sede cresemillas (centro de contactos, SIAU, autorizaciones, gestión documental) y sede fundación (Santiago).

La plataforma tecnológica se encuentra soportada bajo directorio activo Windows 2000 server, Windows 2003, Windows 2008 distribuida y Linux en varios servidores de propósito específico.

El segundo. Ubicado en la ciudad de Cali, denominada Sede Regional Valle – Cauca. Distribuida en tres sedes: Principal kra 42, sede SIAU kra 39 y sede IPSSF Cali.

La interconexión entre estas es a través de una red inalámbrica WIRELESS para datos y voz. Tecnología OFDM. Con un ancho de banda de 54 Mbps su plataforma tecnológica se encuentra bajo la arquitectura Windows 2000 Server, posee tres servidores.[116]

Figura 31. Estructura Networking



Fuente: Empresa Solidaria de Salud Emssanar E.S.S

OFICINAS ZONALES y ESPECIALES

NARIÑO - PUTUMAYO

- Túquerres
- Ipiales
- Mocoa
- Tumaco

[116]EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. Manual plataforma tecnológica. Colombia 2011. 29 p.

- Barbacoas
- Puerto Asís
- La Cruz

VALLE - CAUCA

- Sevilla
- Tuluá
- Popayán
- Buenaventura
- Palmira

CARACTERISTICAS DE LA RED DE DATOS EMSSANAR E.S.S.[117]

La normalización y estándares que se encuentra instalada la red es 568 A UTP categoría 6 y tendido paralelo telefónico 5E.

Se restringen los accesos a la red a personal no autorizado. En la parte lógica se manejan 3 niveles de seguridad, en la parte física los centros de cómputo y áreas de comunicaciones se restringe a personal del área de sistemas.

La empresa cuenta con una óptima administración de redes de datos especializados en:

Validador de claves, servidor de correos, servidor de Internet, servidor de Intranet interno, servidor de base de datos, de aplicativos, hosting y servidor de multitareas.

La empresa aplica controles de acceso y concurrencia. Acceso restringido por usuario a tres niveles y la concurrencia sólo se maneja en el servidor de Internet e intranet.

Para controlar la operación en la red, se cuenta con snnifer que es un programa que permite diagnosticar el estado de funcionamiento de la red, ancho de banda, broadcast, Firewall, servidor de vacunas que se actualiza automáticamente cada 7 días. Se lleva un registro de controles de equipo computadores; procesadores, módems; multiplexores con una base de datos detallada por componente, asignación de recursos a fin de controlar los activos, mantenimiento, soporte.

[117] EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. Manual plataforma tecnológica. Colombia 2011. 29 p.

Conectividad

La empresa solidaria de Salud Emssanar E.S.S trabaja con redes públicas, las mismas que sirven para la conexión a internet, y cuenta con una red privada, la cual es para la conexión interna y subredes para las respectivas zonales.[118]

2.2 ARCHIVO CORRIENTE

Este archivo está compuesto por documentos directamente relacionados con el desarrollo del proyecto.

2.2.1 Plan de auditoría/ metodología

Metodología de la auditoría. Las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada eficaz, razón por la que la metodología utilizada para la realización de la auditoría de sistemas dentro de Emssanar E.S.S es de tipo cuantitativo/subjetivo, basados en un modelo matemático numérico, arrojando como resultado una lista de riesgos obtenidos del análisis de cada uno de los procesos a auditar teniendo en cuenta su importancia e impacto dentro del área de sistemas de ahí su calificación y recomendaciones realizadas.

La metodología aplicada en la realización de esta auditoría, se ejecutó de la siguiente manera:

[118] EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. Manual plataforma tecnológica. Colombia 2011. 29 p.

Etapa1. Exploración del entorno. Este primer paso se realizó con el fin de familiarizarse con el área de sistemas de la entidad Emssanar E.S.S, se hace un estudio previo de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoría, también en esta etapa se definen que elementos se utilizaron para elaborar la auditoría. Se realizaron varias visitas a la sede principal Emssanar E.S.S con el fin de conocer y observar los diferentes procesos, para identificarlos y auditarlos, a través de entrevistas abiertas se dio inicio a la recolección de información, dando el siguiente paso que fueron la aplicación de cuestionarios cuantificables con los funcionarios de los diferentes departamentos, como también la visita a las diferentes sedes que tiene Emssanar, así:

- Sede principal Emssanar E.S.S
- Sede la Aurora Pasto
- Emssanar I.P.S
- Cresemillas (SIAU Atención al Usuario y CC Centro de Contactos)
- IPS Lorenzo.

También se visitaron la zonal que en este caso es el municipio de Ipiales.

Etapa2. Planeación de las actividades de auditoría

Aquí se realizó la planificación de todo el proceso de la auditoría, con las siguientes actividades:

- Se realizó un estudio previo del área de sistemas de Emssanar ESS obteniendo información necesaria respecto al tema.
- Se identificó el alcance y los objetivos de la auditoría a realizar.
- Determinación de los recursos necesarios con los que se realizó la auditoría.
- Se elaboró el plan de trabajo.

Etapa3. Realización las actividades de la auditoría. En esta etapa se realizaron las diferentes actividades implantadas en la etapa anterior, mediante la aplicación de técnicas junto con la aplicación de diferentes herramientas que garantizo el cumplimiento de los objetivos propuestos para la ejecución de la auditoría. En esta etapa se realizaron las siguientes actividades:

Elaboración del plan de auditoría, a través de COBIT permitiendo así la identificación de los procesos y objetivos de control evaluados.

Se elaboran cuadros de definición de fuentes de conocimiento, que facilitan la identificación clara de la fuente de obtención de las pruebas.

Se aplicaron entrevistas con preguntas abiertas y preguntas cerradas para la obtención de información general de la empresa, para luego elaborar diferentes cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT a auditar.

Se realiza la identificación de vulnerabilidades, riesgos y amenazas, y su valoración con respecto a la probabilidad e impacto mediantes la utilización del COBIT (modelo para auditoría y control de sistemas de información).

✓ Identificar las vulnerabilidades, riesgos y amenazas existentes en el sistema.

✓ Valorar los riesgos según la escala definida para la probabilidad e impacto.

Identificación de hallazgos. Mediante el formato de hallazgos, se asigna la probabilidad de ocurrencia e impacto para los riesgos encontrados.

Etapa 4. Presentación del informe final. Etapa en la cual se realizó el informe final que contiene todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa o los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo. Este informe se presentó y se entregó al personal de la jefatura del área de sistemas de la sede principal Emssanar E.S.S, para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

2.2.2 Instrumentos de recolección de datos

Fuentes primarias. Las fuentes primarias en el desarrollo de esta auditoría se poseen las siguientes:

✓ Entrevistas, dirigidas al departamento de sistemas de Emssanar sede Central y elementos y extensiones sede Lorenzo, sede Cresemillas, Sede la Aurora, Sede parque Bolívar.

✓ Ejecución de los cuestionarios en todas las áreas de sistemas sede Central y subsedes en la Empresa solidaria de Salud Emssanar.

✓ Manuales, que estén relacionados con los procesos que se manejan en el área de sistemas en la Empresa solidaria de Salud Emssanar.

Este tipo de pruebas se encuentran como anexos para su consulta ver los siguientes anexos:

- Anexo entrevista seguridad lógica
- Anexos entrevistas y checklist
- Anexos manual de funciones
- Anexo lista de chequeo

Fuentes secundarias. Para el desarrollo de este proyecto de auditoría, se cuenta con la vasta gama de libros referenciales y la web, por lo anterior se podrá consultar temas relacionados con auditorías informáticas de seguridad de la red de datos, información relacionada con software para la auditoría de redes, administración de la seguridad informática. Etc.

Este tipo de pruebas se encuentran como anexos para su consulta ver los siguientes anexos:

- COBIT marco teórico.
- Anexo información suministrada por Emssanar E.S.S

2.2.3 Plan de pruebas. El plan de pruebas permite anotar todas las observaciones durante el proceso de la auditoría de manera secuencial, este contiene lo siguiente: Prueba, proceso, tipo y acción de la prueba.

2.2.4 Programa de auditoría. Para la ejecución de la auditoría física y lógica de la Red de Datos de la Empresa Solidaria de salud EMSSANAR E.S.S sede central y zonal alto putumayo, se utiliza la metodología COBIT (Control Objetives for Information and related Technology) de ISACA (Information System Audit and Control Asociation), que cubre 210 objetivos de control clasificados en 4 dominios y 34 procesos. De los cuales se aplican los siguientes:

Dominio Planificación y Organización (PO).[119]La planificación y el dominio de organización cubren el empleo de tecnología y como puede esta ser mejor utilizada en una empresa para ayudar a alcanzar los objetivos de la empresa y objetivos. Esto también destaca la forma de organización e infraestructura TI debe tomar para alcanzar los resultados óptimos y generar la mayor parte de ventajas del empleo de TI.

[119] IT GOVERANCE INSTITUTE, CobiT4.1.Estados Unidos de América, Pág. 51-54 (ISBN 1-933284-37-4)

Procesos de Dominio Planificación y Organización (PO)

- PO3 Determinar la dirección tecnológica
- PO4 Definir los procesos, organización y relaciones de TI
- PO9 Evaluar y administrar los riesgos de TI

Dominio Adquisición e Implementación (AI).[120]Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, cubre los cambios y el mantenimiento realizado a los sistemas existentes.

Procesos de dominio Adquisición e Implementación:

AI3. Adquirir y mantener infraestructura tecnológica
AI5. Adquirir recursos de TI
AI6. Administrar Cambios de TI

Dominio Entrega y Soporte.[121]En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios.

DS1 Definir niveles de servicio
DS2 Administrar servicios prestados por terceros
DS3 Administrar desempeño y capacidad
DS4 Asegurar servicio continuo
DS5 Garantizar la seguridad de sistemas
DS9 Administrar la configuración
DS10 Administrar problemas e incidentes
DS11 Administrar datos
DS12 Administrar instalaciones
DS13 Administrar operaciones

[120] IT GOVERANCE INSTITUTE, CobiT4.1.Estados Unidos de América, Pág. 72-100 (ISBN 1-933284-37-4)

[121]Ibíd. ,P.101-157

Monitoreo.[122]Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y eficiencia en cuanto a los requerimientos de control.

M1 Monitorear y evaluar el desempeño de TI
M2 Evaluar lo adecuado del control Interno
M3 Obtener aseguramiento Independiente
M4 Proporcionar auditoría independiente
Recolección de información dominio monitoreo

2.2.5 Entrevistas, formato de entrevistas y checklist

Las Entrevistas. Le proporcionan al auditor el conocimiento del personal auditado y como se están llevando a cabo las funciones en la organización, las entrevistas se realizaron al administrador de la red de datos de Emssanar, ingeniero Diego Bastidas, quien posee la información y conocimientos necesarios para brindar toda la información pertinente y necesaria para la auditoría.

Tipo de entrevista utilizada, Se utilizó entrevistas de tipo abierto y tipo cerrado, para la realización de esta auditoría informática**.**

El checklist. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. El conjunto de estas preguntas recibe el nombre de checklist. Salvo excepciones, las checklist deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Formato de checklist utilizado. Las checklist binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo.

[122] IT GOVERANCE INSTITUTE, CobiT4.1.Estados Unidos de América, P. 153-166 (ISBN 1-933284-37-4)

2.2.6 Fuentes de conocimiento y plan de pruebas

Cuadros fuentes de conocimiento y cuestionarios

Cuadro 1. Fuente de conocimiento PO3

Emssanar E.S.S. ¡Siempre cerca de Usted!	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-PO3-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , HeiderQuetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Planeación y Organización (PO)		
PROCESO: PO3 Determinar la Dirección Tecnológica.		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de Conocimiento	**Métricas: Medidas o Indicadores**	**REPOSITORIO DE PRUEBAS APLICABLES**	
		De Análisis	**De Ejecución**
- Entrevista al funcionario encargado del área de sistemas de Emssanar EPS de pasto. -Entrevista al Coordinador de Sistemas y Comunicaciones. -Manual de Procedimientos Asistentes de Soporte y Mantenimiento. -Arquitectura de Red. -Estándares y Directrices de las comunicaciones. -Soluciones tecnológicas.	% de la organización de la red de datos % de aplicabilidad y factibilidad de los planes de contingencia. % de funcionalidad, y relación costo-beneficio en cuanto al plan de infraestructura tecnológica de la red de datos. % factibilidad, relación costo beneficio de las soluciones tecnológicas en cuanto a la red de datos.	-Analizar la estructura y organización de la empresa. -Analizar el Manual de Procedimientos Asistentes de Soporte y Mantenimiento. -Analizar el plan de contingencia para el sistema -Analizar las políticas de seguridad en caso de desastres de la Red. -Análisis del plan de infraestructura tecnológico. -Analizar las soluciones tecnológicas existentes en la empresa.	-Revisión detallada de los manuales de mantenimiento y Procedimientos. -Revisión detallada de la Arquitectura de red, de las políticas y aplicación de las normas. -Revisión detallada de los planes de contingencia, el cumplimiento de estas, el conocimiento por el personal. -Revisar detalladamente el plan de infraestructura tecnológico de la red de datos. -Revisar soluciones tecnológicas en cuanto a la parte de la red de datos.

Cuadro 2. Fuente de conocimiento PO4

Emssanar E.S.S. ¡Siempre cerca de Usted!	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-PO4-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , Heider Quetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Planeación y Organización (PO)		
PROCESO: PO4 Definición Procesos , Organización y Relaciones de TI		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de Conocimiento	**Métricas: Medidas o Indicadores**	**REPOSITORIO DE PRUEBAS APLICABLES**	
		De Análisis	**De Ejecución**
- Entrevista al funcionario encargado del área de sistemas. -Estructura organizacional del Área de Sistemas. -Entrevista con el funcionario encargado de realizar la actualización y el seguimiento a los indicadores. -Manual de funciones del personal de Emssanar EPS, relacionado con los servidores comunicaciones e indicadores. -Descripción de roles y responsabilidades del personal encargado de operar el hardware de los servidores, las comunicaciones e indicadores.	% de concordancia entre aptitudes, capacitación del personal y su asignación de responsabilidades. %de descentralización en funciones dentro de la organización. % de cumplimiento de actividades realizadas versus el manual de funciones.	-Analizar el manual de funciones del personal del área de sistemas. -Analizar la estructura y organización del área de sistemas. -Analizar los roles y responsabilidades del personal encargado de los servidores y las comunicaciones.	-Revisión detallada para evaluar la estructura organizacional del área de sistemas, asignación de responsabilidades y evaluar personal encargado del manejo de los recursos de las TI, identificando las personas claves del manejo de las comunicaciones. -Una revisión detallada de las aptitudes del personal, las funciones y responsabilidades asignadas y separación de funciones. -Evaluar las actividades descritas en el manual de funciones y comparar con las actividades realizadas.

Cuadro 3. Fuente de conocimiento PO9.

	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-PO9-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , Heider Quetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Planeación y Organización (PO)		
PROCESO: PO9 Evaluar y Manejar los Riesgos de TI		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de conocimiento	**Métricas medidas o indicadores**	**Repositorios de pruebas aplicables**	
		De análisis	**De ejecución**
- Entrevista con el coordinador de la red de datos, las comunicaciones y los servidores. -Descripción de la evaluación de los riesgos de la parte física, lógica de las comunicaciones y la red de datos. -Plan de acción contra Riesgos. -Políticas y procedimientos relacionados con la evaluación y gestión de riesgos relacionados con la parte lógica y física de los servidores y la red de datos. -Plan de contingencia contra riesgos informáticos. -Documentos de evaluación de riesgos.	% de concordancia entre aptitudes, capacitación del personal y su asignación de responsabilidades. %de descentralización en funciones dentro de la organización. % de cumplimiento de actividades realizadas versus el manual de funciones.	-Analizar la evaluación de riesgos. - Analizar el documento de la metodología de evaluación de los riesgos, nivel de relevancia, etc. -Analizar el plan de acción contra riesgos, identificar estrategias para evitar, reducir o mitigar el riesgo según sea conveniente, para tener un control óptimo de seguridad de los recursos de la empresa. -Analizar las políticas y procedimientos relacionados con la evaluación y gestión de riesgos relacionados con la parte física de los servidores y la red de datos. -Análisis de los documentos de evaluación del riesgo del hardware de los servidores y de la red de datos y comunicaciones.	-Revisión detallada para evaluar los riesgos físicos y lógicos de la red de datos, identificando la magnitud del riesgo y la priorización del mismo, evaluando el impacto de este, la solución y el nivel de aceptación de estos. -Revisión detallada del plan de acción de riesgos, respuesta de solución de riesgos encontrados, monitorear el cumplimiento de la ejecución de los planes de acción. -Verificar si se han realizado simulacros de los planes de contingencia. -Una revisión detallada del enfoque de evaluación de riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual. -Revisión detallada de los planes de Contingencia.

Cuadro 4. Fuente de conocimiento AI3.

	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-AI3-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , Heider Quetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Adquisición e Implementación (AI)		
PROCESO: AI3 Adquirir y mantener la infraestructura tecnológica		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de Conocimiento	**Métricas: Medidas o Indicadores**	**REPOSITORIO DE PRUEBAS APLICABLES**	
		De Análisis	**De Ejecución**
- Entrevista con el coordinador de Sistemas, de Comunicaciones y de la red de datos. -Documento del plan de Adquisición de Infraestructura tecnológica. -Documento de contratos de adquisición. -Documento de lista de proveedores acreditados Planes de contingencia. -Entrevista con el encargado de aprobar la adquisición de elementos hardware y software de red. -Plan de adquisición e Implementación de hardware de red.	% adquisición de recursos tecnológicos de elementos de la red de datos. %de mantenimiento de los equipos de la red de datos. % de cumplimiento de las políticas en cuanto a la adquisición de recursos tecnológicos.	-Analizar las políticas y la aplicación de las normas relacionadas con la adquisición de la infraestructura tecnológica. - Analizar el plan de mantenimiento de la infraestructura tecnológica de la red de datos. -Analizar el plan de contingencia. -Analizar el plan de mantenimiento de la infraestructura de la tecnología.	-Revisión detallada de los elementos de la red de datos, servidores, instalaciones, cableado, software. -Revisión de documentos relacionados con la adquisición e implementación de nuevos elementos de la red de datos. - Comparar los roles y responsabilidades estipuladas con las que en realidad realiza el personal.

Cuadro 5. Fuente de conocimiento AI5.

	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-AI5-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , Heider Quetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Adquisición e Implementación (AI)		
PROCESO: AI5 Adquirir Recursos		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de Conocimiento	**Métricas: Medidas o Indicadores**	**REPOSITORIO DE PRUEBAS APLICABLES**	
		De Análisis	**De Ejecución**
- Entrevista con el jefe de sistemas encargado de autorizar adquisiciones de hardware y software de la red de datos. -Políticas y procedimientos estándares relacionados con la adquisición de nuevos recursos de TI. - Políticas y procedimientos para modificar y concluir contratos para proveedores. -Selección de proveedores.	% conformidad con políticas y estándares establecidos para adquisiciones tecnológicas. % relación costo beneficio de elección de sus proveedores informáticos. % conformidad con procesos de selección y contratación con los proveedores.	-Analizar la información de las últimas adquisiciones realizadas. -Analizar las políticas y procedimientos estándares relacionados con la adquisición de nuevos recursos TI. - Analizar las políticas y procedimientos para modificar y concluir contratos para proveedores. -Analizar cómo se realiza la selección de los proveedores.	-Revisión detallada de la información de adquisición de recursos TI -Revisión detallada de la información relacionada con los procedimientos para modificar y concluir contratos para proveedores. - Revisar la forma como se selecciona y como se realiza la contratación de proveedores. -Revisar el documento de contratos.

Cuadro 6. Fuente de conocimiento AI6.

Emssanar E.S.S. ¡Siempre cerca de Usted!	Empresa Auditora: Datos y Procesos.	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Evaluación RACI, Pruebas de Análisis y Pruebas de Auditoría.
Entidad Auditada:	**EMSSANAR**	
Área Auditada:	**SISTEMAS**	**Ref: PL-AN-AI6-1**
Objeto de Estudio	**Parte física y lógica de la Red de datos.**	
Responsables:	Diego Alexander Acosta , Heider Quetama Caicedo	
Material de Soporte:	Manual Cobit 4.0: Objetivos de Control, Marco de Trabajo, Directrices de Auditoría, Herramientas de Implementación.	
DOMINIO: Adquisición e Implementación (AI)		
PROCESO: AI6 Administrar Cambios		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoría definidas en la Metodología Cobit, en el ámbito del Sistema		

Fuentes de Conocimiento	**Métricas: Medidas o Indicadores**	**REPOSITORIO DE PRUEBAS APLICABLES**	
		De Análisis	**De Ejecución**
- Entrevista con el jefe encargado de administrar formalmente y controladamente dichos cambios a nivel físico y lógico de la red de datos. -Procedimientos para evaluar cambios en la infraestructura tecnológica y de la red de datos. -Procedimientos para priorizar solicitudes y aprobación de cambios de la infraestructura tecnológica y de redes. -Reportes de solicitudes de cambios.	% cambios en materia de redes que se hacen dentro de la empresa. % efectividad en cuanto a la solución de problemas mediante la aplicación de cambios de la red de datos. % rendimiento y seguimiento a los cambios realizados en la red de datos de la organización.	-Analizar el proceso que se lleva para realizar cambios de la infraestructura tecnológica. -Analizar los procedimientos para dar prioridad y aprobación de solicitudes de cambios. - Analizar los reportes de cambios de la infraestructura.	-Revisión detallada de la información de los cambios de la infraestructura tecnológica. -Revisión detallada de la información relacionada con los procedimientos para priorizar los cambios. - Revisión detallada de los reportes de solicitudes de cambios.

2.2.7 Cuestionarios

Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar. Con la aplicación del cuestionario cuantitativo se obtuvo el porcentaje de riesgo el cual se obtiene aplicando la siguiente fórmula:

$$\textbf{\% de Riesgo} = \frac{\textbf{Sumatoria de SI} * \textbf{100}}{\textbf{Total Encuesta} - \textbf{Totales NA}}$$

% Total de Riesgo = 100 - % de Riesgo

Para determinar el nivel de riesgo total, se tuvo en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

Riesgo bajo: Deficiencias bajas en grado de importancia mayor, fáciles de solucionar a largo plazo.

Riesgo medio: Se debe tomar medidas de solución o mejora en un determinado periodo de tiempo.

Riesgo alto: se debe establecer soluciones inmediatas para reducir el riesgo sin afectar los objetivos del caso de estudio.

Entonces, se calcula así:

% de Riesgo Total = 100 - % de Riesgo

El resultado obtenido, permitió formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que este toma validez con la obtención de pruebas, que verifique los resultados de la encuesta.

Recolección de información DOMINIO PLANEACION Y ORGANIZACIÓN (PO)

Cuadro 7. Cuestionario PO4

Emssanar E.S.S ¡Siempre cerca de Usted!	**CUESTIONARIO CUANTITATIVO**	**REF PLAN PO4**				
ENTIDAD AUDITADA		EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		**PAGINA 1 DE 2**		
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**		Parte física y lógica de la Red de datos.		
RESPONSABLES		Diego Alexander Acosta y Heider Quetama Caicedo.				
MATERIA L DE SOPORTE		COBIT 4.0				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	PO4 Definir los procesos, la organización y las relaciones de TI			
PREGUNTA			**SI**	**NO**	**NA**	**FUENTE**
1. ¿Existe un manual de funciones del personal en el área de sistemas de EMSSANAR?			**4**			
2. ¿El manual de funciones del personal del área de sistemas se encuentra actualizado?				**4**		
2. ¿El manual de funciones del personal es difundido dentro del área de Sistemas de Emssanar?				**3**		
3. ¿Existe un proceso para revisar la estructura organizacional del área de sistemas de forma periódica para ajustar requerimientos de personal?			**4**			
4. ¿Existen prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada?			**4**			
5. ¿Se tiene definido e identificado al personal clave en el área de sistemas de EMSSANAR E.S.S?			**5**			
6. ¿En caso de falta del personal clave en la parte de Redes de datos EMSSANAR E.S.S, se tiene planes de contingencia para su reemplazo en caso de ausencia?				**4**		
7. ¿Se han realizado simulacros al respecto, del reemplazo de funcionarios clave en el área de la red de datos de EMSSANAR E.S.S?				**4**		
6. ¿Existen políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por el área de Sistemas, o de la Organización?			**5**			
7. ¿Existe un manual de funciones para el personal encargado para el funcionamiento de la red de datos?			**5**			
8. ¿Existen planes de contingencia para reemplazar a algunos de los funcionarios en caso de ausencia?				**4**		
9. El plan de contingencia para reemplazar funcionarios cumple con los siguientes requisitos • ¿Está documentado?				**4**		
• ¿Contiene procedimientos para contratación del personal de Reemplazo?				**4**		
10. ¿Existen políticas y procedimientos para realizar la contratación de personal nuevo?			**5**			
11. Las políticas de contratación de personal nuevo cumple con las siguientes características: • ¿Cualquier persona que cumpla con los requerimientos puede aspirar al cargo?			**5**			

• ¿Para la selección del personal de TI a contratar, se aplica el principio de meritocracia?	**5**			
TOTAL	**42**	**27**		
TOTAL CUESTIONARIO		**69**		

PORCENTAJEDE RIESGO = $\frac{42*100}{69}$= 60.87**%.**
% de Riesgo Total = 100 – 60.87= 39.13%
Por lo tanto el Riesgo es MEDIO.

Después de aplicar el cuestionario se determinó que el porcentaje de riesgo en este proceso es medio, debido a que falta documentar procedimientos en el área de sistemas y la realización de simulacros se lleva a cabo pero no se documentan los resultados de las pruebas.

Cuadro 8. Cuestionario DS2.1

Emssanar E.S.S. ¡Siempre cerca de Usted!			**R/PT**	
Cuestionario de Control			**C4**	
Dominio	Entrega de Servicios y Soportes			
Proceso	**Proceso DS2 Administración de servicios prestados por terceros**			
Objetivo de Control	· Monitoreo de la entrega de servicio			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Existen controles o monitoreo sobre los servicios de red prestada por terceros?		4		
¿El monitoreo o control de estos servicios es llevado a cabo por el administrador de la red?		4		
¿Por el jefe de sistemas?		4		
¿Por otro personal encargado?			4	
¿El proveedor de los servicios de red, subcontrata servicios para cumplir con el contrato para Emssanar?				X
¿Se informó a la empresa de esta subcontratación antes de realizarse el contrato?				X
¿Se realizó un análisis de riesgo antes de realizar la subcontratación?			3	
¿Está satisfecho con el contrato de servicios de red que tiene actualmente Emssanar?		4		
los controles a los servicios de red se llevan a cabo de manera diaria				
Semanal		4		
mensual				
Anual				
¿El monitoreo o controles documentado?		4		
¿Se han presentado inconvenientes en la prestación de los servicios			**4**	

de red, que afecten la seguridad lógica o física de la red de Emssanar?			
¿Existe algún inconveniente en caso de cambiar de servicios de red con otro proveedor?		**4**	
¿Son inconvenientes del tipo? Legal			
Administrativo			
Físico		**3**	
Lógico		**4**	
TOTAL	**24**	**22**	
TOTAL CUESTIONARIO			

PORCENTAJE DE RIESGO:= $\frac{24*100}{46}$= 52.17%

% de Riesgo Total = 100 –52.17= 47.83**%**

Por lo tanto el porcentaje de riesgo es MEDIO.

Después de aplicar el cuestionario se determinó que el porcentaje de riesgo en este proceso es medio, debido a que se encontraron debilidades que podrían ocasionar un riesgo para la seguridad de la red de datos ya que varios servicios no satisfacen completamente a la organización.

Cuadro 9. Cuestionario DS4

Emssanar E.S.S. ¡Siempre cerca de Usted!		**R/PT**		
Cuestionario de Control		**C4**		
Dominio	Entrega de Servicios y Soportes			
Proceso	**Proceso DS4 Asegurar continuidad del servicio**			
Objetivo de Control	Clasificación de severidad, plan documentado.			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Existen planes de contingencia en caso de ataques físicos a la red?		4		
¿Se encuentran documentados?			4	
¿Se han hecho simulacros al respecto?			5	
¿Existen planes de contingencia en caso de ataques lógicos a la red?		4		
¿Se encuentran documentados?			4	
¿Se han hecho simulacros al respecto?			4	
¿Existen políticas para el uso de los computadores conectados a la red de Emssanar?		4		
¿Existe diagrama de la red de datos de Emssanar?		5		
¿Esta actualizado el diagrama de Red de datos de			5	

Emssanar E.S.S?			
¿Se encuentra documentado?		4	
¿Existen sistemas de comunicación alternativos en caso de avería o fallo?	4		
En los contratos de comunicaciones ¿Están claramente reflejados los parámetros que definen la calidad de servicio, como ancho de banda, tiempo de respuesta de averías?	4		
TOTAL	**25**	**26**	
TOTAL CUESTIONARIO	**51**		

PORCENTAJE DE RIESGO:= $\frac{25*100}{51}$= 49.02%

% de Riesgo Total = 100 – 49.02= 50.98**%**

Por lo tanto el porcentaje de riesgo es MEDIO.

Después de aplicar el cuestionario se determinó que el porcentaje de riesgo en este proceso es medio, debido a que existe información de la red que no ha sido actualizada, además falta entregar información documentada a los usuarios finales.

Cuadro 10. Cuestionario D12

		R/PT		
Cuestionario de Control		**C3**		
Dominio	Entrega de Servicios y Soportes			
Proceso	DS12: Administración de Instalaciones.			
Objetivo de Control	Escolta de Visitantes			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Las instalaciones (cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de cómputo?		4		
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?		4		
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?		4		
¿Existen lugares de acceso restringido?		4		
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?		5		
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?			4	
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?		5		
¿Se tienen medios adecuados para extinción de fuego en el centro de		4		

cómputo?			
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?	3		
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?	3		
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?	4		
¿Son funcionales los muebles instalados dentro del centro de cómputo archiveros, mesas de trabajo, etc.?	3		
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?		3	
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?		3	
¿Con cuanta frecuencia se limpian las instalaciones? Semanal		3	
Mensual			
Anual			
¿Se cuenta en los cuartos de comunicaciones con piso falso?	4		
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)? Semanal			
Mensual	4		
Anual			
Emssanar ¡Siempre cerca de Usted!	**R/PT**		
Cuestionario de Control	**C4**		
Dominio	Entrega de Servicios y Soportes		
Proceso	**DS12**Protección contra Factores Ambientales		
Objetivo de Control	Controles Ambientales		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿El centro de cómputo tiene alguna sección con sistema de refrigeración?	4		
¿Con frecuencia se revisan y calibran los controles ambientales?		4	
¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental?		4	
¿Se tienen instalados y se limpian regularmente los filtros de aire?	3		
¿Con frecuencia se limpian los filtros de aire?		3	
¿Se tiene plan de contingencia en caso de que fallen los controles ambientales?		4	
TOTAL	**58**	**28**	
TOTAL CUESTIONARIO	86		

PORCENTAJE DE RIESGO:= $\frac{58*100}{86}$= 67.44%

% de Riesgo Total = 100 – 85.71=32.56**%**

Por lo tanto el porcentaje de riesgo es MEDIO.

Después de aplicar el cuestionario se determinó que el porcentaje de riesgo en este proceso es medio, debido a que la organización se preocupa por la seguridad

física de sus instalaciones, pero faltan carteles de señalización que guíen a los visitantes en caso de estar cerca a los equipos de cómputo ,cableado o routers.

Cuadro 11. Cuestionario DS12.2 protección contra factores ambientales

Emssanar E.S.S. ¡Siempre cerca de Usted!			**R/PT**
Cuestionario de Control			**C6**
Dominio	Entrega de Servicios y Soportes		
Proceso	**DS12**Protección contra Factores Ambientales		
Objetivo de Control	Seguridad Física		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se tienen lugares de acceso restringido?	3		
¿Se poseen mecanismos de seguridad para el acceso a las salas de cómputo y cuartos de comunicaciones?	3		
¿A este mecanismo de seguridad se le han detectado debilidades?		4	
¿Tiene medidas implementadas ante la falla del sistema de seguridad?		4	
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso? Mensual	4		
Bimestral			
Anual			
¿Se tiene un registro de las personas que ingresan a las instalaciones?	4		
TOTAL	10	8	
TOTAL CUESTIONARIO	18		

PORCENTAJE DE RIESGO:= $\frac{10*100}{18}$= 55.56%

% de Riesgo Total = 100 – 55.56= 44.44**%**

Por lo tanto el porcentaje de riesgo es MEDIO.

Después de aplicar el cuestionario se determinó que el porcentaje de riesgo en este proceso es medio, debido a que es un proceso de vital importancia para la seguridad de la red de datos, especialmente la actualización de contraseñas y planes de contingencia en caso de fallas del sistema de seguridad.

2.2.8 Análisis y evaluación de riesgos

Lista de riesgos

A) Riesgos Dominio Planeación Y Organización

- **PO3 Determinar la dirección tecnológica**

R1. El plan de infraestructura tecnológica se encuentra completo pero no actualizado.

R2. Se lleva un control y una actualización del plan de infraestructura tecnológico, pero no está documentada.

R3. No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware de la red de datos de Emssanar E.S.S.

R4.Existe un inventario actualizado del hardware de comunicaciones, pero no se encuentra documentado.

R5.Se toma en cuenta el impacto de los cambios de actualización o mejora en el plan de infraestructura tecnológica, pero no está totalmente documentado.

- **PO4 Definir los procesos, la organización y las relaciones de TI**

R6. El manual de funciones del personal del área de sistemas no está actualizado, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.

R7. Existen prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, pero no está documentada ni se lleva un registro.

R8. En caso de falta del personal clave en la parte de redes de datos EMSSANAR E.S.S, no se tiene planes de contingencia para su reemplazo en caso de ausencia y no está documentado.

R9. No se han hecho simulacros al respecto de funcionarios clave del área de red de datos de EMSSANAR E.S.S.

- **PO9 Evaluar y administrar los riesgos de TI**

R10. No se tiene actualizado ni documentado el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S

R11.Elplan de seguridad informática no se encuentra debidamente documentado.

R12. No se cuenta con pólizas de seguros para el manejo del riesgo.

B) Riesgos Dominio Adquisición Y Mantenimiento

R13 las políticas para la adquisición de equipos hardware de la red de datos de EMSSANAR E.S.S, no está completamente documentadas.

C) Riesgos Dominio (Ds) Entrega Y Soporte

- **Proceso DS1 Definición de niveles de servicio**

R14.Las deficiencias en los niveles de servicio en cuanto a la red de datos de EMSSANAR E.S.S. No están identificadas.

Proceso DS2 Administración de servicios prestados por terceros

R15.Faltan simulacros, en cuanto al cambio de servicios de red adquiridos con terceros.

R16.No se lleva un registro de inconvenientes con la prestación de los servicios de red que presta EMSSANAR E.S.S, que puede afectar la seguridad lógica y física de la red de datos.

- **Proceso DS4 Asegurar continuidad del servicio**

R17.Los planes en caso de ataques físicos y lógicos de la red de datos de EMSSANAR E.S.S, no se encuentran documentados.

R18.No se han hecho simulacros al respecto del riesgo anterior R17.

R18.1El diagrama de la red de datos de Emssanar E.S.S no se encuentra actualizado.

R19.Existen políticas para el uso de los computadores conectados a la red de Emssanar, pero no están documentadas.

R20. No existe la vigilancia de los servidores las 24 horas.

- **DS12: Administración de instalaciones**

R21.En algunas sedes como la de recepción en la sede de la Aurora las oficinas o cubículos no son los adecuados para el área de computo.

R22. No Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores.

R23. La parte de cableado de la red de datos en Cresemillas se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.

R24. Existen prohibiciones para fumar, consumir alimentos y bebidas, pero falta suficientes carteles en lugares visibles.

R25.Con poca frecuencia se revisa y calibra los controles ambientales.

R26.No se tiene un plan de emergencia si falla los controles ambientales.

R27. No se Realizan simulacros con la planta eléctrica.

R28. No se tienen medidas implementadas en caso de falla del sistema de seguridad del área de sistemas de Emssanar E.S.S

- **DS13 Administración de operaciones**

No se encontraron riesgos destacables.

D) ME3 Garantizar el cumplimiento con requerimientos externos

R29. No se compara periódicamente el desempeño de las metas en el área de Sistemas de Emssanar E.S.S.

R30. Se tienen políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios en Emssanar, pero no se siguen en su totalidad o cabalmente.

2.2.9 Matriz de impacto con riesgos encontrados en proceso

Matriz de probabilidad e impacto. Según el MECI este componentes primordial en el desarrollo de la auditoría ya que permite determinar el nivel de riesgo de cada uno de los hallazgos encontrados, tanto cualitativa como cuantitativamente. Por medio de esta clasificación se puede observar cuál de los riegos es catastrófico, importante, moderado o aceptable y a su vez el respectivo valor del riesgo.

Matriz de probabilidad e impacto.

Figura 32. Matriz de probabilidad e impacto.

Probabilidad				
	Alto(3)	Riesgo Moderado (15)	Riesgo Importante (30)	Riesgo Inaceptable (60)
	Medio(2)	Riesgo Tolerable (10)	Riesgo Moderado (20)	Riesgo Importante (40)
	Bajo (1)	Riesgo Aceptable (5)	Riesgo Tolerable (10)	Riesgo Moderado (20)
		Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
			Impacto	

Fuente: RICARDO, Sánchez. Seguridad de los sistemas. Disponible en internet:http://mismamente-yo.blogspot.com/2012/05/seguridad-de-los-sistemas-de.html.

2.2.10 Hallazgos de la auditoría

Descripción del formato de hallazgos

- **ENTIDAD AUDITADA:** hace referencia al nombre de la entidad auditada.
- **REF:** cuestionario que determino el hallazgo.
- **AREA AUDITADA:** se refiere al área de TI la cual será el objeto de estudio.
- **SISTEMA:** hace referencia al nombre del sistema actual de la entidad auditada.
- **RESPONSABLES:** hace referencia a los nombres del equipo encargado de la auditoría.
- **Probabilidad:** hace referencia a la posibilidad de ocurrencia del riesgo.
- **Impacto:** hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- **Descripción Hallazgo:** se refiere a los detalles del hallazgo.
- **NIVEL DE RIESGO:** hace referencia al valor cualitativo o cuantitativo del riesgo.
- **CONSECUENCIA:** se refiere al efecto actual o futuro, que tendrá la organización, de no tomar las precauciones oportunas.
- **RECOMENDACIONES:** hace referencia a las descripciones correctivas de carácter preventivo.
- **EVIDENCIAS:** hace referencia a las pruebas que soportan los hallazgos, pueden ser anexos, entrevistas, cuestionarios, checklist, o videos.

Cuadro 12. Cuadro de hallazgos.

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. Plan**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definición de la arquitectura de información: (PO2)
Descripción Hallazgo:			
Probabilidad :		**Impacto:**	
Nivel de Riesgo:			
Consecuencia:			
Recomendaciones:			
Evidencias:			

Hallazgos encontrados

Cuadro 13. Cuadro de hallazgos PO3.

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**		**Ref. Plan PO3**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S			
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.	
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO				
Material de Soporte: COBIT				
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definición de la arquitectura de información: (PO3)	
Descripción Hallazgo:				
PO3 Determinar la Dirección Tecnológica R1 El plan de infraestructura tecnológica se encuentra completo pero no actualizado. R2 Se lleva un control y una actualización del plan de infraestructura tecnológico, pero no está documentada. R3. No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware de la red de datos de Emssanar E.S.S. R4.Existe un inventario actualizado del hardware de comunicaciones, pero no se encuentra documentado. R5.Se toma en cuenta el impacto de los cambios de actualización o mejora en el plan de infraestructura tecnológica, pero no está totalmente documentados				
Probabilidad : alta		**Impacto: moderado**		
Nivel de Riesgo: importante				
Consecuencia:				
El plan de infraestructura tecnológica es importante tenerlo actualizado ya que permite tener una visión más completa de las metas que se quieren alcanzar a nivel de las tic y de la empresa, el no hacerlo dificulta estas tareas. El control y actualización del plan de infraestructura es importante tenerlo documentado ya que esto facilita el logro de las metas propuestas, llevando un registro de las mismas y su avance. El no realizar simulacros a las fallas que pueden presentar tanto el software como el hardware de la red de datos de Emssanar E.S.S, hace más difícil la solución de las fallas cuando se presenten, ya que no se tiene una idea practica de costos, materiales necesarios y el tiempo que se tardaría en solventar dichas fallas. No llevar un inventario actualizado y documentado del software de comunicaciones de la red de datos de Emssanar E.S.S, dificulta el control de la red de datos, la seguridad, perdidas de equipos, recursos obsoletos y recursos necesarios de actualización y mantenimiento. El no documentar los cambios o mejoras al plan de infraestructura tecnológica, dificulta el logro de los mismos e impide determinar y difundir entre las partes interesadas, lo referente a estos procesos de mejoramiento tecnológico de la empresa.				
Recomendaciones:				
Actualizar el plan de infraestructura tecnológica de la red de datos de Emssanar E.S.S, periódicamente, para lograr alcanzar de mejor manera las metas propuestas de la empresa a nive tecnológico. Documentar el plan de infraestructura tecnológica de la red de datos, ya que de esta forma se lleva un registro del avance del mismo. Realizar simulacros de posibles fallas de software y hardware de la red de datos de Emssanar E.S.S, para estar preparados en caso de una falla real y saber si los procesos de contingencia planeados, son óptimos y eficaces en su desarrollo. Llevar un inventario documentado y actualizado del software de comunicaciones de la red de datos de EmssanarE.S.S, ya que de esta forma se puede tener un control sobre los recursos con los que se cuenta y lo que se necesita a futuro, y manejar de la mejor manera los recursos con los que se cuenta dentro de la empresa. Documentar los cambios o mejoras al plan de infraestructura tecnológica, para así tener una mejor visión del logro de los mismos facilitar su difusión entre las partes interesadas, en cuanto a lo referente a estos procesos de mejoramiento tecnológico que desarrolla la empresa Emssanar E.S.S.				
Evidencias:				
Anexocarpeta:Información Suministrada por Emssanar E.S.S/INFRAESTRUCTURA Y SOPORTE /Procedimiento planeación de infraestructura y soporte tecnológico.pdf No se lleva registro de simulacros de posibles fallas de software y hardware de la red de datos de Emssanar E.S.S. Anexo inventario.				

Cuadro 14. Cuadro de hallazgos PO4.

Emssanar ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. PO4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definición de los procesos, la organización y las relaciones de TI (PO4)
Descripción Hallazgo:			
PO4 Definir los procesos, la organización y las relaciones de TI R6. El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable. R7 Existen prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, pero no está documentada ni se lleva un registro. R8 En caso de falta del personal clave en la parte de Redes de datos EMSSANAR E.S.S, no se tiene planes de contingencia para su reemplazo en caso de ausencia O no está documentado.			
Probabilidad : medio		**Impacto: alto**	
Nivel de Riesgo:			
Importante			
Consecuencia:			
El no tener actualizado el manual de funciones del personal del área de sistemas, periódicamente, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable; provoca sobrecargas laborales, confusión en lo que deben hacer los funcionarios, cuáles son sus funciones y responsabilidades de su cargo, provocando así una barrera para el logro de los objetivos de la empresa Emssanar E.S.S. El no documentar y llevar registro de las practicas que tiene la empresa Emssanar E.S.S, para supervisar los roles y las responsabilidades de las funciones del personal se ejerzan de forma apropiada, provoca deficiencias en la mejora continua de la empresa Ya que no se evalúa a los funcionarios de la organización de Emssanar E.S.S. El no tener un plan de contingencia documentado para el reemplazo del personal clave en la parte de Redes de datos de Emssanar E.S.S, en caso de ausencia, hace que cuando se presente un caso de este tipo, existan traumatismos en cuanto su reemplazo y su acoplamiento al manejo de la red de datos.			
Recomendaciones:			
Actualizar el manual de funciones del personal del área de sistemas de forma periódica con sus respectivas funciones, descripción de cargo y requerimientos, del personal responsable. De esta manera los funcionarios de la Empresa Emssanar E.S.S conocerán cuáles son sus funciones, sus responsabilidades y se enfocaran sobre ellas, y se mejorara la eficiencia en las mismas, y el logro de objetivos de la empresa. Documentar y llevar registro de las prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, para así evaluar el desempeño y las mejoras que se puedan presentar en caso de fallas, o debilidades encontradas, dentro de la Empresa Emssanar E.S.S. Tener planes de contingencia para el reemplazo del personal clave en la parte de Redes de datos en Emssanar E.S.S, para así evitar contratiempos, en cuanto al reemplazo y demoras en el sistema de la red de datos.			
Evidencias:			
Anexos: Entrevistas y Checklist/entrevistas diego bastidas.docx. No se entregó manual de Funciones, aunque se dijo que si existía. Anexo Carpeta: Información Suministrada por Emssanar E.S.S/INFRAESTRUCTURA Y SOPORTE /Manuales/Manual de plataforma Tecnológica.pdf No tiene en cuenta el reemplazo del personal clave en el área de sistemas, en caso de que sea necesario realizar este procedimiento.			

Cuadro 15. Cuadro de hallazgos PO9.

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. PO9**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Evaluación y administración de los riesgos de TI (PO9)
Descripción Hallazgo:			
PO9 Evaluar y administrar los riesgos de TI R10 No se tiene actualizado ni documentado el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S R11. El plan de seguridad informática no se encuentra debidamente documentado. R12 no se cuenta con pólizas de seguros para el manejo del riesgo.			
Probabilidad :alto		**Impacto: moderado**	
Nivel de Riesgo:			
Importante			
Consecuencia:			
El no tener actualizado ni documentado el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S, ocasiona traumatismos en la toma de decisiones, en la forma de priorizar los activos y los controles necesarios para salvaguardarlos en caso de amenaza o riesgos potenciales. El no tener debidamente documentado el plan de seguridad informática ocasiona retrasos en recuperación del sistema, demoras en el tiempo de respuesta, costos adicionales o no presupuestados, perdida de activos importantes dentro de la Empresa E.S.S. El no tener pólizas de seguros para el manejo del riesgo. Provoca que se tengan que asumir costos no presupuestados, gastos adicionales para el manejo de accidentes o daños de los elementos y personas que operan en el área de sistemas de Emssanar E.S.S			
Recomendaciones:			
Actualizar y documentar el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S, ya que de esta manera se garantiza que los activos de la empresa estén correctamente valorados, protegidos y salvaguardados de acuerdo a su importancia y de acuerdo con los riesgos a los que se ven expuestos. Documentar el plan de seguridad informática, para evitar retrasos en el tiempo de respuestas, tener en claro el costo, tiempo y recursos necesarios en caso de pérdida o intrusión de agentes externos a la empresa Emssanar E.S.S y así lograr evitar tomar riesgos y retrasos innecesarios. Obtener pólizas de seguros para el manejo del riesgo, tanto para personal como para elementos de la Empresa Emssanar E.S.S, para así tener un respaldo en caso de accidentes fortuitos que se puedan presentar dentro de la empresas Emssanar E.S.S.			
Evidencias:			
Anexo Carpeta: Inf. Suministrada por Emssanar E.S.S/INFRAESTRUCTURA Y SOPORTE /Manuales/Manual de plataforma Tecnológica.pdf Se cuenta con una matriz de riegos, pero no se tiene definido un plan de evaluación de riesgos, ni tampoco un plan de seguridad informática bien definido.			

Cuadro 16. Cuadro de hallazgos AI.

Emssanar E.S.S. ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. AI**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Adquisición Y Mantenimiento (AI)	**Proceso:**	Adquisición Y Mantenimiento (AI)
Descripción Hallazgo:			
R13 las políticas para la adquisición de equipos hardware de la Red de datos de EMSSANAR E.S.S, no está completamente documentadas.			
Probabilidad :medio		**Impacto: alto**	
Nivel de Riesgo:			
Importante			
Consecuencia:			
El no tener completamente documentadas las políticas para la adquisición de equipos hardware de la Red de datos de EMSSANAR E.S.S. provoca que al adquirir nuevos elementos de red se incurra en errores que se pueden evitar teniendo un adecuado control del proceso de adquisición de elementos de red, sus características, sus especificaciones, y garantías.			
Recomendaciones:			
Documentar las políticas de adquisición de equipos hardware de la red de datos de Emssanar E.S.S, para de esta manera poder controlar los riesgos que se puedan presentar en este proceso de adquisición.			
Evidencias:			
Anexo Carpeta: Información Suministrada por Emssanar E.S.S/INFRAESTRUCTURA Y SOPORTE /Procedimientos/1 Procedimiento Planeación de Infraestructura y Soporte Tecnologico.pdf. El plan que se tiene es muy general debería ser más específico para cada elemento informático, haciendo énfasis en costos, en proveedores, especificaciones. Etc.			

Cuadro 17. Cuadro de hallazgos DS2.

	**Hallazgos**	**Ref. DS2**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y Soporte(DS)	**Proceso:**	DS2 Administración de servicios prestados por terceros
Descripción Hallazgo:			
R14 Falta simulacros, referentes a un posible cambio de servicios de red adquiridos con terceros			
Probabilidad :Media		**Impacto: Alto**	
Nivel de Riesgo:			
Moderado			
Impacto:			
El no llevar a cabo simulacros de cambio de proveedores de servicios, conlleva a que se mantenga una incertidumbre ya que en caso de la falta del servicio, bien sea por motivos económicos o legales no se tiene una evaluación del impacto real que tendría en la red de datos de Emssanar. El no llevar a cabo simulacros de cambio de proveedores de servicios crea dependencia hacia un proveedor externo, dependencia que puede repercutir en costos o deficiencia del servicio prestado.			
Recomendaciones:			
Realizar simulacros periódicos para evaluar un posible cambio de proveedor y documentar los resultados.			
Evidencias:			
No existe un plan de simulacro en el caso de cambiar de proveedores de servicios de red, no documentado.			

Cuadro 18. Cuadro de hallazgos DS2.1

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS2**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte (DS)	**Proceso:**	DS2 Administración de servicios prestados por terceros.
Descripción Hallazgo:			
R15 No se lleva un registro documentado de inconvenientes fallas o deficiencias con la prestación de los servicios de red que presta EMSSANAR E.S.S, que puede afectar la seguridad lógica y física de la red de datos			
Probabilidad :alta		**Impacto: medio**	
Nivel de Riesgo:			
Moderado			
Consecuencia:			
El no llevar un registro documentado de los inconvenientes fallas o deficiencias de los servicios de red prestados por terceros se constituye en una debilidad para los administradores de la red, ya que el no llevar un registro hace que las fallas o deficiencias no se han corregidas antes de que sucedan. El no llevar un registro documentado de los inconvenientes, fallas o deficiencias de los servicios de red prestados por terceros también provoca ineficiencia en la administración ya que se puede estar presentando la misma falla una y otra vez sin ser corregida de manera terminal.			
Recomendaciones:			
Llevar un registro de las fallas o anomalías para mantener un control de los servicio. Mantener registro documentado que ayuda a controlar mejor los servicios ya que se pueden tomar medidas correctivas de manera más exhaustiva si el problema persiste o se presenta continuamente.			
Evidencias			
No existe un registro de fallas o anomalías de servicios prestados por terceros, no documentado.			

Cuadro 19. Cuadro de hallazgos DS2.2 administración de servicios prestados por terceros

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS2**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte (DS)	**Proceso:**	DS2 Administración de servicios prestados por terceros
Descripción Hallazgo:			
R16 Se ha pensado en cambiar los servicios de red adquiridos por: diseño lógico de la red, ya que presenta fallas o debilidades por la falta de segmentación de la red.			
Probabilidad :baja		**Impacto: medió**	
Nivel de Riesgo:			
Tolerable			
Impacto:			
Un diseño lógico incorrecto de la red ocasiona una carga de trabajo extra para el administrador ya que es él quien tiene que controlar todo lo que sucede en la red, además el mal diseño lógico puede ocasionar un riesgo en su seguridad pues los atacantes pueden utilizar esta debilidad para atacar la red. Al no estar debidamente segmentada la red de datos de Emssanar E.S.S, se pueden presentar más tráfico y colisiones que provocan demoras y retrasos en el buen funcionamiento de la Red de Emssanar E.S.S.			
Recomendaciones:			
En el momento de contratar los servicios de red prestados por terceros revisar de manera concienzuda el diseño lógico de la red, de manera especial lo referente al número de equipos que se podrán conectar a la red y la segmentación de red que utilizaran. Segmentar la red de datos de Emssanar E.S.S, en las diferentes áreas y sedes en que esta hace presencia, para mejorar en seguridad y aislar el tráfico entre segmentos de la red, como también lograr más ancho de banda por usuario mediante la creación de dominios de colisión más pequeños.			
Evidencias			
Anexo listado de Ips.			

Cuadro 20. Cuadro de hallazgos DS4

	**Hallazgos**	**Ref. DS4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS4 Asegurar continuidad del servicio.**
Descripción Hallazgo:			
R17Los planes de contingencia en caso de ataques físicos y lógicos de la red de datos de EMSSANAR E.S.S, no se encuentran documentados.			
Probabilidad :media		**Impacto: alto**	
Nivel de Riesgo:			
Importante.			
Impacto:			
El plan de contingencia garantiza que en caso de ataques físicos o lógicos a la red la empresa continúe prestando un servicio sin necesidad de parar sus operaciones, el no tener un pan de contingencia documentado crea un ambiente de inestabilidad en caso de emergencia. El no llevar un plan de contingencia documentado que en caso de ataques físicos o lógicos a la red aumenta la carga de trabajo sobre el administrador de la red ya que en caso de ataques la responsabilidad recae en el y su equipo de trabajo. El no llevar un plan de contingencia documentado en caso de ataques físicos o lógicos a la red provoca que los usuarios no tengan conocimiento de los pasos que deben seguir para evitar un mayor daño y al contrario podrían realizar procesos que aumentarían el riesgo.			
Recomendaciones:			
Llevar un plan de contingencia documentado en caso de ataques físicos o lógicos a la red de datos. Socializar entre los usuarios dicho plan de contingencia. Mantener una evaluación constante del plan de contingencia. Realizar capacitaciones para los usuarios de la red, para enseñar la manera de utilizar el plan de contingencia.			
Evidencias			
No existe un plan de contingencia en caso de ataques físicos o lógicos a la red documentado.			

Cuadro 21. Cuadro de hallazgos DS4.1 asegurar continuidad del servicio

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS4 Asegurar continuidad del servicio.**
Descripción Hallazgo:			
R18 .No se realizan simulacros de ataques físicos o lógicos de la red de datos.			
Probabilidad :Alta		**Impacto: Medio**	
Nivel de Riesgo:			
Importante.			
Impacto:			
La no realización de los simulacros de ataques físicos o lógicos a la red crea un ambiente de seguridad inestable ya que puede ser que se esté trabajando en una red insegura sin tener conocimiento de esto. La no realización de los simulacros de ataques físicos o lógicos a la red no proporciona datos de evaluación de los sistemas de seguridad, evaluación que puede ayudar a detectar posibles anomalías en la red. Pueden existir debilidades en la parte física o lógica que pueden ser utilizadas por personal mal intencionado los cuales pueden causar daño o espionaje a la red atreves de estos puntos fallas que solo se descubrirían realizando los simulacros de ataques.			
Recomendaciones:			
Realizar un plan documentado de simulacro de ataques físicos y lógicos a la red teniendo en cuenta el tipo de ataque que se realiza, el software que utilizara y el área evaluada. Documentar los hallazgos encontrados. Hacer una evaluación de los simulacros realizando una comparación, de manera que se compare si los posibles hallazgos encontrados fueron reparados o no sean realizadas las correcciones pertinentes.			
Evidencias			
No existe un plan de simulacros de ataques físicos o lógicos documentados.			

Cuadro 22. Cuadro de hallazgos DS4.2 continuidad del servicio

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS4 Asegurar continuidad del servicio**
Descripción Hallazgo:			
R19. El acceso a internet no se encuentra restringido.			
Probabilidad :Alta		**Impacto: Medio**	
Nivel de Riesgo:			
Importante.			
Impacto:			
Se puede acceder a páginas que contengan virus e infectar los equipos de cómputo. Se pone en riesgo la red ya que existen páginas demasiado riesgosas en internet a través de las cuales personal mal intencionado podría ocasionar daños a la red de datos de Emssanar. Sin el conocimiento necesario los usuarios podrían ingresar a páginas sin restringir y descargar programas infecciosos que dañarían el equipo ocasionando demora en los procesos y sobrecarga de trabajo para el área de sistemas.			
Recomendaciones:			
Implementar filtros de contenidos que permitan bloquear el acceso a páginas web cuya dirección contenga un determinado patrón o el propio contenido de la página web contenga determinadas palabras. Actualizar las bases de datos del firewall para bloquear accesos a páginas que deben ser restringidos como facebook.			
Evidencias			
Imagen_facebook ,imagen_sin_filtro.			

Cuadro 23. Cuadro de hallazgos DS4.3

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS4 Asegurar continuidad del servicio**
Descripción Hallazgo:			
R18.1El diagrama de la red de datos de Emssanar E.S.S no se encuentra actualizado.			
Probabilidad :Alta		**Impacto: Medio**	
Nivel de Riesgo:			
Importante.			
Impacto:			
No se tiene un diagrama de red de datos actualizado que muestre la cantidad de equipos conectados a la red, provoca inseguridad ya que puede haber equipos sin control del administrador. El no tener un diagrama de la red de datos de Emssanar E.S.S actualizado llena de sobrecarga de trabaja al administrador de la red ya que debe mantener constante vigilancia del tipo lógica y física para evitar equipos intrusos. En caso de cambio de personal en el área de sistemas la falta de un diagrama de red actualizado crearía una mayor dificultad de adaptación, traumatismo y dificultad en el acoplamiento para el nuevo personal.			
Recomendaciones:			
Actualizar el plano de red. Documentar el plano de red. Socializar el plano de red entre todos los miembros del área de sistemas.			
Evidencias			
Anexo imagen_red_de datos.			

Cuadro 24. Cuadro de hallazgos DS4.4

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS4**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS4 Asegurar continuidad del servicio**
Descripción Hallazgo:			
R19 Existen políticas para el uso de los computadores conectados a la red de Emssanar, pero no están documentadas.			
Probabilidad :alta		**Impacto: bajo**	
Nivel de Riesgo:			
Moderado.			
Impacto:			
El no documentar las políticas para el uso de los equipos conectados la red crea independencia en los usuarios dejando que estos utilicen los equipos según su nivel de conocimientos, generando un riesgo de mal manejo posibilitando un ataque de ingeniería social. También puede generar desconocimiento por parte de los usuarios que podrían instalar software no autorizado generando riesgo en los equipos y por lo tanto en la red de datos. El no documentar las políticas de uso de los equipos puede convertirse en motivo de escusa en caso de daño de un equipo pues el usuario puede defenderse diciendo que no tenía conocimiento sobre lo que estaba haciendo mal. Los ataques del tipo lógico utilizan esta falta de conocimiento para ingresar a los equipos vulnerables y luego utilizar esos equipos para atacar la red de datos.			
Recomendaciones:			
Documentar las políticas para el uso de los equipos de cómputo en el cual se debe detallar que tipo de software puede ser utilizado, además de una clara normatividad que evite que los usuarios instalen software no autorizado o desconocido. Además en este documento de debe incluir la manera en que se deben utilizar el uso de discos extraíbles como memorias USB para evitar que la red sea puesta en riesgo por atacantes externos, ya que las memorias pueden ser portadoras de virus que no están en la red y de esta manera infectar el equipo y poner en riesgo la red.			
Evidencias			
No existe una política documentada para el uso de los equipos de cómputo por parte de los usuarios de Emssanar.			

Cuadro 25. Cuadro de hallazgos DS12

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS12**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS12: Administración de Instalaciones**.
Descripción Hallazgo:			
R20 En algunas sedes como la de recepción en la sede de la Aurora las oficinas o cubículos no son los adecuados para el área de computo.			
Probabilidad :media		**Impacto: bajo**	
Nivel de Riesgo:			
Tolerable.			
Impacto:			
El manejo de la red por parte del usuario es una parte fundamental a la hora de evitar riesgos o amenazas a la red del tipo físico o lógico. La comodidad hace parte de este uso un usuario puede dañar las conexiones de red si estas se encuentran mal ubicadas o expuestas al usuario, provocando daño en el equipo o daño en la conexión generando demora en la atención y sobrecarga de trabajo para los administradores de la red.			
Recomendaciones:			
Realizar el adecua miento de las zonas en las que se presentan los problemas mencionados especialmente los cubículos de recepción por donde pasa el cableado de la red.			
Evidencias			
Anexo Carpeta con imágenes de los cubículos.			

Cuadro 26. Cuadro de hallazgos DS12.1

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS12**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS12: Administración de Instalaciones**.
Descripción Hallazgo:			
R21 la parte de cableado de la red de datos (en las sedes de Emssanar) se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.			
Probabilidad :alta		**Impacto: medió**	
Nivel de Riesgo:			
Moderado.			
Consecuencia:			
El cableado fuera de las canaletas puede generar daños en la conexión, traumatismo que conllevaría a mala atención y sobrecarga de trabajo para los administradores quienes tendrían que buscar el punto de daño. El cableado suelto que se encuentra cerca de los usuarios de la red podría causar daños físicos al personal de Emssanar no solo los que están en los cubículos sino a los empleados que pasen por estas zonas. La existencia de cableado expuesto genera un punto de inseguridad en la red pues personas mal intencionadas podrían dañar el cableado o utilizar esos puntos para acceder a la red y realizar daños lógicos.			
Recomendaciones:			
Realizar la conexión y tendido del cableado en las sedes de acuerdo a la norma estándar ANSI/TIA/eia-568 y 569 para los ductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones. Mantener una revisión constante del cableado, canaletas y puntos de conexión en las sedes para evitar cableado fuera de la norma estándar. Documentar los puntos de cableado donde se está encontrando daños, para saber el motivo que lo provoca y verificar si en ese punto se está realizando un posible sabotaje de la red.			
Evidencias			
Anexo Carpeta con imágenes cableado.			

Cuadro 27. Cuadro de hallazgos DS12.2

Emssanar E.S.S ¡Siempre cerca de Usted!	**Hallazgos**	**Ref. DS12**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS12: Administración de Instalaciones**.
Descripción Hallazgo:			
R22 Existen prohibiciones para fumar, consumir alimentos y bebidas, pero falta suficientes carteles en lugares visibles.			
Probabilidad :baja		**Impacto: bajo**	
Nivel de Riesgo:			
Aceptable.			
Impacto:			
El consumir alimentos o bebidas cerca de los equipos puede causar daño de los equipos además de constituir un riesgo en la seguridad del tipo físico pues personas mal intencionadas pueden derramar bebidas sobre los equipos provocando además perdida de información.			
Recomendaciones:			
Aumentar el número de carteles en los lugares visibles, además de ser estrictos en cuanto al consumo de comida y bebidas cerca de los equipos. También se debe educar al personal para que no consuma comida cerca de los equipos y así prevenir deterioro de los mismos. Aumentar la señalización y seguridad cerca de los router y switch en las sedes especialmente aquellos que se encuentran con acceso cercano a los usuarios de Emssanar.			
Evidencias			
Anexo carpeta falta de señales de seguridad.			

Cuadro 28. Cuadro de hallazgos DS12.3

	**Hallazgos**	**Ref. DS12**	
Entidad Auditada:	EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S		
Área Auditada:	Sistemas	**Objeto de Estudio**	Sistemas Parte física y lógica de la Red de datos.
Responsables: DIEGO ACOSTA Y HEIDER QUETAMA CAICEDO			
Material de Soporte: COBIT			
Dominio:	Entrega y soporte(DS)	**Proceso:**	**DS12: Administración de Instalaciones**.
Descripción Hallazgo:			
R27 No se Realizan simulacros con la planta eléctrica o reguladores UPS.			
Probabilidad :media		**Impacto: alto**	
Nivel de Riesgo:			
Importante			
Impacto:			
Los reguladores tipo UPS adjuntados a cada equipo han sido previamente configurados para que estos provean de energía cuando exista suspensión del servicio eléctrico, pero no se han realizado simulacros para saber concretamente si su funcionamiento será correcto. La falta de simulacros evitan tener la plena seguridad de que estos cumplen con su función la que es de proveer de energía cuando exista suspensiones de luz., sin su correcto funcionamiento se puede tener pérdida de productividad e información importante y necesaria para Emssanar y sus usuarios.			
Recomendaciones:			
Realizar un plan de simulacro de las plantas eléctricas UPS en el cual se tenga en cuenta, tiempo de carga de las baterías configuración y cantidad de equipos que debería respaldar. Documentar los posibles hallazgos, fallas o debilidades que se encuentren en el simulacro.			
Evidencias			
No existe un plan de simulacro para probar el correcto funcionamiento de las UPS.			

2.3 RESULTADOS DE LA AUDITORÍA Y NIVEL DE MADUREZ.

A continuación se presentan los resultados definitivos de la auditoría y las recomendaciones de mejoramiento por cada proceso COBIT auditado, una vez revisadas las observaciones y aclaraciones hechas al grupo auditor.

2.3.1 Dominio: Planeación y Organización (PO).

Proceso: Definición de la arquitectura de información: (PO3)

Objetivo de Control: PO3.2 Plan de infraestructura tecnológica

Dictamen: Nivel de madurez 3 La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado, aunque no se encuentra actualizado. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología.

Hallazgos que soportan el dictamen: Existe un Plan de infraestructura tecnológica pero es del año 2011, por lo que se hace necesario su actualización.

No se documenta los cambios o mejoras al plan de infraestructura tecnológica de Emssanar E.S.S.

Recomendación: Actualizar el plan de infraestructura tecnológica de la red de datos de Emssanar E.S.S, periódicamente, para lograr alcanzar de mejor manera las metas propuestas de la empresa a nivel tecnológico.

Documentar el plan de infraestructura tecnológica de la red de datos, ya que de esta forma se lleva un registro del avance del mismo.

Documentar los cambios o mejoras al plan de infraestructura tecnológica, para así tener una mejor visión del logro de los mismos facilitar su difusión entre las partes interesadas, en cuanto a lo referente a estos procesos de mejoramiento tecnológico que desarrolla la empresa Emssanar E.S.S.

Proceso: **Definición de los procesos, la organización y las relaciones de TI (PO4).**

Objetivo de Control: Definir los procesos, organización y relaciones de TI

Dictamen: Nivel de madurez 2 Repetible pero intuitiva ya que la función de TI está organizada para responder de forma táctica aunque de forma inconsistente a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica.

Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores. No presenta documentación completa y actualizada de roles y funciones de los empleados y administradores del área de sistemas.

Hallazgos que soportan el dictamen: El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.

Existen prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, pero no está documentada ni se lleva un registro. En caso de falta del personal clave en la parte de redes de datos EMSSANAR E.S.S, no se tiene planes de contingencia para su reemplazo en caso de ausencia, no está documentado.

Recomendación: Actualizar el manual de funciones del personal del área de sistemas de forma periódica con sus respectivas funciones, descripción de cargo y requerimientos, del personal responsable. De esta manera los funcionarios de la Empresa Emssanar E.S.S conocerán cuáles son sus funciones, sus responsabilidades y se enfocaran sobre ellas, y se mejorara la eficiencia en las mismas, y el logro de objetivos de la empresa.

Documentar y llevar registro de las prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, para así evaluar el desempeño y las mejoras que se puedan presentar en caso de fallas, o debilidades encontradas, dentro de la Empresa Emssanar E.S.S.

Tener planes de contingencia para el reemplazo del personal clave en la parte de Redes de datos en Emssanar E.S.S, para así evitar contratiempos, en cuanto al reemplazo y demoras en el sistema de la red de datos.

Proceso: Evaluación y administración de los riesgos de TI (PO9)

Objetivo de Control: Evaluar y administrar los riesgos de TI.

Dictamen: Nivel de madurez 1 Inicial, ya que los riesgos de TI se toman en cuenta de manera ad hoc, al momento en que se requieran. Se realizan evaluaciones informales de riesgos en el área de sistemas de Emssanar E.S.S.

Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.

Hallazgos que soportan el dictamen: No se tiene actualizado ni documentado el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S

El plan de seguridad informática no se encuentra debidamente documentado.

No se cuenta con pólizas de seguros para el manejo del riesgo.

Recomendación: Actualizar y documentar el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S, ya que de esta manera se garantiza que los activos de la empresa estén correctamente valorados, protegidos y salvaguardados de acuerdo a su importancia y de acuerdo con los riesgos a los que se ven expuestos.

Documentar el plan de seguridad informática, para evitar retrasos en el tiempo de respuestas, tener en claro el costo, tiempo y recursos necesarios en caso de pérdida o intrusión de agentes externos a la empresa Emssanar E.S.S y así lograr evitar tomar riesgos y retrasos innecesarios.

Obtener pólizas de seguros para el manejo del riesgo, tanto para personal como para elementos de la empresa Emssanar E.S.S, para así tener un respaldo en caso de accidentes fortuitos que se puedan presentar dentro de la empresa Emssanar E.S.S.

2.3.2 Dominio: Adquisición Y Mantenimiento (AI).

Proceso: Adquisición y Mantenimiento de la infraestructura tecnológica.

Objetivo de Control: Adquirir y Mantener la infraestructura tecnológica.

Dictamen: Nivel de madurez 3 proceso definido: Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores.

El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento del área de Sistemas de Emssanar E.S.S. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.

Hallazgos que soportan el dictamen: Aunque existen modelos para la adquisición de elementos informáticos, las políticas para la adquisición de equipos hardware de la red de datos de EMSSANAR E.S.S, no está completamente documentada.

Recomendación: Documentar las políticas de adquisición de equipos hardware de la red de datos de Emssanar E.S.S, para de esta manera poder controlar los riesgos que se puedan presentar en este proceso de adquisición.

2.3.3 Dominio: Entrega de servicios y soporte.

Proceso: DS2 Administración de servicios prestados por terceros

Objetivo de Control: Administración de Riesgos del Proveedor.

Dictamen: Nivel de madurez 1 Inicial La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de

contratos. Los procesos siguen un patrón regular o estándar; pero no se ha documentado suficientemente

Hallazgos que soportan el dictamen: No existe un registro de fallas o anomalías de servicios prestados por terceros, no documentado.

No existe un plan de simulacro en el caso de cambiar de proveedores de servicios de red, no documentado.

Recomendación: El Administrador de la red debe realizar identificación adecuada de los riesgos que conllevaría el cambio de proveedores, sugerir a las directivas gestionar los planes de contingencia y documentar los planes.

Proceso: DS4 asegurar continuidad del servicio.

Objetivo de Control: Planes de continuidad de TI, pruebas del plan de continuidad, recuperación y reanudación de los servicios de TI, revisión post reanudación.

Dictamen: nivel de madurez 2 Repetible pero intuitivo. Se asigna la responsabilidad para mantener la continuidad del servicio los enfoques para mantener la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, La eficiencia y eficacia depende en gran parte del conocimiento y profesionalismo de los empleados.

Hallazgos que soportan el dictamen: No existe un plan de simulacros de ataques físicos o lógicos a la red, no están documentados, El acceso a internet no se encuentra restringido, los planos de red no están actualizados, no existe una política documentada para el uso de los equipos de cómputo por parte de los usuarios de Emssanar.

Recomendación: El Administrador de la red debe realizar identificación adecuada de los riesgos que ocasionaría un ataque físico o lógico a la red, realizar un plan de simulacros gestionando responsabilidad y evaluando el tiempo y esfuerzo que

requiere retomar la continuidad del servicio. Documentar y dar a conocer el plan de simulacros a la gerencia para su posterior puesta en práctica.

Actualizar el plano de red y restringir el acceso a internet con la utilización de software para filtrar las paginas no autorizadas por la entidad.

Proceso: DS 12 administración de las instalaciones

Objetivo de Control: Medidas de seguridad física. Definir e implementar medidas de seguridad física, las medidas deben incluir pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

Dictamen: nivel de madurez 3 Definido. Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad.

Hallazgos que soportan el dictamen: En algunas sedes como la de recepción en la sede de la Aurora las oficinas o cubículos no son los adecuados para el área de cómputo.

Recomendación: El administrador de la red a través de sus asistentes y colaboradores debe gestionar la correcta instalación del cableado, eliminar elementos inadecuados e informar a la gerencia la necesidad de adquirir elementos nuevos como mesas y escritorios para los equipos de cómputo, velando no solo por el servicio de red sino que además por la satisfacción de los usuarios.

Proceso DS12 administración de las instalaciones

Objetivo de Control: Protección contra factores ambientales.

Dictamen: 3 Definido se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad.

Hallazgos que soportan el dictamen: la parte de cableado de la red de datos (en las sedes de Emssanar) se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido. Existen cables en el suelo que estorban a los usuarios, Existen en el techo de las salas cables sueltos.

Recomendación: El Administrador de la red de datos debe realizar adecuar de manera correcta de acuerdo a las normas el tendido de red, cubrir, desinstalar las conexiones que generen riesgo a los usuarios, garantizar que se cumpla con los estándares de cableado estructurado.

Proceso: DS 12 administración de las instalaciones

Objetivo de Control: administración de instalaciones físicas

Dictamen: Nivel de madurez 3 Definido. Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad.

Hallazgos que soportan el dictamen: Existen prohibiciones para fumar, consumir alimentos y bebidas, pero falta suficientes carteles en lugares visibles.

Especialmente los de restricción que evite que las personas se acerquen a elementos importantes como lo son los routers o switch.

Recomendación: El administrador de la red debe informar la falta de señales y gestionar la adquisición de los elementos de señalización faltante.

Proceso: DS 12 administración de las instalaciones

Objetivo de Control: Suministro ininterrumpido de energía.

Dictamen: Nivel de Madurez 2 Repetible pero Intuitivo. Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos.

Hallazgos que soportan el dictamen: No se realizan simulacros con la planta eléctrica o reguladores UPS. No está documentado.

Recomendación: El Administrador de las aulas de informática debe realizar mantenimiento a las UPS realizar un plan de simulacro, donde se planee poner en funcionamiento las plantas eléctricas medir los resultados, documentar los resultados y socializarlos con la gerencia de tal manera que se tenga total conocimiento del funcionamiento de las plantas eléctricas.

3 PLAN DE MEJORAMIENTO

Con la realización de la auditoría se espera que se implemente un plan estratégico como el siguiente, mediante el cual se mitiguen los riesgos y amenazas en cuanto a la seguridad física y lógica de la red de datos de Emssanar E.S.S. y de esta manera asegurar la calidad del área de sistemas en la parte de la red de datos.

- El plan de mejoramiento debe mitigar los riesgos y asegurar los procesos del área de sistemas en cuanto a:

- Gestión de riesgos de hardware/físicos de la red de datos de la empresa Emssanar E.S.S.

- Documentar la gestión de la red de comunicaciones

- Documentación de planos de red de datos.

- Diseño de la red de datos en la entidad Emssanar E.S.S. (Documentación y segmentación en la red de datos).

Ejecución de pruebas y simulacros en cuanto a fallas físicas y lógicas de la red de datos para la verificación de la efectividad de los controles implantados para su mitigación, que den lugar a acciones correctivas, preventivas solidas en la búsqueda de la calidad y mejoramiento continuo de la entidad.

3.1 PLAN DE AUDITORÍA PROPUESTO

3.1.1 Plazo de implantación. Es importante tener en cuenta que hay acciones de mejora, cuyo alcance está totalmente definido y no suponen un esfuerzo excesivo, con lo que pueden realizarse de forma inmediata o a corto plazo. Por otro lado, existirán acciones que necesiten la realización de trabajos previos o de un mayor tiempo de implantación.

PLAZO
1 LARGO 2 MEDIO 3 CORTO 4 INMEDIATO

1 LARGO PLAZO: a un periodo de más de 5 años.

2 MEDIO PLAZO: más de un año y menos de 5 años.

3 CORTO PLAZO: periodo de un año.

4 INMEDIATO: un semestre.

3.1.2 Prioridad. Hace referencia sobre el orden de importancia de las acciones de mejora a ejecutar, alta, media y baja. Medida de acuerdo a la dificultad, el plazo y el impacto de las mismas.

PRIORIDAD **1 ALTA 2 MEDIA 3 BAJA**

1 PRIORIDAD ALTA: es importante tenerla en cuenta para el cumplimiento de los objetivos, afecta a varios elementos del plan de acción.

2 PRIORIDAD MEDIA: es un tanto importante tenerla en consideración en el plan de acción para cumplir los objetivos.

3 PRIORIDAD BAJA: su importancia es mínima a tenerla en cuenta, no afecta a varios elementos a la vez del plan de acción.

3.1.3 Impacto en la organización. Se define como impacto, el resultado de la actuación a implantar, medido por medio del grado de mejora conseguido. Es importante también tener en cuenta el grado de despliegue al que afecta la medida. Si ésta afecta a varias titulaciones su impacto será mayor y la prioridad también deberá serlo.

IMPACTO **1 BAJO (leve) 2 MEDIO (moderado) 3 ALTO (catastrófico)**

1 IMPACTO BAJO (leve): Si la ejecución de la acción de mejora provoca una mejora mínima en los objetivos propuestos.

2 IMPACTOMEDIO (moderado): Si la ejecución de la acción de mejora provoca una mejora considerable de los objetivos propuestos.

3 IMPACTOALTO (catastrófico): Si la ejecución de la acción de mejora provoca una mejora importante de los objetivos propuestos y evita riesgos catastróficos para la organización.

3.2 ACCIONES DE MEJORA

Nº	Acciones de mejora	Responsable	Plazo	prioridad	Impacto
1	Actualizar el plan de infraestructura tecnológica de la red de datos de Emssanar E.S.S, de forma periódica.	Ing. Diego Bastidas	largo	Media	moderado
2	Documentar el plan de infraestructura tecnológica de la red de datos.	Ing. Diego Bastidas	largo	media	moderado
Nº	**Acciones de mejora**	**Responsable**	**Plazo**	**prioridad**	**Impacto**
3	Realizar simulacros de posibles fallas de software y hardware de la red de datos de Emssanar E.S.S.	Ing. Diego Bastidas	corto	media	alto
4	Llevar un inventario documentado y actualizado del software de comunicaciones de la red de datos de Emssanar E.S.S.	Ing. Diego Bastidas	largo	media	moderado
5	Actualizar el manual de funciones del personal del área de sistemas.	Ing. Diego Bastidas	corto	media	alto
6	Tener planes de contingencia para el reemplazo del personal clave en la parte de Redes de datos en Emssanar E.S.S.	Ing. Diego Bastidas Ing. Harold Caicedo	largo	alto	alto
7	Actualizar y documentar el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S.	Ing. Diego Bastidas Ing. Harold Caicedo	largo	alto	alto
Nº	**Acciones de mejora**	**Responsable**	**Plazo**	**prioridad**	**Impacto**
8	Documentar el plan de seguridad informática.	Ing. Diego Bastidas Ing. Harold Caicedo	mediano	alto	alto

9	Documentar las políticas de adquisición de equipos hardware de la red de datos de Emssanar E.S.S.	Ing. Diego Bastidas Ing. Harold Caicedo	corto	media	alto
10	Realizar simulacros periódicos para evaluar un posible cambio de proveedor y documentar los resultados.	Ing. Diego Bastidas Ing. Harold Caicedo	mediano	media	alto
11	Llevar un registro de las fallas o anomalías en el área de sistemas en la parte de la red de datos.	Ing. Diego Bastidas	mediano	media	moderado
12	Segmentar la red de datos de Emssanar E.S.S, en las diferentes áreas y sedes de la empresa.	Ing. Diego Bastidas Ing. Harold Caicedo	largo	alto	alto
13	Llevar un plan de contingencia documentado en caso de ataques físicos o lógicos a la red de datos.	Ing. Diego Bastidas	corto	media	alto
Nº	**Acciones de mejora**	**Responsable**	**Plazo**	**prioridad**	**Impacto**
14	Realizar un plan documentado de simulacro de ataques físicos y lógicos a la red teniendo en cuenta el tipo de ataque que se realiza, el software que utilizara y el área evaluada.	Ing. Diego Bastidas	medio	alto	alto
15	Implementar filtros de contenidos que permitan bloquear el acceso a páginas web indebidas dentro de la organización. (Restringir facebook)	Ing. Diego Bastidas	medio	media	moderado
16	Actualizar, documentar y socializar el plano de red de datos de Emssanar E.S.S.	Ing. Diego Bastidas Ing. Harold Caicedo	largo	alto	moderado
17	Documentar las políticas para el uso de los equipos de cómputo de la red de datos.	Ing. Diego Bastidas Ing. Harold Caicedo	mediano	alto	bajo
Nº	**Acciones de mejora**	**Responsable**	**Plazo**	**prioridad**	**Impacto**
18	Realizar el adecua miento de las zonas en las que se presentan problemas en cuanto a la ergonomía de los cubículos de recepción por donde pasa el cableado de la red.	Ing. Diego Bastidas	mediano	media	moderado

19	Realizar la conexión y tendido del cableado en las sedes de acuerdo a la norma estándar ANSI/TIA/eia-568 y 569 para los ductos, pasos y espacios necesarios.	Ing. Diego Bastidas	largo	alta	moderado
20	Mantener una revisión constante del cableado, canaletas y puntos de conexión en las sedes para evitar cableado fuera de la norma estándar.	Ing. Diego Bastidas Ing. Harold Caicedo	mediano	alta	alto
21	Aumentar el número de carteles en los lugares visibles, además de ser estrictos en cuanto al consumo de comida y bebidas cerca de los equipos.	Ing. Diego Bastidas	corto	baja	moderado
22	Aumentar la señalización y seguridad cerca de los router y switch en las sedes especialmente aquellos que se encuentran con acceso cercano a los usuarios de Emssanar.	Ing. Diego Bastidas	corto	media	alto
23	Realizar un plan de simulacro de las plantas eléctricas UPS en el cual se tenga en cuenta, tiempo de carga de las baterías configuración y cantidad de equipos que debería respaldar.	Ing. Diego Bastidas	mediano	media	alto
24	Realizar una evaluación periódica que permita conocer el desempeño del área de sistemas en búsqueda del mejoramiento continuo.	Ing. Diego Bastidas Ing. Harold Caicedo	largo	alto	alto

El plan de mejoramiento propuesto no se implementara por parte de los auditores, sino que es responsabilidad exclusiva del administrador de la red de datos de Emssanar E.S.S, implementarlo para beneficio de la organización.

CONCLUSIONES

Con el desarrollo de este proyecto de grado se ejecutó la auditoria en lo referente a la seguridad de la parte física y lógica en la red de datos de la Empresa Solidaria de Salud Emssanar E.S.S, identificando los principales riesgos en cuanto a falencias del cableado estructurado, y en cuanto a la no segmentación de la red de datos, lo cual se presenta en las sedes de esta entidad de salud.

La auditoría de redes realizada siguió el estándar de auditoría COBIT, con entrevistas a los administradores, aplicación de cuestionarios y la utilización de software de intrusión kali Linux, con una de sus herramientas llamada METASPLOIT, logrando poner a prueba la seguridad física y lógica de la red de datos de la Empresa Emssanar E.S.S. Aunque la empresa Emssanar E.S.S se encuentra en la parte de sistemas bien coordinada y administrada, presenta riesgos importantes que deben ser tenidos en cuenta para obtener un rendimiento óptimo de sus recursos tecnológicos.

Con la realización de los cuestionarios cuantitativos de auditoría en Emssanar E.S.S se logró identificar los siguientes riesgos importantes en el estándar COBIT en procesos como: (PO4) Definir los procesos, la organización y las relaciones de TI,(PO9)Evaluación y administración de los riesgos de TI, Proceso (DS2) Administración de servicios prestados por terceros, Proceso (DS4) Asegurar continuidad del servicio, proceso (DS12)Administración de Instalaciones, DS12 Protección contra Factores Ambientales, entre otros.

La auditoría informática a la red de datos de Emssanar E.S.S, facilitó el diseño del plan de mejoramiento, el cual debe mitigar los riesgos y asegurar los procesos del área de sistemas en cuanto a: Gestión de riesgos de hardware/físicos de la red de datos de la empresa Emssanar E.S.S, documentar la gestión de la red de comunicaciones, documentación de planos de red de datos y el diseño de la red de datos en la entidad Emssanar E.S.S. (Documentación y segmentación en la red de datos).

La auditoría informática realizada a Emssanar E.S.S, es una poderosa herramienta para solucionar problemas, detectar probables riesgos y amenazas, en las empresas en general, siendo esto así, se deben tener en cuenta las recomendaciones de las auditorias ejecutadas y ejecutar periódicamente auditorias que evalúen y prueben la eficiencia y la optimización de sus sistemas de información y tecnología.

RECOMENDACIONES

De acuerdo a las principales falencias encontradas con respecto al hardware y al software dentro de Emssanar E.S.S con el desarrollo de este proyecto, se expone las siguientes recomendaciones:

- Actualizar el plan de infraestructura tecnológica de la red de datos de Emssanar E.S.S, periódicamente, para lograr alcanzar de mejor manera las metas propuestas de la empresa a nivel tecnológico.

- Documentar el plan de infraestructura tecnológica de la red de datos, ya que de esta forma se lleva un registro del avance del mismo.

- Realizar simulacros de posibles fallas de software y hardware de la red de datos de Emssanar E.S.S, para estar preparados en caso de una falla real y saber si los procesos de contingencia planeados, son óptimos y eficaces en su desarrollo.

- Llevar un inventario documentado y actualizado del software de comunicaciones de la red de datos de Emssanar E.S.S.

- Actualizar y documentar el plan de evaluación de riesgos del área de sistemas en la parte de redes de Emssanar E.S.S, ya que de esta manera se garantiza que los activos de la empresa estén correctamente valorados, protegidos y salvaguardados de acuerdo a su importancia y de acuerdo con los riesgos a los que se ven expuestos.

- Documentar el plan de seguridad informática, para evitar retrasos en el tiempo de respuestas, tener en claro el costo, tiempo y recursos necesarios en caso de pérdida o intrusión de agentes externos a la empresa Emssanar E.S.S y así lograr evitar tomar riesgos y retrasos innecesarios.

- Realizar el adecuado mantenimiento de las zonas en las que se presentan los problemas mencionados especialmente los cubículos de recepción por donde pasa el cableado de la red.

- Realizar la conexión y tendido del cableado en las zonas de acuerdo a los norma estándares **TIA/EIA 568-B-2, TIA/EIA 569-B, TIA/EIA 606A, TIA/EIA**

607 y TIA/EIA/TSB-67 para los ductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones.

- Mantener una revisión constante del cableado, canaletas y puntos de conexión en las sedes para evitar cableado fuera de la norma estándar.

- Actualizar el sistema operativo instalado en el servidor de Emssanar E.S.S migrar la versión 2003 a la última versión 2008.

- Segmentar la red de datos de Emssanar E.S.S para aumentar la seguridad de la red, dividiéndola por departamentos, municipios, sedes y oficinas de manera que un intruso en caso de ataque solo pueda tener acceso a una sola área de la empresa y no a toda la red de datos.

- Implementar el protocolo de Transferencia de Hiper-Texto (HTTPS) que es la versión segura del http (Hyper Text Transfer Protocool) ya que con este protocolo permite realizar transacciones de forma más segura.

- Implementar el plan de mejoramiento propuesto en este proyecto de auditoría a la red de datos de Emssanar E.S.S, en cuanto a: la gestión de riesgos de hardware/físicos de la red de datos, a su documentación y segmentación la red de datos de Emssanar E.S.S; ya que de esta manera se logra que esta empresa alcance un nivel óptimo de calidad a nivel de las tecnologías de información con el cual alcanzar sus metas y cumplir con su misión y visión.

- Llevar a cabo auditorías a la parte física y lógica de toda la red de datos periódicamente, para tener un análisis completo del nivel de eficiencia y eficacia que se maneja dentro de Emssanar E.S.S y así tomar las respectivas acciones de mejora que a su vez lleven a una mejora continua dentro de la organización.

BIBLIOGRAFÍA

ARCE Norma y TACURI Andrés, Auditoría física y lógica a las redes de comunicaciones de computadores de la fábrica pasamanería s.a. Cuenca Ecuador, 2010, 364 p. Trabajo de grado (Ing. De Sistemas).Universidad Politécnica Salesiana. Facultad De Ingenierías. Departamento de Sistemas.

CAICEDO, Liliana. ORDOÑEZ, Claudia. Técnicas de Auditoría de Sistemas Aplicadas al Proceso de Contratación y Páginas Web en Entidades Oficiales del Departamento de Nariño. Universidad de Nariño. 2010.

ECHENIQUE GARCÍA, José Antonio. Auditoría en Informática. 2 Edición. México: Mc Graw Hill, 2001.

ESTRADA, Oscar. Auditoría de Sistemas Aplicada al Sistema Integral de Información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto. Universidad de Nariño.2007

GUSTIN Edith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011.

NOGUERA, Laura y SANCHEZ Edy Yanira. Auditoría Informática en el Área de Sistemas e Indicadores de Funcionamiento del Hardware en la Empresa Solidaria de Salud Emssanar E.S.S. del Departamento de Nariño. Universidad de Nariño. 2012

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed, Alfa omega/RA-MA, México D.F, 2001.

WEBGRAFÍA

AHARON MatiI, COPPOLA William, Tutorial de Metasploit Framework de offensive-security, http://ns2.elhacker.net/timofonica/manuales/Manual_de_Metasploit_Unleashed.pdf . Consultado marzo 2014.

ANONIMO. Topología y redes. Topologías físicas y lógicas. Disponible en internet: http://topologiayredes.wordpress.com/tag/broadcast/ Consultado marzo 2014.

BLOG, Clasificación de los tipos de auditoría. http://myblog-bilky.blogspot.com/[Citado 13 de junio de 2012]

CANAVES. Mario. Auditoría informática. Disponible en internet: <http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml>. [Citado 16 de enero de 2012]

CATEDRAS INGENIERIA. Metodología de la auditoría informática. Disponible en internet: <http://www.ub.edu.ar/catedras/ingenieria/auditoría/tpmetodo/tpmetodo2.htm#p2-1-1>. Consultado: 5 de mayo de 2014.

CATARINA. Seguridad informática. Conceptos básicos. Disponible en internet: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf Consultado marzo 2014.

DEBIANHACKERS. Nmap: Escanner de puertos. Disponible en: http://www.debianhackers.net/nmap-escaner-de-puertos, Consultado marzo 2014.

DITUYI. Capa de red. Disponible en internet: http://www.dituyi.net/capa-de-red/ Consultado marzo 2014.

EMSSANAR E.S.S. Código de buen gobierno y ética de Emssanar, Colombia, 1991. 18.p. Disponible en internet: http://www.emssanar.org.co/contenidos/EPSEmssanar/RENDICION_DE_ CUENTAS /CODIGO_DE_BUEN_GOBIERNO_Y_ETICA.pdf.

FERNÁNDEZ Nubia. Importancia de la auditoría informática en las organizaciones, Disponible en internet: <http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica>. [Citado el 5 agosto de 2014]

FELLOWS, Russ. Copia de seguridad completa, incremental o diferencial: cómo elegir el tipo adecuado .Disponible en internet: http://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado Consultado marzo 2014.

GALLEGOS, Alex. Red de computadoras. Monografías. Disponible en internet: http://www.monografias.com/trabajos72/red-computadoras/red-computadoras.shtml Consultado marzo de 2014.

GOMESZ, Sebastián. Redes corporativas. Clasificación de las redes según su propiedad. Disponible en internet: http://sebastiangomezm.blogspot.com/2011/09/clasificacion-de-las-redes-segun-su_7508.html consultado marzo 2014.

HERNANDEZ, Jorge. Redes satelitales. Monografías. Disponible en internet: http://www.monografias.com/trabajos29/redes-satelitales/redes-satelitales.shtml. Consultado Marzo 2014.

KALI LINUX. Seguridad ofensiva limitada. Documentación Oficial kali Linux. Disponible en internet: http://www.kali.org/official-documentation/. Consultado: 20 de Enero de 2014.

LEONARDO, Camelo. Seguridad de la información en Colombia. Disponible en internet: http://seguridadinformacioncolombia.blogspot.com/2010/07/que-es-cobit.html. Consultado: 28 de Julio de 2010

MORGADO Gastby. Auditoría fiscal y auditoría. Disponible en internet:<http://www.monografias.com/trabajos16/auditoría-fiscal/auditoría-fiscal.shtml>. [Citado 11 de Febrero de 2008]

NOGUERA, Laura y SANCHEZ Edy Yanira. Auditoría informática en el área de sistemas e indicadores de funcionamiento del hardware en la Empresa Solidaria de Salud Emssanar E.S.S. del Departamento de Nariño. Universidad de Nariño. 2012.

PEREZ, Rafael. Redes e instalaciones. Clasificación de las redes. Disponible en internet: http://conocimientosdehoy.blogspot.com/2014/10/clasificacion-de-las-redes.html Consultado marzo 2014.

PEÑA, Katherine. Enrutadores inalámbricos. Monografías. Disponible en internet: http://www.monografias.com/trabajos72/enrutadores-inalambricos/enrutadores-inalambricos2.shtml Consultado marzo 2014.

PORTAL EDUCATIVO, TiposDe.org. Tipos de servidores. Disponible en internet: http://www.tiposde.org/informatica/131-tipos-de-servidores/ Consultado marzo 2014.

REDES LOCALES. Clasificación de las redes por método de conexión. Disponible en internet: https://sites.google.com/site/redeslocalesmaria/2-clasificacion-de-las-redes/por-metodo-de-conexion Consultado marzo 2014.

RIOS, Julio. Seguridad informática. Disponible en internet: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml Consultado marzo 2014.

SIMONELLI, Andreina. Fundamentos de la informática. Redes. Disponible en internet: http://fundamentosinformaticaunerg.blogspot.com/p/redes.html Consultado: marzo 2014.

TEXTOS CIENTIFICOS. Tcp/ip y el modelo osi. Disponible en internet: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi Consultado marzo 2014.

UAZUAY, Estudios. Vlans. Disponible en internet: http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf consultado marzo 2014.

UNICEN, Cátedras. El modelo osi. Disponible en internet: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf Consultado marzo 2014.

UNIVERSIDAD CESAR VALLEJO. Router y switch. Disponible en internet: http://es.slideshare.net/mcwilmermary/ucv-sesion-13-router1 Consultado marzo 2014.
[1]Ibíd., Consultado marzo 2014.

XDEXTECNOLOGIA. Cableado estructurado. Disponible en internet: blog2009/06/cableado-estructurado.htmlxdextecnologia.blogspot.com/ Consultado marzo 2014.

ANEXOS

Los anexos relacionados a continuación se entregan por medio magnético en CD y se adjuntan al presente informe.

ANEXO 1. Procedimiento planeación de infraestructura y soporte tecnológico.

ANEXO 2. Entrevistas Diego Bastidas.

ANEXO 3. Manual de plataforma Tecnológica.

ANEXO 4. Imágenes cableadas.

ANEXO 5. Falta de señales de seguridad.

ANEXO 6. Diagrama de red.

ANEXO 7. Entrevista seguridad lógica.

ANEXO 8. Imágenes cubículos.

ANEXO 9. Imágenes sin filtro.

ANEXO 10. Inventario de equipos de Emssanar.

ANEXO 11. Lista de chequeo.

ANEXO 12. Listado de Ips e imágenes.

ANEXO 13. Pruebas de intrusión.

ANEXO 14. Entrevistas y checklist.

ANEXO 15. Cobit marco teórico.

ANEXO 16. Manual de Funciones Emssanar E.S.S.