FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA RED DE LA ENTIDAD CYBER XPRESS DETECTANDO SUS FORTALEZAS Y DEFICIENCIAS.

Trabajo de Titulación presentado en conformidad a los requisitos

establecidos para optar por el título de

Tecnólogo en redes y telecomunicaciones

Profesor Guía

Ing. Rómulo Guerrero V.

Autor:

Byron Stalin Espin Mena

Año:

2013

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante BYRON ESPIN, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación.

_____

Rómulo Guerrero V.

Ingeniero en Electrónica y Telecomunicaciones

C.I = 0102702016

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, no se ha plagiado de ninguna parte, se han citado las fuentes correspondientes y en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes. Por lo cual dejo constancia de la dedicación y esfuerzo empleado para su realización.

_____

Byron Stalin Espin Mena

C.I = 1721519005

AGRADECIMIENTOS

Agradezco principalmente a Dios por darme la vida y a mis padres la motivación para realizar este trabajo, a mi madre Marcela Mena y mi padre Galo Espin por su apoyo incondicional a mi hermana por estar siempre cuando la necesite, en especial al Ing. Rómulo Guerrero por su apoyo, su paciencia y sus enseñanzas a lo largo de toda mi carrera.

DEDICATORIA

Este trabajo va dedico a las personas que siempre me apoyaron familia, amigos, compañeros y a los profesores que ayudaron a mi formación. Mención especial a las personas de mi familia que perdimos este año.

RESUMEN

Las tecnologías de la información son vitales y estas se basan en las redes de información las cuales son atacadas a diario por diferentes amenazas, por ello se quiere obtener un método aplicable en el cual se pueda identificar los riesgos en una infraestructura de red pequeña, la cual permitirá conocer las amenazas informáticas más comunes internas y externas que involucrará de forma general a una red pequeña como de un cyber.

En el capítulo 1 se conoce la composición del cableado estructural sus elementos, los tipos de cables, los estándares y topologías existentes.

Se describe los modelos de conexión de red OSI y TCP / IP. Se conoce la ubicación del establecimiento a realizar la auditoria y la legislación que lo rige en el Ecuador.

En el capítulo 2 se determina los conceptos sobre seguridad informática, los componentes físicos y lógicos de la red. Se detallan los delitos informáticos, tipos de ataques, los métodos de control y la legislación que los controla.

En el capítulo 3 se realiza un estudio de la red preventivo, se ejecuta la auditoria de seguridad a la red utilizando como herramienta auditable la norma ISO 27001. Partiendo de la verificación del funcionamiento de la red, empleando un monitoreo auditable del cual se obtiene los resultados presentados.

En el capítulo 4 se conoce las conclusiones y recomendaciones obtenidas. Como afecta el ambiente en el que se encuentran instalados los equipos al desempeño de estos, además proponer una alternativa para mejorar la operatividad de esta, permitiendo un cambio en su ubicación. Los beneficios que de esto se obtiene, permitirá establecer una respuesta concreta que mejore su desempeño y disminuya las probabilidades de ser atacada.

ABSTRACT

The information technologies are vital and these are based on information networks which are attacked daily by different threats, so you want to get an applicable method in which risks can be identified in a small network infrastructure, which will reveal the most common threats to internal and external generally involve a small network as a cyber.

In Chapter 1, we know the composition of its elements structured wiring, cabling types, standards and existing topologies.

The networking models OSI and TCP / IP. He knows the location of the facility to conduct the audit and legislation governing it in Ecuador.

Chapter 2 lays the concepts about computer security, physical and logical components of the network. Are detailed cybercrime, types of attacks, methods of control and the control law.

Chapter 3 is a study of the network preventive runs to safety audit as a tool auditable network using ISO 27001. Based on the verification on the performance of the network, using an audit monitoring which yields the results presented.

Chapter 4 is called the conclusions and recommendations obtained. How it affects the environment in which computers are installed to perform these also propose an alternative to improve the operability of this, allowing a change in placement. The benefits of this achieved, will establish a concrete answer to improve their performance and reduce the likelihood of being attacked.

INDICE

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

Este tema surge por el auge de las nuevas tecnologías y con el crecimiento de las redes es importante controlar las amenazas a las que se ve expuesta una red.

Con la necesidad de conocer un método que se pueda emplear, para identificar los riesgos en la infraestructura de red, las deficiencias y posibles amenazas de un cyber, tanto internas como externas.

El objetivo general:

Realizar una auditoría de seguridad informática para detectar fortalezas, deficiencias y las amenazas a la red del cyber XPRESS, sector Guamaní Maldonado (S-60).

Objetivos específicos:

- Utilizar una metodología que demuestre el estado de la seguridad de la red.
- Conocer mediante la ISO 27001 las diferentes amenazas que pueda tener la red.
- Determinar cuál son las principales causas por las cuales está siendo vulnerable la red.
- Establecer si el ambiente en el que se encuentran afecta la operatividad de los equipos.
- Analizar posibles soluciones a los problemas encontrados.

CAPÍTULO I

1 Cableado estructural y conectividad de red.

1.1 Conectividad de red.

La necesidad de compartir información da como resultado que se cree una comunicación.

Para obtener una comunicación entre dos o más elementos es necesario que se establezca una conexión entre los mismo utilizando las nuevas tecnologías. Así surge la conectividad entre dispositivos sin estar sujetos a un sistema central.

Con la visión y evolución de las nuevas tecnologías, aparición de topologías como *Ethernet IEEE 802.3, ARCNET, Token Ring, FDDI* y dispositivos como el repetidor, el puente, el ruteador y el switch, han permitido el gran crecimiento de las redes y por ende una mayor conectividad de los dispositivos.

1.1.1 Modelo de protocolo de control de transmisión / protocolo de internet TCP / IP.

El TCP / IP: (Protocolo de control de trasmisión / protocolo de internet). Este protocolo que trabaja en capas es el que permite que sean enviados los paquetes de datos 0 y 1 en una comunicación entre dos equipos de la misma o diferente red, garantizando la entrega y el orden con el que son enviados los datos, dividiendo estos paquetes en cuatro octetos de 8 bits.

Estos 32 bits son direcciones que permiten establecer el origen y el destino de los paquetes de datos. Ejemplo: 192.168.16.2

Este modelo consta de cuatro capas que tienen su origen el modelo OSI de siete capas, a pesar de tener su origen después del modelo OSI el TCP/IP es el más utilizado en el mundo.

Las cuatro capas de las que consta este modelo son:

1.1.1.1 Aplicación:

Especifica los protocolos de aplicación como HTTP, TELNET, DNS y como los programas se conectan a la capa de transporte, su referencia en OSI capa 5, 6 y 7. Es un nivel simple por medio del cual se encuentran aplicaciones con las cuales se accede a servicios de internet disponible.

1.1.1.2 Transporte:

Aprueba la conexión para transporte de datos de las capas de los host y conocer el nivel de servicio de la conexión, su referencia en OSI capa 4. Los paquetes enviados son los mismos en las capas del transmisor como del receptor. En esta capa el receptor se encarga de ordenar y unir la información para que quede igual a la original.

1.1.1.3 Internet:

Realiza enrutamiento en los paquetes de datos, empaquetando los mismos en datagramas con direcciones de origen y destino acepta una solicitud para enviar un paquete determinando si el paquete debe ser enviado o procesarse de manera local, su referencia en OSI capa 3 Red.

1.1.1.4 Interfaz de red:

Es la capa de nivel inferior en la cual se determina de forma detallada la manera en que los datos son enviados por el medio físico, es decir las señales eléctricas 0 y 1 binarios son enviadas por un medio como par trenzado, etc. Su referencia en OSI capa 1 y 2.

1.1.2 Modelo de interconexión de sistemas abiertos OSI.

Para detallar el funcionamiento de las redes y por ende del internet se desarrolló el modelo OSI el cual permite conocer como se establece la comunicación entre las redes teniendo en común el origen y transporte de datos por capas. Este es el estándar internacional para comunicaciones de red implementado por la ISO en la década de los 70.

Está formada por siete capas:

1.1.2.1 Aplicación:

“Sirve de ventana a los procesos de aplicación. Tiene en cuenta la semántica (significado) de los datos.

Funciones y servicios:

Servicios de directorio (Transferencias de archivos).

Manejo de correo electrónico.

Terminal virtual.” (Corletti. 2011. P. 30.)

Aquí se desarrollan las aplicaciones que interactúan con el usuario y los procesos con los cuales se obtiene acceso a los servicios de red.

1.1.2.2 Presentación:

Muestra datos al usuario de forma que este pueda entender la información que recibe de las capas inferiores, es decir traduce bits a lenguaje de usuario que es enviado a la capa aplicación.

1.1.2.3 Sesión:

Es la encargada de establecer sesiones, origina y finaliza estas entre los usuarios. Realiza las funciones que permiten a estos procesos comunicarse a través de la red.

1.1.2.4 Transporte:

Recibe los datos de las capas superiores se encargada de que los datos lleguen sin errores en secuencia y sin perdidas a la capa de red, para ello segmenta los datos en paquetes. Es el traductor de la red ya que transforma los datos que se pueden ver en un formato de capa aplicación a un formato común de estación emisora.

“Proporciona la capa presentación:

Traducción del código de carácter: por ejemplo, ASCII a EBCDIC.

Conversión de datos: bits de orden, punto flotante entero CR-CR/LF y así sucesivamente.

Compresión de datos: reduce el número de bits que deben ser transmitidos en la red.

Cifrado de datos: cifrar los datos por motivos de seguridad. Por ejemplo, el cifrado de contraseña.” (http://support.microsoft.com/kb/103884/es)

1.1.2.5 Red:

Controla el funcionamiento de los medios de la parte física de la red, para transferir secuencias de datos entre el origen y destino entre una o más redes mediante rutas. “Las rutas pueden ser basado en tablas estáticas, y rara vez cambia. También pueden ser determinadas al comienzo de cada conversación, por ejemplo, una sesión de terminal”. (A. S. Tanenbaum. (2003), pag 40).

1.1.2.6 Enlace:

Se determina errores en los paquetes de datos que provienen de la capa física, transmitiendo datos en la red y permitiendo que las capas superiores los reciban sin fallas.

- “Establecimiento y finalización de vinculo: establece y se termina el vínculo lógico entre dos nodos.
- Control de tráfico de trama: le indica al nodo transmisor que dé "marcha atrás" si no hay un búfer de trama disponible.
- Secuencia de tramas: transmite y recibe tramas secuencialmente.
- Confirmación de trama: proporciona/espera de confirmaciones de trama. Detecta y recupera de los errores que se producen en la capa física retransmitiendo tramas no reconocidas y controlando el recibo de tramas duplicados.
- Delimitación de la trama: crea y reconoce los límites de la trama.

- Comprobación de errores de trama: comprueba la integridad de las tramas recibidas
- Administración de acceso al medio: determina cuándo el nodo "tiene el derecho" utilizar el medio físico."

(http://support.microsoft.com/kb/103884/es)

1.1.2.7 Física:

Se establece, se modula y controla los datos a transmitir, además selecciona el medio físico por el cual se realiza la comunicación.

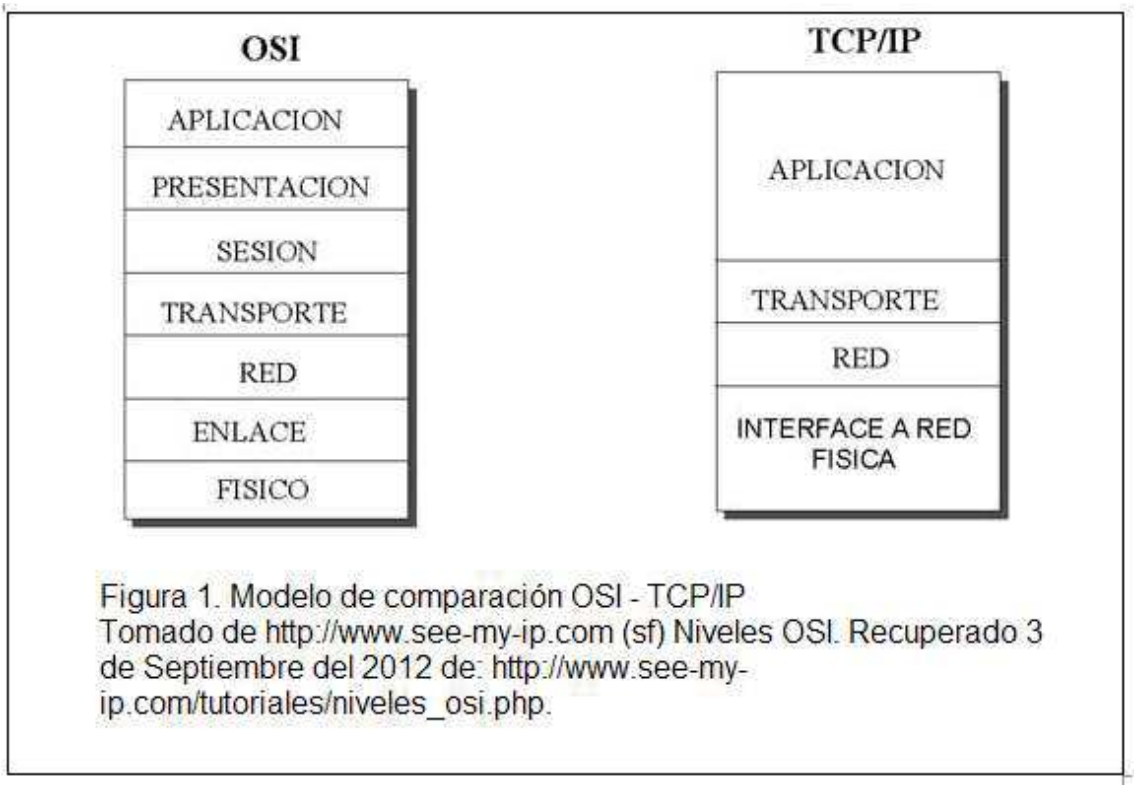


Figura 1. Modelo de comparación OSI - TCP/IP
Tomado de http://www.see-my-ip.com (sf) Niveles OSI. Recuperado 3 de Septiembre del 2012 de: http://www.see-my-ip.com/tutoriales/niveles_osi.php.

1.2 Cableado estructurado de red.

El cableado estructurado de una red está compuesto por las conexiones entre equipos de comunicaciones por un medio como: par trenzado, coaxial o fibra óptica.

Tiene como elementos principales el cableado horizontal y el cableado vertical o backbone.

Cableado Horizontal: Es el cableado correspondiente al área de trabajo de la red, y se dirige hasta el cuarto de telecomunicaciones.

Cableado Vertical o Backbone: Es el cableado correspondiente a la conexión de áreas de trabajo en un edificio vertical, los cuartos de telecomunicaciones y de equipos. El Backbone es un conducto especial que permite comunicar varios segmentos de una red.

1.2.1 Introducción al cableado estructurado de red.

"Primeros años de la década del '80:

– Construcción de edificios sin consideración de los servicios de comunicaciones

– Tendido independiente

– Instalación de cableado telefónico en el momento de la construcción

– Instalación del cableado de datos, posterior al momento de la construcción.

A inicios de los 80´s apareció la tecnología Ethernet con cable coaxial de 50 Ω.

RG 58. Remplazada luego por el par trenzado."

(http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf)

Con estos antecedentes aparecen normas para estandarizar el cableado de las redes al inicio con *Ethernet* que se convirtió en el más popular en redes de área local superando a otros como *token ring*. Se tenía dos modelos principales para conectar los equipos CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) - (Acceso múltiple con escucha de portadora y Detección de Colisiones), y el CSMA/CA (*Carrier Sense, Multiple Access, Collision Avoidance*) (acceso múltiple por detección de portadora con evasión de colisiones).

La diferencia principal radica en que el CA se utiliza en las redes en las que no se puede utilizar CD. CD escucha al medio antes de negociar una comunicación, que esté disponible el canal y los recursos para transmitir.

“CSMA/CA cada equipo anuncia su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio este libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal”.

(http://es.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance).

Ethernet se estandarizo como IEEE 802.3 en 1980.

Las conexiones pueden ser a través de un medio como fibra óptica, coaxial o el par trenzado.

1.2.1.1 La fibra óptica.

Son mensajes enviados por medio de haces de luz que pasan de un lado a otro incluyendo filos y esquinas sin interrupción, está compuesto por filamentos de vidrio flexibles esta se hacen de arena o sílice que es más abundante que el cobre.

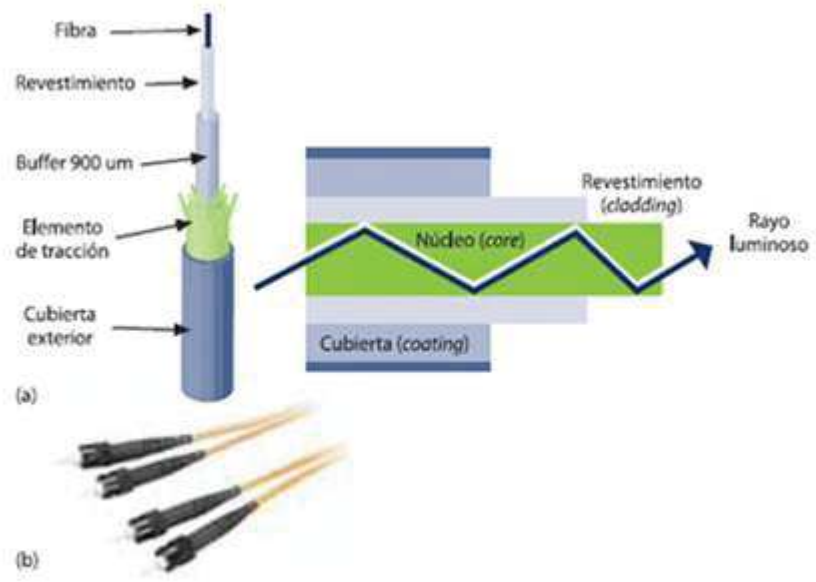


Figura 2. Composición de la fibra óptica.
Tomado de http://alberto3003.wikispaces.com (sf) Sistemas de fibra óptica. Recuperado el 6 de febrero del 2013 de: http://alberto3003.wikispaces.com/Sistemas+de+fibra+optica.

Los elementos principales de la fibra son el núcleo y el recubrimiento, el núcleo es la parte interna la cual lleva el haz de luz y el recubrimiento es la parte que protege el núcleo.

Tipos de fibras ópticas.

- **Fibras ópticas multimodo.**

Son aquellas que pueden guiar y transmitir varios rayos de luz por sucesivas reflexiones, (modos de propagación). Los modos son formas de ondas admisibles, se transmiten varios modos electromagnéticos por la fibra óptica, la palabra modo significa trayectoria.

- **Fibras ópticas mono modo.**

Son aquellas que por su especial diseño pueden guiar y transmitir un solo rayo de luz (un modo de propagación) y tiene la particularidad de poseer un ancho de banda elevadísimo.

En estas fibras mono modo cuando se aplica el emisor de luz, el aprovechamiento es mínimo, el costo es más elevado, la fabricación difícil y los acoples deben ser perfectos.

1.2.1.2 Coaxial.

Un cable coaxial consta de un núcleo de hilo de cobre rodeado por un aislante, un recubrimiento de metal trenzado y una cubierta externa.

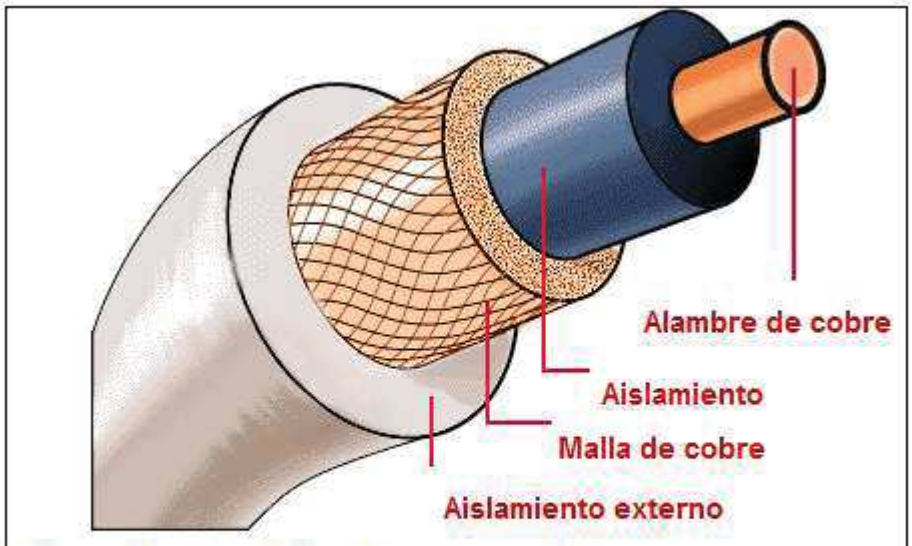


Figura 3. Composición del cable coaxial.
Tomado de http://bryan.bligoo.ec (sf) Cable coaxial.
Recuperado el 17 de Septiembre del 2012 de:
http://bryan.bligoo.ec/cable-coaxial#.UAmwPWHCpkg.

Una de las características del cable coaxial es que es más resistente a interferencias y atenuaciones que el par trenzado. Este cable dispone de dos partes esenciales un conductor central que es el encargado de llevar la información a través de señales eléctricas, el conductor externo o recubrimiento que funciona como protección y tierra para este cable.

Las utilizaciones más comunes de coaxial se pueden ver en las instalaciones de televisión por cable y en las redes interurbanas de telefonía.

Tipos de cable coaxial.

Existen dos tipos de cable coaxial, su diferencia está en las características físicas como en sus características técnicas y de capacidad.

- **EL grueso o cable amarillo:** este fue empleado en la mayoría de las redes porque su capacidad es grande en velocidad y cubre grandes distancias, sin embargo es demasiado grueso para utilizar en conexiones donde hay mucho cableado y su costo es elevado.
- **El fino o Thin:** a diferencia del anterior no cubre distancias grandes necesita regenerar cada cierto tramo la señal, al contrario del cable amarrillo es más fino y su costo es barato. Se utiliza para solventar las desventajas del cable grueso.

1.2.1.3 Par trenzado.

Este cable es el más utilizado en las conexiones de red, cable susceptible a atenuación, que está formado por una serie de cables de cobre entrelazados en pares con varios colores, Par 1: Blanco- Azul/Azul Par 2: Blanco-Naranja/Naranja Par 3: Blanco-Verde/Verde Par 4: Blanco-Marrón/Marrón El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se habla de cables multipar.

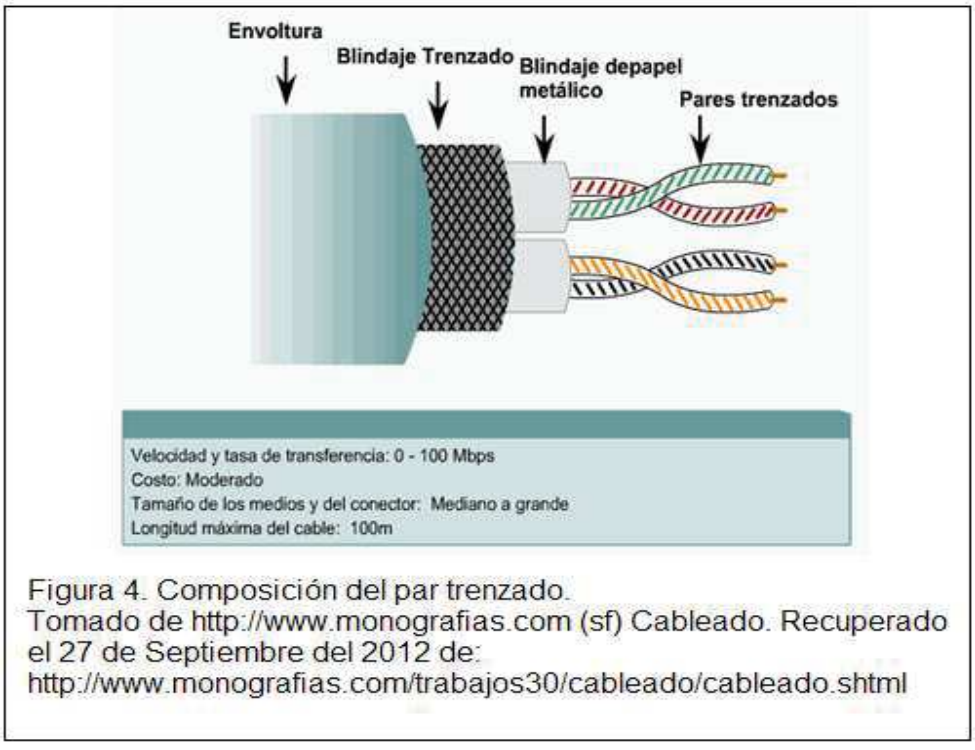


Figura 4. Composición del par trenzado.
Tomado de http://www.monografias.com (sf) Cableado. Recuperado el 27 de Septiembre del 2012 de:
http://www.monografias.com/trabajos30/cableado/cableado.shtml

“Los conductores son de cobre obtenido por procedimientos electrolíticos y luego recocido.

• El aislante, salvo en los antiguos cables que era en papel, es de polietileno de alta densidad.

• El paso de pareado (longitud de la torsión) es diferente para reducir desequilibrios de capacidad y por tanto la diafonía entre pares.

• Los pares, a su vez, se cablean entre sí para formar capas concéntricas.

• En algunos casos, los intersticios existentes entre los hilos se rellenan con petrolato, de forma que se evite la entrada de humedad, o incluso de agua, en caso de producirse alguna fisura en la cubierta del cable que, también es de polietileno, antes era de plomo”.

(http://www.rnds.com.ar/articulos/052/RNDS_136W.pdf).

Tipos de cable de par trenzado.

Existen tres tipos de cable de par trenzado UTP, STP y el FTP, su diferencia se da tanto en sus características físicas como en las técnicas y de capacidad.

- **Cable de par trenzado apantallado o STP:**

En este cable los pares tienen la malla conductora que los protege de interferencias como el ruido, sin embargo requiere de configuración de interconexión a tierra para que la pantalla sea más fuerte.

Su impedancia es de 150 ohm, es robusto, es costoso y difícil de instalar. Su protección a factores externos es mayor que UTP y los conectores son los RJ 49.

- **Cable de par trenzado con pantalla global o FTP:**

Se diferencia del STP en que no es un apantallamiento por pares, es completo mejorando el nivel de protección ante interferencias externas.

Su impedancia es de 100 ohm, sus propiedades de transmisión son parecidas al UTP, su costo no es muy elevado y los conectores son los RJ 45.

- **Cable de par trenzado sin blindaje UTP:**

Son cables de par trenzado que su diferencia con los dos anteriores es que no tienen una protección ante interferencias, no son apantallados, el costo es bajo se utiliza para redes locales por su fácil uso para trabajar, pero producen más errores que los otros cables en distancias más largas.

Su impedancia es de 100 ohm.

Los elementos de un buen cableado estructurado además de los cables son el cuarto de telecomunicaciones el cual está definido para alojar únicamente el cableado que hace posible las comunicaciones de los datos y no debe ser simultáneo con otro tipo de instalaciones eléctricas. El esquema de este espacio debe suponer, el cuarto de equipos es de uso concreto para equipos de telecomunicaciones, como central telefónica, servidores y sistemas de video, estos incluyen: espacio de trabajo para personal de telecomunicaciones, cuarto de entrada de servicios el que está definido para recibir la entrada de los servicios de telecomunicaciones. En este se agregare de ser posible el backbone, que conecta a otros edificios bajo una topología de red tipo estrella y al final las áreas de trabajo en el cual está el final del cableado horizontal y corresponde a los puntos de borde donde se conectan las estaciones de trabajo de los usuarios finales. Además todo cableado debe tener sistemas de puesta a tierra donde se conectan todos los segmentos metálicos de los equipos que acceden a un sistema eléctrico.

1.3 Estándares o normativas de cableado.

Existen tres principales estándares de cableado:

- **EIA / TIA 568A -** Esta es la norma estadounidense y fue la primera en ser publicada (1991).
- **ISO / IEC 11801 -** La norma internacional para sistemas de cableado estructurado.
- **CENELEC EN 50173 -** El estándar de cableado Europeo.

La razón para tener un estándar es definir un método de conexión de todos los

tipos de proveedores de equipos de voz y datos. Además un sistema de cableado que utiliza un medio de comunicación habitual, con conectores y una topología común. Esto significa que un edificio puede ser cableado para todas sus necesidades de comunicación sin que el planificador o arquitecto tenga que saber en qué tipo de equipo será utilizado.

En 1991, la TIA / EIA lanzó el estándar TIA / EIA 568 *Standard Commercial Building* Cableado de Telecomunicaciones. Teniedo en cuenta que el cliente ISO/IEC-11801 (norma genérica de locales de cableado), es un estándar de cableado internacional que se basa en el estándar de cableado ANSI/TIA/EIA-568.

Las normas (TIA / EIA cableado estructurado), definen la forma de diseñar, construir y administrar un sistema de cableado que se estructura. Lo que significa que el sistema está diseñado en elementos que tienen características de rendimiento muy específicos. Los elementos están integrados en una forma jerárquica creando un sistema de comunicación unificado. Por ejemplo, grupo de trabajo LAN representan un elemento con un menor requisito, que el bloque de red básica, que requiere un alto rendimiento de la fibra óptica en la mayoría de los casos. La norma define el uso de cable de fibra óptica mono modo y multimodo, el cable STP par trenzado blindado, y el cable UTP par trenzado sin blindaje.

El primer TIA / EIA 568 documento fue seguido por varias actualizaciones y mejoras como se indica a continuación. Una importante actualización del estándar fue publicado en 2000, que incorpora los cambios anteriores.

TIA/EIA-568-A-1995: Para edificios comerciales, las normas de cableado de telecomunicaciones define un estándar para la construcción del sistema de cable para edificios comerciales compatibles con las redes de datos, voz y vídeo. También define los criterios técnicos y de rendimiento para el cableado.

Actualizaciones TIA/EIA-568-A (1998-1999), el TIA/EIA-568 se actualiza varias veces a través de este período de tiempo. Actualización de la A1 se describe la propagación y retrasos de los parámetros de inclinación. Actualización de la A2 se especifica cambios diversos. Actualización A3 requisitos especificados para el

conjunto de cables e híbridos. Actualización A4 devuelva los requisitos de la pérdida de los cables de conexión. Por último, la actualización A5 define los requisitos de rendimiento para la Categoría 5 Mejorada (Categoría 5E).

TIA 568-B.1-2000 telecomunicaciones para edificios comerciales estándar de cableado, en el año 2000 los paquetes de actualización, los apéndices anteriores y actualizaciones de servicio en una nueva versión y lo más importante. Se especifica que el cable categoría 5E es el tipo de cable preferido que puede proporcionar niveles aceptables de rendimiento. Varias adiciones se publicaron también para especificar la información técnica para el par trenzado, apantallado de dos pares de cable y cable de fibra óptica.

TIA/EIA-569-A-1995. Estándar de edificio comercial de rutas y espacios de telecomunicaciones. Esta norma define cómo construir las vías y espacios para los medios de telecomunicación.

TIA 570-A-1998. Residencial y comercial ligero estándar de cableado de telecomunicaciones, este específica el cableado residencial.

TIA/EIA-606-1994. Edificio de Administración de Infraestructura de las Américas, esta norma define las directrices de diseño para la gestión de una infraestructura de telecomunicaciones.

TIA/EIA-607-1995. Puesta a tierra y los requisitos de fortaleza, este estándar define la conexión a tierra y uniendo los requisitos de cableado y equipos de telecomunicaciones.

La tendencia actual es la evolución de las normas de apoyo a redes de alta velocidad como Gigabit Ethernet y conectores como categoría cuatro pares de cable de categoría 6 y 7. Categoría 6 tiene una capacidad de rendimiento de canal de hasta 200 MHz, mientras que la categoría 7 tiene hasta 600 MHz.

El estándar TIA define los parámetros para cada parte del sistema de cableado, que incluye el cableado del área de trabajo, cableado horizontal, armarios de telecomunicaciones, salas de equipos, conexiones cruzadas, la columna vertebral (vertical) de cableado y las instalaciones de entrada.

1.3.1 Norma norteamericana ANSI/EIA/TIA-568A.

“El cableado estructurado para redes de computadores tiene dos tipos de normas, la EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B). Se diferencian por el orden de los colores de los pares a seguir en el armado de los conectores RJ45. Si bien el uso de cualquiera de las dos normas es indiferente, generalmente se utiliza la T568B para el cableado recto.

Si un cable de conexión que se necesita, utilizar la norma 568A en un extremo y 568B en el otro extremo.”

(http://www.garciagaston.com.ar/verpost.php?id_noticia=46)

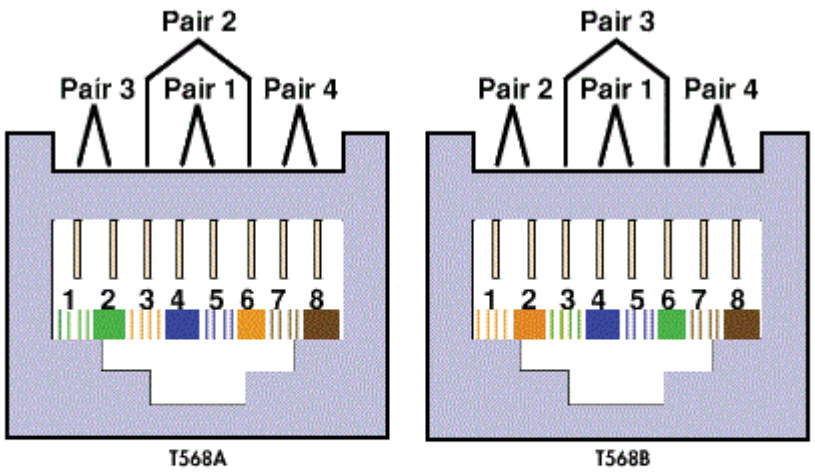


Figura 5. Código de colores conectores RJ - 45.
Tomado de http://www.utm.edu. (sf) Estándar EIA TIA 568 A y 568 B.
Recuperado el 17 de Octubre del 2012 de:
http://www.utm.edu/staff/leeb/568/568.htm.

1.3.1.1 Cableado entre dispositivos.

“Cable Recto (Straight Through):

Es el cable cuyas puntas están armadas y la misma norma (T568A <----> T568A ó T568B<---->T568B). Se utiliza entre dispositivos que funcionan en distintas capas del Modelo de Referencia OSI. De PC a Switch/Hub. De Switch a Router.

Cable Cruzado (Crossover):

Es el cable cuyas puntas están armadas con distinta norma (T568A <----> T568B). Se utiliza entre dispositivos que funcionan en la misma capa del Modelo de Referencia OSI.

De PC a PC, de *Switch/Hub a Switch/Hub*, de *Router* a *Router* (el cable serial se considera cruzado)."

(http://www.garciagaston.com.ar/verpost.php?id_noticia=46)

1.3.2 TIA/EIA-568-A-1995

(Para edificios comerciales, las normas de cableado de telecomunicaciones)

Define un estándar para la construcción de sistema de cable para edificios comerciales compatibles con las redes de datos, voz y vídeo. También define los criterios técnicos y de rendimiento para el cableado. Esta norma señala los requisitos mínimos para cableado de telecomunicaciones dentro de un edificio comercial, incluyendo la salida del conector de telecomunicaciones y entre los edificios en un ambiente de campus. Especifica los requisitos de los elementos, del cableado de telecomunicaciones: las distancias, las configuraciones de salida de conector y una topología recomendada. La norma tiene por objeto apoyar una amplia gama de diferentes sitios de construcción comercial y sus aplicaciones (como ejemplo: voz, datos, texto, vídeo e imagen).

Típicamente, esto incluye los sitios con una extensión geográfica de 3.000 metros hasta 1.000.000 m^2 de espacio de oficina, y con una población de hasta 50.000 usuarios individuales. Sistemas de cableado de telecomunicaciones especificados por esta norma y pretende tener una vida útil de más de diez años. Esta norma se aplica a los sectores de telecomunicaciones sistemas de cableado de los edificios para las empresas comerciales que es la oficina de orientación.

1.4 topologías de red.

Existen dos tipos de topologías la física y la lógica:

La topología lógica es la que permite pasar información entre las diferentes estaciones de trabajo de una red, mientras que la topología física especifica la configuración de los cables, ordenadores y otros periféricos. Las principales físicas son las siguientes:

- Bus
- Estrella
- Árbol
- Anillo
- Malla

1.4.1 Bus:

Los elementos o estaciones de trabajo de la red se conectan de forma lineal todas dirigidas en un cable lineal o bus.

1.4.2 Estrella:

Los elementos o estaciones de trabajo de la red se conectan de forma punto a punto a un concentrador “equipo” central de red.

1.4.3 Árbol:

La topología estrella y la bus se combinan para formar la topología árbol, es decir en una estructura árbol, hay pequeñas estrellas unidas entre sí por medio de un bus esto permite que la red pueda tener un crecimiento de capacidad en equipos.

1.4.4 Anillo:

En esta topología los elementos o estaciones de trabajo están conectados entre sí por un mismo medio un cable en forma circular, las estaciones de trabajo funcionan como repetidoras una tras otra, si un elemento de estos se cae se pierde la conexión completa.

1.4.5 Malla:

En esta topología los elementos o estaciones de trabajo tienen múltiples caminos para llegar al destino, lo cual favorece si hay tráfico o se pierde una conexión se podrá tomar una ruta diferente para llegar al destino.

1.5 El cyber.

Implementado en un establecimiento de una sola planta, con espacio reducido pero apto para su correcto desempeño su ubicación es en el sector de Guamaní el barrio de la Florencia, avenida Maldonado (S-60) frente a la gasolinera Petrocomercial.

Surge con la necesidad de cubrir la demanda de internet de los moradores del sector ya que no pueden cubrir un servicio de internet en casa.

Un objetivo a cumplir es establecerse como el centro de cómputo más importante de la zona y su tarea es brindar un servicio de calidad a los usuarios que así lo requieran.

La competencia para el establecimiento son los cyber de la zona a una distancia que permitir captar más usuarios a cada centro.

En el establecimiento se encuentra funcionando a la par La empresa MPG estudio que se encargara de vender herramientas para vdj, música, mixes y programas.

”Somos una empresa creada en el año 2004, la cual se dedica a vender productos en INTERNET.

Nuestra mayor satisfacción es cumplir con las expectativas del cliente en nuestras publicaciones.

Contamos con una reputación 100% confiable, misma que ha sido otorgada por nuestros clientes.” (http://santydj.blogspot.com/p/quienes-somos.html).

1.6 Legislación del Ecuador sobre cybercafés.

El Consejo Nacional de Telecomunicaciones CONATEL mediante la resolución 132-05 del 2009, regula los centros de acceso a la información y aplicaciones disponibles en la red de internet conocidos como cyber o cybercafé. Esta indica que los cybercafés previo a su operación tienen que adquirir un registro en la Secretaria Nacional de Telecomunicaciones para lo cual deben cumplir los siguientes requisitos.

Personas Naturales:

- Solicitud dirigida al señor Secretario Nacional de Telecomunicaciones.
- Formulario de registro a publicarse en la página web del CONATEL.
- Copia de RUC.
- Copia de cedula de ciudadanía y papeleta de votación.
- Copia del contrato del proveedor ISP autorizado.
- Copia del contrato firmado con la empresa de servicios portadores o finales que provea en enlace hacia el ISP.

Personas Jurídicas:

- Solicitud dirigida al señor Secretario Nacional de Telecomunicaciones.
- Formulario de registro a publicarse en la página web del CONATEL.
- Copia de la escritura de la constitución de la compañía o en caso de sociedades extranjeras de la que contenga su domiciliación en el Ecuador.
- Copia del nombramiento del representante legal debidamente inscrito en el registro mercantil.
- Copia de RUC.
- Copia de cédula de ciudadanía y papeleta de votación del representante legal de la compañía.
- Copia del contrato del proveedor ISP autorizado.
- Copia del contrato firmado con la empresa de servicios portadores o finales que provea en enlace hacia el ISP.

CAPÍTULO II

2 Seguridad Informática.

¿Que se quiere proteger?

La información.

¿Qué es la información?

Es la unión o conjunto de datos por los cuales se genera un significado especifico.

¿Qué es un dato?

Es la mínima parte de un valor de información específico.

Ejemplo: Datos = 0,9,9,5,4,5,6,1,5,7 Información = 0995456157.

¿Qué es la seguridad?

La seguridad es una certeza, algo indubitable firme que no registra riesgos.

¿Qué es la seguridad informática?

Es una característica de los sistemas informáticos, consiste en mantener los datos, información del usuario, de forma que solo este tenga acceso a la misma y permanezca sin modificaciones externas sin sufrir ninguna clase de riesgos. Está basado en tres premisas: confidencialidad, disponibilidad e integridad. La seguridad en el entorno de red debe de otorgar garantías para poder desarrollar operaciones con la certeza de que la información va hacer privada y protegida, esto se lo realiza con políticas de seguridad.

El uso de usuarios y contraseñas es una pauta básica de seguridad informática, en las redes, los elementos físicos, la protección de la infraestructura son medidas de seguridad. Las estructuras de seguridad tradicionales se basan en el pc del usuario, una dirección ip, un protocolo de red, un puerto, un firewall sea físico o lógico, pero a medida del crecimiento de las redes tradicionales y la forma

de acceder al internet, sea por diferentes medios como laptop, tablet, teléfono celular los riesgos cada vez son mayores a pesar de los medios que se utilicen para lograr una conexión segura no se tendrá una conexión completamente invulnerable.

2.1 Seguridad de red.

La seguridad de la red consiste en la disponibilidad e integridad de esta para su utilización, se debe conocer lo que se va a proteger, no se puede utilizar solo un método de seguridad la opción más adecuada es un conjunto de elementos entre los que tenemos firewalls, proxies, control de acceso, cifrado, seguridad del edificio, servidores, switches, routers y host, los que generan un sistema de respuesta más completo a las amenazas más comunes.

El sistema de seguridad debe de generar una respuesta a las posibles vías de ataque que puedan ser utilizadas por terceros para causar daño a esta. Un buen conocimiento de la estructura y de las debilidades que esta posee nos permitirá una rápida respuesta a cualquier imprevisto que afecte el sistema.

Un sistema de red seguro es aquel en que el hardware, software y la información (datos) de los usuarios están a salvo ante cualquier inconveniente. Si un usuario accede a una cuenta de correo o a una red social, mantener el flujo de datos de esa conexión de uso y para uso exclusivo del dueño de la cuenta es un componente de estos sistemas.

La continuidad de las operaciones en la red es un objetivo primordial para cualquier organización, la falta de medidas de seguridad genera un problema cada vez más grande por causa de los atacantes con mayores recursos y conocimientos para causar daño. Un sistema seguro debe mantener un orden en la distribución de sus elementos, tratar de ser lo menos complejo para poder detectar y corregir los problemas que ocurran en el momento.

Un componente primordial de estos sistemas es el personal encargado de la red, la labor de estos en el apoyo a los usuarios, además de la atención y la vigilancia continua metodología del desempeño genera una pronta respuesta.

Un conjunto de recursos bien utilizados permiten obtener un sistema seguro, con la implementación de objetivos, entre los principales están:

- Impedir que usuarios no autorizados intervengan en el sistema con fines malignos.
- Impedir que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
- Salvar los datos mediante la previsión de fallas.
- Garantizar que no se interrumpan los servicios de la red.

2.1.1 Seguridad física.

Para un sistema físico seguro se debe conocer la estructura de la red la composición y distribución de los componentes que la forman. Además al tanto de los elementos de seguridad disponibles en esta estructura y la aplicación de estas, los puntos donde la red se distribuye y se pueden generar conflictos, los mismos, pueden ser utilizados como puntos de control.

La seguridad es un conjunto de recursos destinados a defender la red de las amenazas internas y externas. Entre los recomendados para un sistema físico se tienen:

- Un servidor de datos en el cual se almacena todos los datos relevantes de la instalación y el lugar donde va estar ubicado.
- Firewall físico para tener el control de los accesos a datos relevantes.
- Mantenimiento a los equipos de la red.
- Cableado estructurado normado.
- Renovación de equipos obsoletos o averiados.
- Puesta a tierra.
- Resguardo para los equipos contra robos y destrucción.

El hardware es el elemento más costoso de una red y por ende es el factor que más costo puede generar en mantener y recuperar. Después de un conflicto las principales causas para que se vea afectado son: acceso físico, desastres naturales y alteraciones del entorno.

El acceso físico es un punto de inflexión en cualquier sistema dado que un usuario con este recurso puede hacer todo el daño posible y dejar obsoleto cualquier sistema de seguridad implementado hasta el momento, es decir un usuario con acceso al servidor puede apagar este y dejar sin sistema a la red o vasta con desconectar un equipo como un Router o un switch para afectar a la red.

Para prevenir la mala utilización o el acceso no permitido a los elementos de la red es importante que se implemente medidas de seguridad de control de acceso hacia partes de la red y de los elementos ubicados en ella.

El desastre natural es un aspecto mucho más impredecible es así que no se pueden preveer cuando ocurrirán ni que parte de la red afectaran. Es aquí que entra la capacidad de los diseñadores de la red, para saber dónde ubicar de forma correcta los equipos, según la normativa y recomendaciones para el lugar donde se implemente la red. Para que en caso de humedad, corto circuito etc, se vean afectados lo menos posible, además de tener equipos de respaldo para poder reponer en caso de dejar de funcionar uno de ellos. Un problema de la seguridad física son las filtraciones de agua, las inundaciones por varias causas son las que más daño pueden causar a los equipos y dejarlos completamente inservibles.

Los terremotos, temblores, tormentas eléctricas son un factor importante que hay que tomar en cuenta en cuanto a una posible causa de daño a la red. Para evitar riesgos no hay que ubicar los equipos en lugares muy altos ante un temblor fuerte o un terremoto se pueden caer y averiar sobre todo en el Ecuador que es un país por su ubicación susceptible a movimientos telúricos, inundaciones, ceniza volcánica, húmeda y tormentas eléctricas.

Las alteraciones del entorno son conflictos que se pueden solucionar sin mucha complejidad si se tiene un conocimiento muy bueno de la estructura y disposición de la red, si un elemento de la red se ve afectado por el cambio del entorno, los elementos dejan de funcionar por factores como la electricidad estática, el ruido eléctrico, el mal estado de los tomas de corriente o la no utilización de equipo de

control del fluido eléctrico ante posibles cortes de energía o descargas de voltaje. Es importante la ubicación de los elementos dentro de un marco seguro para su desempeño y de fácil acceso para poder reemplazarlos fácilmente ante un percance. Como medidas de seguridad preventiva ayudaría una puesta a tierra de calidad. Que el hardware no este expuesto a mucho calor o mucho frio por que dañan los componentes y que no esté comprometido con los factores que produzcan ruido, polvo, etc.

Los incendios es otro factor a tomar en cuenta en la seguridad física ya que pueden ser causados por un cortocircuito o un descuido de los usuarios u operadores de la red, como medida de prevención el equipamiento de extintores y una correcta ventilación del establecimiento así como lugares de evacuación son oportunos para brindar una solución a este factor.

Una medida de seguridad importante en la parte física son los firewall o corta fuegos, es importante la implementación de estos ya que son los encargados en permitir o denegar las trasmisiones de una de una red a otra. En la comunicación de la red interna con el internet, su función es la de un filtro y a pesar de que hay firewalls lógicos, son mucho más seguros los físicos, es importante para evitar que personas no autorizadas ingresen en la red. Su aplicación se basa en las comunicaciones de la red y en los servicios que se configuren en él, como correo, ftp o web, en permitir todos o escoger los que son útiles para ese usuario en específico. Esto permite un control y optimiza el uso de banda ancha de internet. La ubicación de esta pared o cortafuegos es entre la red interna de la organización y la conexión externa a internet que entregan los proveedores.

Como se ve son varios los factores que pueden averiar la parte física de la red, por ende es importante implementar un plan de seguridad sólido en el cual tendremos controles de acceso y una correcta normativa de implementación de la estructura de red con sus respectivos respaldos de información.

2.1.2 Seguridad lógica.

La protección física no es el único elementó en seguridad de redes y para complementar un buen sistema es necesario la parte lógica. Todas las herramientas encaminadas por software que sean parar proteger la información del usuario y de la red conforman la seguridad lógica.

Es aquí cuando entran las medidas de seguridad software de protección como los firewalls lógicos o herramientas tecnológicas como la utilización de V.P.N.s redes privadas virtuales, que ayudan a establecer conexiones seguras internas así como la comunicación entre la red local y el internet.

La utilización de métodos de control como la utilización de contraseñas es un elemento importante en seguridad que permite q cada usuario tenga o no acceso a funciones específicas del sistema.

Como elemento de seguridad se implementa la utilización de privilegios según las tareas a realizar por los usuarios y con restricciones delimitadas según sus funciones en la empresa.

Es importante que los programas utilizados por el usuario estén debidamente controlados. Es común la utilización de puertas o grietas que generan ataques por estos puertos previamente abiertos por un software destinado a otro fin.

Lo más común en ataques a la red se dan por software maliciosos como troyanos, bombas, spam y para evitar que estos causen daño o reducir al mínimo la posibilidad de ataques a la red es necesario la utilización de un antivirus funcionando y actualizado constantemente.

Lo más importante en la red es la información y los elementos que la conforman son los encargados de tener disponible siempre esos datos hacia y desde los usuarios, que esta sea intangible además de inviolable; la pauta importante en la seguridad es que la información que sale de un transmisor llegue al receptor sin ser alterado, se debe tener un sistema de respaldo de transmisión para cuando falla el principal, así como un backup de la información si se dispone de un servidor.

El backup o copia de seguridad es importante para poder restaurar los datos originales partiendo de las copias almacenadas hasta antes del suceso o pérdida de información.

2.1.3 Controles de accesos físicos y lógicos.

Los controles de acceso son los que permiten saber que usuarios están operando, en que área están trabajando y lo que están realizando. Es la medida de seguridad que se implementa en cualquier sistema seguro. La implementación de estos está basada en lo que se quiere proteger de una red, y en la importancia de esta, es así que no es lo mismo la protección de un sistema bancario que un cyber café, la mejor opción depende del costo beneficio de la entidad. Entre los más comunes tenemos los siguientes:

Accesos físicos:

- Implementación de personal para controlar las acciones de los usuarios de la red.
- Utilización de sensores inteligentes para controlar el flujo de personal.
- Verificación de voz para acceder a ciertas áreas de la red.
- Método de control de acceso mediante huella digital.
- Sensores de retina son los más seguros y con un costo monetario alto.
- Circuitos cerrados de televisión.
- Dispositivos luminosos y sectorización según tareas a realizar por el personal.
- Detectores de sonido o ruido.
- Utilización de detectores de metales.
- Utilización de tarjetas inteligentes.
- Disposición de una edificación o establecimiento con todas las características tecnológicas para obtener un edificio inteligente.

Accesos Lógicos:

- Identificación de los usuarios de la red con usuario y contraseña.
- Encriptación de la información a trasmitir de un punto a otro.

- Lista de control de los usuarios y sus accesos a la red.
- Restricciones a los usuarios sobre las operaciones en la red.
- Designación de los recursos según las necesidades de cada usuario.
- Control de puertos a través de un equipo físico que permita que el usuario opere solo en puertos establecidos previamente.
- La utilización de firewalls y puertas de seguridad para filtrar o bloquear el acceso de la red interna hacia una externa como el internet.
- Perfiles de acceso según la clase de usuario sea interno o un consultor externo temporal.
- Vigilancia por software de dispositivos de almacenamiento externos.

Todas estas herramientas de control tanto físicas como lógicas permiten conocer a los usuarios de la red y las acciones que realizan en ella. Pero el mantenimiento, supervisión y una administración eficaz de estos debe ser constante; los encargados de esto son los administradores de la red, los que realizan pruebas y corrigen errores, así como son quienes crean los perfiles de usuario y dan acceso o no a la red.

Como conclusión se conoce que un sistema seguro en un 100 % no se puede obtener, sin embargo la implementación de un control físico más un control lógico permitirá tener cada vez sistemas más confiables, es importante implementar el aumento de controles a la par de que la red va creciendo.

Las políticas de seguridad que se deseen implementar siempre van a estar sujetas a los recursos disponibles de la organización y con el avance de la tecnología cada vez aparecen nuevas amenazas, sin embargo las herramientas de seguridad van mejorando con el tiempo.

2.2 Seguridad por capas según el modelo de interconexión de sistemas abiertos OSI.

El modelo de interconexión de sistemas abiertos OSI, fue una implementación de la ISO Organización Internacional de Normalización como guía de funcionamiento del hardware y software de red, definiendo como se integran estos a través de las

diferentes capas para transmitir la información entre los usuario de una red al usuario de la otra red. Los datos que se transmiten de la red se mueven de capa en capa hasta alcanzar el destino. Estos paquetes son conocidos como PDU (unidad de paquetes de datos) y cada uno de estos lleva la dirección de destino. Para que esta información sea tratada y corregida correctamente en el momento de recepción y envió, entra la utilización de los protocolos que son los traductores de las computadoras como el IP protocolo de internet.

El modelo OSI se encuentra compuesto de 7 capas que son:

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de datos
- Física

Como ya se detalló el modelo OSI en el capítulo 1.1.2, en este capítulo se estudiaran las amenazas y las seguridades en cada una de estas capas de interconexión del OSI

Este modelo está diseñado para que cada capa opere independientemente es decir si los ataques se dan en una capa la siguiente no sabrá del ataque y continuará enviando el paquete, es de ahí la importancia de la seguridad por cada una de las capas.

Capa física: es donde se inicia la comunicación entra a operar las conexiones de cables, conectores, concentradores entre los equipos de esta; se basa en la utilización de pulsos eléctricos o de luz que generan valores positivos y negativos que dan bits 1 o 0

La seguridad en la capa física está dada por el estado de los elementos que la conforman, la correcta configuración de estos así como su correcta utilización.

Las amenazas en esta capa están dadas por factores externos como la ambiental

humedad, descargas de voltaje, la no refrigeración y el acceso de personal no autorizado al cuarto de equipos.

Capa de enlace: En esta capa los PDU son enviados a cada punto de conexión de la red para su correcto funcionamiento se agrega a los paquetes un chequeo de redundancia cíclica a cada trama tanto para la computadora que emite como la receptora y si los dos tienen el mismo valor es un paquete con éxito.

La seguridad en esta capa está dada por los dispositivos que operan en ella, hub, switch, bridge, tarjetas de red, direcciones MAC, y la protección que se puedan dar a estos.

La utilización de las VLANs permite tener una conexión segura en la teoría. Más en la práctica las VLANs no están completamente aisladas unas de otras. Ya que para transmitir múltiples VLANs a través del mismo enlace físico se utiliza trunk port que tiene acceso a todas ellas. El atacante a una red puede utilizar un dispositivo para alterar la VLAN de los paquetes encapsulados para el trunking, para transmitir o recibir los paquetes de varias VLANs. Para evitar esto es necesario utilizar una VLAN dedicada para los puertos trunk, deshabilitar el auto trunking, los puertos de los usuarios en modo no trunking y deshabilitar los puertos no utilizados.

Las direcciones MAC control de acceso de medio, pueden ser falsificadas la capa enlace para entregar los paquetes utiliza las direcciones MAC que son únicas para cada computador de la red. Pero si se falsifica esta dirección se tiene acceso a la información destinada a esa dirección y se puede utilizar para atacar la red desde ese host ficticio. Entre los ataques más comunes basados en esta técnica tenemos el ARP spoofing.

Como el protocolo ARP no proporciona seguridad para reservar o validar direcciones IP o MAC, su función es emitir tráfico de difusión broadcast como ARP *request* y *reply*. El ARP *spoofing* funciona enviando mensajes falsos ARP para que tome como valido la dirección MAC del hacker por una dirección IP asociada dentro de la red con esto permitirá leer el trafico modificar eh incluso

detener el flujo de información.

Con este ataque el hacker puede ocasionar una denegación de servicio DoS a un usuario en específico, este ataque se basa en hacer inaccesible la red a otro usuario, causar que no se pueda hacer uso del sistema asociando una dirección MAC insistente a la IP de un usuario eh incluso sobrecargar o saturar el servicio para que se caiga el sistema.

La seguridad en esta capa se la consigue cambiando las tablas ARP de dinámicas a estáticas.

La otra opción es en una tabla dinámica establece que no actualice la dirección de la puerta de enlace de la red así permanecerá estática.

Capa de red: En esta capa los PDU que provienen de la capa enlace son distribuidos de la mejor manera por las tablas de rutas que utilizan los dispositivos que trabajan en esta capa como los switch de capa 3 y routers que utilizan las direcciones IP lógicas previamente convertidas de las MAC para su comunicación y envió de datos con el nombre de paquetes.

Como medidas de seguridad entran las normas de filtrado para conexiones de proveedor ISP.

Las principales amenazas son la deficiente protección de los datos en el tránsito, así como el acceso a los recursos sensibles de la red, en esta capa se puede hacer cualquier ataque que afecte un datagrama IP un paquete de datos. Se incluye en esta capa los ataques de *sniffing*, suplantación de mensajes, modificación de datos los retrasos de mensajes y la denegación de mensajes, el reemplazo de un paquete si indica que viene de otro usuario. La suplantación de mensajes se puede dar por muestra dando respuesta a un paquete primero o antes que lo haga el suplantado. Encontramos problemas de autentificación, algunos de los ataques más comunes o conocidos son las denegaciones de servicio DoS debidas a protocolos de transporte utilizados en la capa anterior, también hay posibilidad de interceptación de sesiones IP establecidas, con el objetivo de apropiarse y dirigirlas a otros equipos con fines desconocidos.

Capa de transporte: Esta capa es encargada de proporcionar una conexión fiable orientada de extremo a extremo los servicios comunicando con su capa superior. Entre los objetivos en esta capa están la transferencia de datos confiable, contabilizar y ordenar paquetes, controlar el flujo para que funcione bien.

La comunicación se realiza a través de los sockets o puertos entre el 0 y el 1024 públicos reservados como el web puerto 80, ftp 20 y 21. Los de libre uso 1025 a 65000. Esta capa no se encarga de asignar los puertos a las diferentes aplicaciones pero contiene la información del puerto.

Como medida de seguridad se puede implementar la autentificación del origen de los datos, control de acceso, confidencialidad orientada a conexión o no conexión y autenticación de identidad del extremo de la conexión.

Capa de sesión, presentación y aplicación: En la capa de sesión se inicia y finaliza las sesiones de comunicación eh intercambio de datos. La capa de presentación es la encargada de trasformar los datos dándoles formato, encriptado y comprimiendo para que se puedan leer en la capa superior. La capa de aplicación es la encargada de establecer la interfaz de comunicación con el usuario con programas como el de correo, reproductores etc. Como medidas de seguridad están la autenticación del origen de los datos, confidencialidad orientada a conexión, autenticación del origen de los datos, autenticación de identidad del extremo de la conexión, y el no repudio en el origen y la recepción de datos.

2.3 Delitos informáticos.

El infligir una norma o una regla especifica con intención o no, se convierte en un delito. Un delito informático está relacionado con las acciones que perjudican a un sistema informático donde se utiliza como herramienta la tecnológica para cometerlos.

Los delitos tienen sujetos activos y sujetos pasivos los primeros son los que cometen los delitos y los segundos son las víctimas, como sujeto activo se

encuentran los hackers y crackers y sujetos pasivos los usuarios atacados, las entidades bancarias, tecnológicas, etc. Todas aquellas que sus sistemas sean vulnerados.

Entre los delitos informáticos tenemos los siguientes:

- Sabotaje informático consiste en dañar la red en su parte lógica o física a través de su hardware y software.
- Fraude a través de los host en cual consiste en la manipulación de datos falsos para generar ganancias. Por ejemplo: phishing o pharming, suplantar páginas de instituciones bancarias.
- Copiar y vender derechos de autor como música, películas y programas. Ejemplo: pirata informático.
- Acceso a los sistemas no autorizados con objetivos dañinos o por desafío aquí entran los hackers y crackers.
- Manipulación de programas o modificación de la información sin autorización. Ejemplo: tampering.
- Plagio de datos encriptados mediante un dispositivo electrónico. Ejemplo: claves de cajeros y tarjetas de crédito ah este ataque se le conoce como skimming.
- Acoso a una persona mediante la tecnología conocida como *cyberbulling*. Ejemplo: acoso a través de las redes sociales.
- Pornografía infantil.

2.3.1 Legislación nacional del Ecuador.

Mientras se trabaja en el nuevo código orgánico integral penal se trabaja con leyes supletorias ya que los artículos vigentes tienen más de una década se ocupa con los artículos de la legislación ecuatoriana indicados en la siguiente tabla:

Tabla 1. Artículos del código penal del Ecuador.

Articulo	Detalle	Castigo
202 A	La violación de sistemas de seguridad para obtener información, que se rompa la confidencialidad, reserva y secretos a través de cualquier medio informático. Si la información es de índole comercial o de seguridad nacional.	3 – 6 meses de prisión y 500 USD de multa. 1 – 3 años de prisión y 1500 USD.
202 B	La utilización de la información personal para la malversación de esta sin autorización de su titular o titulares.	2 meses - 2 años de prisión y de 1000 – 1500 USD
262	Empleado o encargado público que destruya o suprima documentos, títulos, programas, datos, base de datos o cualquier mensaje de sistema o de la red o de que fueran depositados en su calidad de tales o encontrados sin razón al cargo.	3 – 6 años de prisión.
353	Es culpable de falsificación electrónica quien con ánimo de lucro o para causar perjuicio utilizando cualquier medio altere, modifique y simule un mensaje o parte induciendo un error.	Sancionados de acuerdo a los artículos mencionados aquí.
415 A	El causante de cualquier modo o con un medio de destruir, altere, utilice, suprima, dañe de forma temporal o definitiva la información o la red se considera como	6 meses – 3 años de prisión. 60 – 150 USD.

	daño informático.	
415 B	Si no se tratase de un delito mayor la destrucción, alteración, utilización de la infraestructura o instalaciones físicas necesarias para la transmisión de información.	8 meses – 4 años de prisión. 200 – 600 USD.
353 A	Se considera apropiación ilícita los que utilizan fraudulentamente sistemas de información o redes eléctricas para facilitar la apropiación del bien ajeno, quien procure la transferencia no consentida de bienes, valores o derechos de una persona perjudicándola.	6 mese – 5 años de prisión. 500 – 1000 USD.
353 B	Si para la apropiación ilícita ha empleado sistemas de alarma o guardas, descubrimiento o descifrado de claves secretas o encriptados, controles o instrumentos de apertura a distancia o la violación de seguridades electrónicas, informáticas o semejantes.	1 – 5 años de prisión. 1000 – 2000 USD
563	La persona que cometiera un delito utilizando cualquier medio o medios electrónicos o telemáticos.	La pena máxima de prisión establecida en estos artículos y de 500 a 1000 USD

Nota: Se muestran los artículos con su acción y con su respectiva sanción en el Ecuador.

Complementado con la ley de comercio electrónico y firmas, la resolución 55/63 aprobada por la asamblea de la ONU y convenio de cibercriminalidad de Budapest.

El desconocimiento de la ley no exime de responsabilidad a los causantes de los daños o perjuicios a los sistemas de información, redes de datos, infraestructuras

de red, apoderamiento de información de terceros sin consentimiento, descifrado de claves y falsificación de la información serán castigados con los artículos previstos en la legislación ecuatoriana.

2.3.2 Legislación internacional de los Estados Unidos de América.

La legislación Norteamérica apareció en 1985 con la ley federal de protección de sistemas, en 1986 se implementa en más estados y en 1994 se adopta el acta federal de abuso computacional, modificando el acta de 1986. Conocido como la 18 U.S.C sección 1030.

"(18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos muy técnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. Como todos los países del mundo han adoptado la informática para el desarrollo de sus actividades, existen también convenios internacionales que tratan de normas y evitar los delitos informáticos, así: TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE (TLC), firmado por México, Estados Unidos, Canadá en 1993, con un apartado sobre propiedad intelectual, la sexta parte del capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución. El Acuerdo General de Aranceles Aduaneros y Comercio (GATT), en su ronda uruguaya, en este acuerdo en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, será protegido como creaciones de carácter intelectual. En Europa se ha constituido la BUSINESS SOFTWARE ALLIANCE (BSA), que es

una asociación que actúa legalmente contra la piratería informática en Europa, Asia y Latinoamérica.”

(http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426)

2.4 Auditoria de seguridad informática.

¿Qué es una auditoria?

Es una visión de la estructura de la empresa cuya función es analizar y apreciar los planes, objetivos, controles, forma de operación, equipos humanos y físicos para identificar los que requieren de mejoras.

¿Qué es auditoria de seguridad informática?

Es el uso de herramientas o técnicas de forma ordenada y lógica, que permitan detectar deficiencias en los sistemas, estructuras y servicios, con los que se consigue elaborar acciones preventivas y correctivas para eliminar los problemas que se detectan.

¿Qué es el proceso auditable?

Consiste en el análisis de métodos relacionados con la seguridad, pueden ser físicos, lógicos o de los dos, orientados a la protección de la información. Se basa en la elección un método o metodología aplicable que sea estable, difundida y libre.

2.5 ISOS sobre seguridad.

La gestión, auditoría y certificación de la seguridad de la información se basa en la norma 27000 y su serie de estándares. Sus 2 primeras derivaciones o estándares, las normas ISO 27001 y 27002 son la base complementadas con las siguientes. Una es la ISO 27005 que establece el marco de referencia para la gestión de riesgos. La otra, ISO 27004, trata las métricas para medir el desempeño de las medidas de seguridad. Complementado con la ISO 27003 con la especificación, planeación, implementación y aprobación de un sistema de gestión de seguridad de la información SGSI.

2.5.1 La ISO 27000.

Lo primordial en una organización es la información puesto que es su activo más importante, proteger este es la base de un sistema de información seguro. Esta ISO está compuesta por un conjunto de normas y estándares siendo desarrollados o ya desarrollados por la IOS Organización Internacional de Estandarización y la Comisión Electrotécnica Internacional IEC, que son los encargados de establecer un marco de gestión parar la seguridad. Esta estándar proporciona un concepto general a las normas que la componen que van desde la 27000 a 27019; 27030 a 27044 y su finalización en 27799.

Fue publicada en el 2009 el 1 de Mayo y su segunda edición 1 de Diciembre del 2012

2.5.2 La ISO 27001.

Es la norma principal de la serie en la que se basan las organizaciones a nivel mundial para establecer sistemas de gestión de seguridad informática. Las auditoras se basan en esta norma para realizar los procesos de control en las organización como herramienta utilizan anexos A, B y C.

El anexo A es un resumen que determina una serie de controles como objetivos a cumplir para un sistema de gestión de seguridad informática se aplican los controles que desarrolla la ISO 27002 de 2005.

Fue publicada el 15 de Noviembre del 2005 y está bajo supervisión de un comité con su fecha de publicación para 2014.

2.5.3 La ISO 27002.

Es una guía de buenas prácticas que indica los objetivos de revisión y controles para la seguridad de la información en las organizaciones. Está formado por 39 controles y 133 objetivos de control agrupados en 11 directrices.

Fue publicada el 1 de Julio de 2007 y no es certificable.

2.5.4 La ISO 27003.

Es la guía que muestra las normas, controles y aspectos críticos para el diseño y la implementación de un sistema de gestión de seguridad informática SGSI. Indica el proceso de especificación y diseño desde la creación hasta la implementación de planes de realización. Indica del proceso para la obtención de aprobación por parte de la dirección para implementar un SGSI.

Fue publicada el 1 de Febrero del 2010 y no es certificable.

2.5.5 La ISO 27004.

Indica la utilización de medidas o métricas que pueden ser aplicadas para conocer la eficiencia o eficacia de un sistema de gestión de seguridad informática SGS y de los controles o grupo implementados según la ISO 27001.

Fue publicada 15 de Diciembre del 2009 y no es certificable.

2.5.6 La ISO 27005.

Indica las directrices para la gestión de riesgo en la seguridad de la información. Apoya los conceptos de la ISO 27001 y ayuda a la aplicación satisfactoria de la seguridad de información con una orientación en los riesgos.

Fue publicada 15 de Junio del 2008 con segunda edición el 1 de Junio del 2011 y no es certificable.

2.5.7 La ISO 27006.

Determina y especifica los requisitos para acreditar a las entidades que quieren realizar auditorías y certificación de sistemas de gestión de seguridad de información.

Fue publicada 1 de Marzo del 2007 con segunda edición 1 de Diciembre del 2011.

2.5.8 Evaluación de riesgos.

Una evaluación de riesgos está compuesta por la visualización, planificación, prevención, reducción y detección de los factores que pueden ocasionar conflicto

en un sistema. Tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de los datos de los usuarios.

La magnitud del conflicto que perjudique al sistema de forma económica, determina las respuestas que debe tener la red, entra aquí la visión de las personas encargadas de la evaluación para calcular donde pueden ocurrir los conflictos.

El nivel de seguridad a implementar depende del riesgo al que está expuesto lo que se vaya a proteger y de su importancia, las organizaciones realizan sus diferentes funciones en busca de ganancias económicas, por ende los niveles de seguridad obedece al nivel de riesgo de cada elemento de la red.

SI se establecen categorías baja, media y alta para los posibles ataques a la red o sistema, con una posibilidad baja hay una seguridad baja y no muy costosa. Ejemplo: los incendios no son algo muy común y con la disponibilidad de extintores se solucionaría el conflicto. Por otra parte con una posibilidad media se genera en una seguridad más alta y a un coste mayor. Ejemplo: Fallas de equipos, el reemplazo ya tiene un costo adicional, la implementación por software antivirus para contrarrestar virus, gusano, y de más, la implementación de seguridad para los acceso no autorizados general un costo a la empresa. Finalmente los posibles riesgos altos necesitan herramientas de seguridad altas.

Ejemplo: El ataque a la red y apoderamiento de información, donde se necesita implementar equipos de seguridad como firewalls que generan un costo mayor, el robo de equipos importantes dada el costo de su reposición es elevado.

2.5.9 Plan de contingencia.

Para conocer un sistema en su totalidad es necesario realizar esta auditora informática, la cual permitirá establecer una respuesta concreta que mejore o restaure su desempeño y disminuya las probabilidades de ser atacada. Además permitirá conocer los puntos a corregir en esta red, por lo cual el proceso de control se hará punto a punto en su estructura para transformar debilidades en fortalezas y lo ideal para poder desarrollar una respuesta a los problemas que se

den, conocer el estado, el funcionamiento, la utilidad de los elementos que la componen. Partiendo de estos conocimientos se puede desarrollar un plan de respuestas que solvente el funcionamiento del sistema a cuidar.

Las estrategias pueden ser muy variadas dependiendo de los recursos y lo que se vaya a proteger. Sin embargo no hay un plan que garantice ser completamente seguro.

Como plan de contingencia se puede priorizar el cuidar los elementos de la red más importantes, el servidor es uno de ellos, la solución está en el backup de archivos del mismo, que permite recuperar la información integra que se va almacenado y poder restablecer al estado anterior a la falla.

Otra forma de conocer las posibles falencias es con un personal interno o externo contratado dedicado a realizar pruebas de rendimiento, control y vulnerabilidades de la red.

2.6 Comercio electrónico.

El comercio se conoce como la actividad social y económica que se realiza para adquisición de bienes o servicios a través de un intercambio económico para generar una utilidad o ganancia. Si está implicada la tecnología en esta transacción se conoce como comercio electrónico.

Está involucrado en la transmisión electrónica de datos que los usuarios utilizan para comprar o vender un producto, bien o servicio.

Para poder realizar el comercio electrónico se dispone de varias formas de concretar la transacción depósito bancario, transacción bancaria, tarjetas de crédito, firma electrónica y dinero.

2.6.1 La firma electrónica.

La firma es un instrumento legal que disponemos para concretar un contrato amparado en los estatutos legales vigentes, como su contraparte física la firma digital tiene la misma valides que esta y se encuentra normada en la ley de comercio electrónico. Su composición es un conjunto de datos 0 y 1 que se

añaden a un archivo encriptado.

2.6.2 Ley de comercio electrónico del Ecuador.

La composición de esta ley permite establecer parámetros o reglas sobre el uso de la información de pertenecía y de protección de la misma así como las sanciones a quien o quienes incumplan con estas normas o estatutos expuestos en ella.

Considerando que en cualquier estado o país es indispensable que cuente con las herramientas jurídicas para proteger el uso de los medios electrónicos, la red de información, el comercio electrónico y los medios telemáticos. Se ha desarrollado esta ley para regular, controlar los mensajes electrónicos en sus diferentes medios, así como la firma electrónica los servicios descertificación, la contratación electrónica y telemática, presentación de servicios electrónicos como el comercio electrónico y la protección a los usuarios de estos sistemas.

Con esta ley se permite reconocer los principios de comercio electrónico, firmas electrónicas y mensajes de datos. La certificación de la firma electrónica, entidades de certificación de información y organismos de promoción de servicios electrónicos.

Además indica las leyes para los servicios electrónicos, contratación electrónica, telemática, los derechos de los usuarios e instrumentos públicos y de la prueba con las notificaciones electrónicas.

La legislación del Ecuador consta con esta ley, con un total de 64 artículos de los cuales se enumeran los más relevantes:

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

“Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellos referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del

momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

Ser individual y estar vinculada exclusivamente a su titular; que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos, que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado. Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario y que la firma sea controlada por la persona a quien pertenece.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento.

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa sobre:

Su derecho u opción de recibir la información en papel o por medios no electrónicos, su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción, los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada y los procedimientos para que posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir."

(http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=48%3Anormas-del-sector&id=98%3Aley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&Itemid=103).

2.7 Tipos de ataques por niveles.

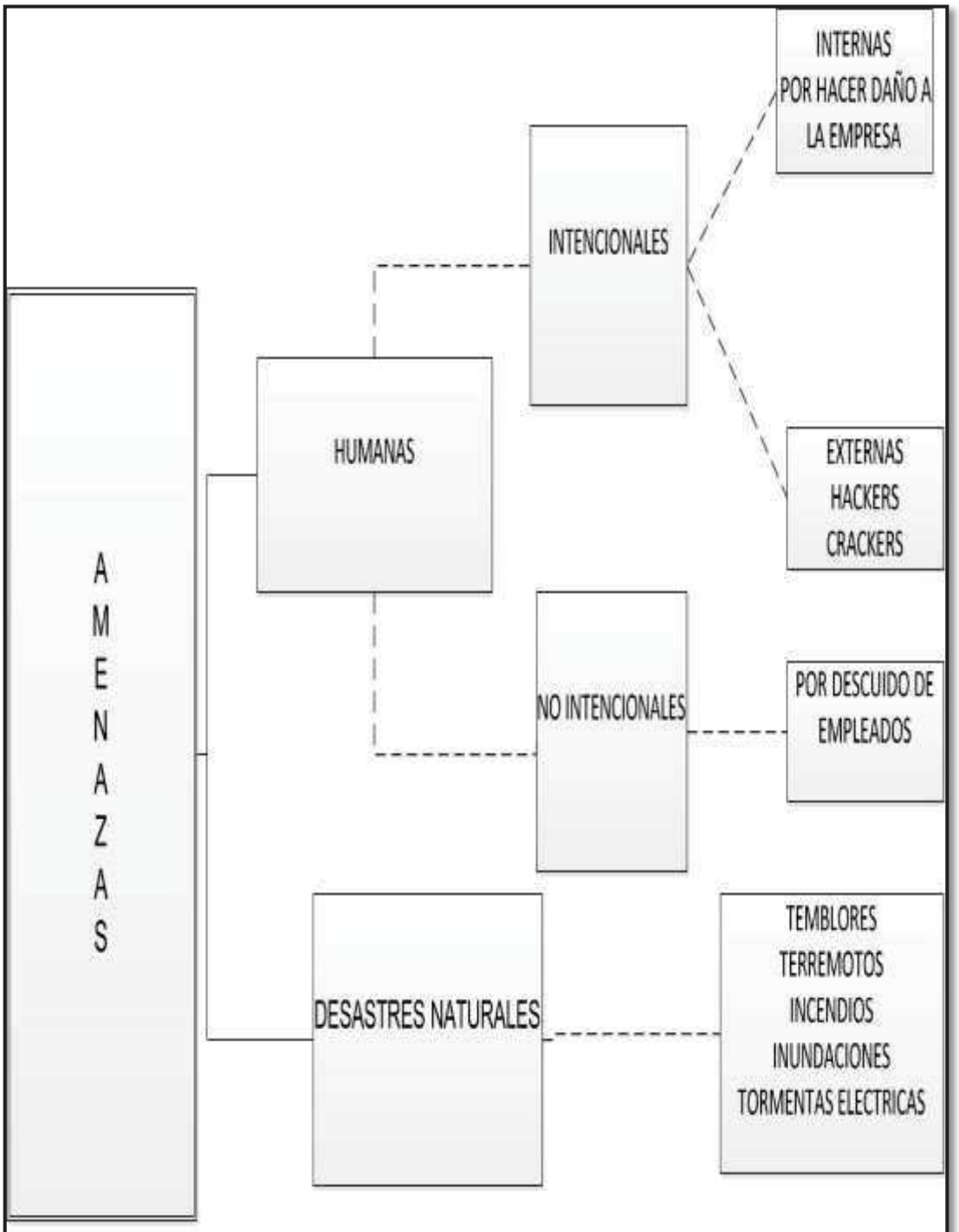


Figura 6. Clasificación de las amenazas.

Elaboración propia.

a. Se dividen las amenazas en 2 niveles principales con sus respectivos factores de influencia.

2.7.1 Nivel externo no intencional natural.

En este nivel se encuentran los desastres naturales como inundaciones, incendios y terremotos. Aquí los elementos físicos son los que se ven afectados.

2.7.2 Nivel usuario no intencional.

En este nivel se encuentra los usuarios internos, empleados que por la mala utilización de los equipos provocan que estos sufran daños. Incluso por utilización de software desconocido que en su contenido posee malware. La ignorancia no exime de responsabilidad.

2.7.3 Nivel usuario intencional hacker.

En este nivel encontramos usuarios o personas que sin autorización accede de forma física o a través de software a la red con propósitos desconocidos. Su meta varía dependiendo de cada persona y pueden ocasionar desde leves hasta graves perjuicios al sistema. Entre ellos tenemos a los hackers y crackers.

“El hacking físico: Se llama así al acto de estar frente al servidor o terminal interna, con las manos puestas sobre el la máquina desde la que el intruso intenta comprometer a la organización y sin permiso apropia, desvía, copia, destruye o altera información de la misma.” (Tori. 2008. P. 290).

2.7.3.1 El hacker y cracker.

Un hacker es el que cuenta con un conocimiento superior en lo que respecta a la programación. Su motivación es diversa y en muchos casos la curiosidad es la causa de su actividad. No busca un objetivo económico más bien un reconocimiento de su capacidad.

El cracker es aquel usuario que se especializa en realizar ataques a sistemas informáticos y su motivación es la obtención de un premio o ganancia económica.

2.8 Herramientas de seguridad.

Las herramientas de seguridad que disponen las redes de comunicación son varias entre las más comunes tenemos firewalls, antivirus, analizadores de la red como *bindview*. Las herramientas son varias y la utilización depende de los administradores de la red.

2.9 Situación Actual.

La situación actual determina el estado de los elementos que componen la red o el sistema informático así como su composición y características. Permite conocer los componentes de que forman la estructura además de los detalles de su funcionamiento.

2.9.1 Formación de la estructura de red.

"Las redes tienen tres niveles de componentes: software de aplicaciones, software de red y hardware de red:

• **El software de aplicaciones,** programas que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).

• **El software de red**, programas que establecen protocolos para que los ordenadores se comuniquen entre sí. Dichos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes.

• **El hardware de red**, formado por los componentes tangibles que unen los ordenadores. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, además recibe paquetes desde el software de red y transmite instrucciones y peticiones a otros ordenadores.

Las redes están formadas por conexiones entre grupos de ordenadores y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. En estas estructuras, los diferentes ordenadores se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Dichos servidores son ordenadores como las estaciones de trabajo, pero con funciones administrativas y están dedicados en exclusiva a supervisar, controlar el acceso a la red y a los recursos compartidos. Además de los ordenadores, los cables, existe en la red el módem para permitir la transferencia de información convirtiendo las señales digitales a analógicas y viceversa. También existen en esta estructura los llamados Hubs y Switches con la función de llevar a cabo la conectividad."

(http://ticsredesinformaticas.blogspot.com/2009/07/estructura-de-las-redes-las-redes.html).

La red está compuesta por un conjunto de elementos funcionales y operativos que permiten brindar el servicio para el cual fueron creados. Todas las redes constan de los elementos detallados anteriormente, además estos son primordiales para su funcionamiento dentro de la empresa o entidad a la que están sujetos.

2.9.1.1 Hardware de red de la empresa.

En la estructura tiene un conjunto de 7 computadores con sistema operativo Windows xp formando una red con topología estrella, la cual posee un cableado UTP categoría 5e, 1 impresora compartida en red, 1 switch d-link que realiza la función de repetidor de la señal que proviene de un punto de acceso que funciona como WDS (sistema de distribución wireless), Ubiquiti Airos nano station, el cual recibe la señal del proveedor por medio de wireless emitida desde una antena con dirección IP pública.

Características del hardware:

Tabla 2. Características computador 1.

Computador 1	Particularidad
Procesador	dual core
Memoria	4 Gb de RAM
Almacenamiento	Disco duro de 250 GB
Unidad De Disquete	Si
Unidad Óptica	Si
Puertos USB	Si
Parlantes	Si
Auriculares	Si
Teclado y monitor	Si
Mouse	Si

Nota: Se relación los factores de disponibilidad de elementos del cyber xpress con sus respectivas características.

Tabla 3. Características computador 2, 3, 4, 5, 6.

Computador 2	Características
Procesador	Pentium 4 CPU 3.20 GHz
Memoria	1 Gb de RAM
Almacenamiento	Disco duro de 80 GB
Unidad De Disquete	Si
Unidad Óptica	Si
Puertos USB	Si
Parlantes	Si
Auriculares	Si
Teclado y monitor	Si
Mouse	Si

Nota: Se relación los factores de disponibilidad de elementos del cyber xpress con sus respectivas características.

Tabla 4. Características Access Point Airmax Ubiquiti.

1 Access Point Airmax Ubiquiti Nanostation M2 630mw 2.4ghz.
· Procesador Atheros MIPS 24KC 400MHz
· Memoria de 32MB SDRAM y 8MB Flash
· Soporta Power over Ethernet Pasivo
· Dispone de dos puerto Ethernet 10/100Mbps
· Enclosure para Outdoor
· Antena incorporada de 16dBi de ganancia (5.475-5.825GHz)
· Barrido de onda Horizontal: 43º
· Polarización Vertical
· Incluye Kit de Montaje
· Incluye Fuente de Poder / PoE
· Ajuste de Velocidad
· Soporta encriptación WPA, WPA2, TKIP, AES, WEP
· Soporta filtrado por MAC
· Soporta diferentes modos de operación: Acces Point, WDS, Cliente
· Temperatura de Operación -40C a 85C
· Humedad 5 a 95%
· Puede establecer conexiones sobre 15km
. Ajuste de Canales a 10/20/40 MHz

Nota: Se enlista los factores de operatividad y características del equipo ubiquiti que opera en el cyber xpress.

Tabla 5. Características del Switch.

Características de D-link DES-1008D Switch 8 Puertos 10/100Mbps
Características
- Conmutador Nivel 2 - 8 puertos 10/100Mbps - Soporte full-dúplex y half-dúplex para cada puerto - Puerto de interconexión MDI para expansiones sencillas - Autocorrección de la inversión de polaridad rx - Gama completa de LEDs de diagnosis - De pequeñas dimensiones, ligero - FCC Clase A, Marca de la CE, VCCI Clase A, C-Tick, BSMI Clase A - UL, CSA
Prestaciones
- Método de conmutación: Store and Forward - RAM buffer asignado dinámicamente para cada puerto - Autoaprendizaje de la configuración de red - Control de flujo IEEE 802.3x - Porcentajes filtro/envío de los paquetes Ethernet: 14,880 pps por puerto - Porcentajes filtro/envío de los paquetes Fast Ethernet: 148,800 pps por puerto - Tabla de filtro para direcciones: 1K por dispositivo - RAM buffer: 1MB por dispositivo

Nota: Se enlista las prestaciones de operatividad y características del equipo D-link DES-1008D que opera en el cyber xpress.

Tabla 6. Características de la impresora.

CANON Epson artisan 835
Caracterísi cas
Impresión, copia y escaneo Inyección a tinta. Entrada máxima de 120 hojas. Fax. Velocidad de modem 33.6. kbit/s. Numero de cartucho 6. Imprime DVD/CD. Conectividad con o sin cables. Wireless LAN b,g,n. Ethernet. Wifi. Pantalla LCD táctil 7.8

Nota: Se enlista las características del equipo CANON Epson artisan 835 que opera en el cyber xpress.

2.9.1.2 Software de red de la empresa.

Esta estructura posee un software de administración de servicio para controlar el tiempo que los usuarios disponen para utilizar en la maquina respectiva.

Tabla 7. Software de red.

software de control y seguridad
El CiberControl versión 4.0 pro. C. cleaner MacAfee security scan plus USB disk security Avast free antivirus

Nota: Se enlista los programas y herramientas de protección disponibles en los equipos del cyber xpress.

2.9.1.3 software de aplicaciones.

Este sistema posee el software para el brindar un servicio para el que fue creado y cubrir las necesidades de los usuarios del mismo.

Tabla 8. Software de aplicaciones.

software de aplicaciones	licenciado
Windows XP professional service packs 3.	No
Microsoft office 2010	No
Juego Grand theft auto Vice city	No
Juego PES 2012	No

Nota: Se enlista los programas instalados en los equipos del cyber xpress.

2.9.2 Situación de la estructura de la red.

La estructura de red está dispuesta y armada conforme a las necesidades de la empresa, para poder brindar un buen servicio y satisfacer las necesidades de los usuarios.

La estructura en si está formada por una topología estrella, es decir formada por 7 computadores de escritorio, accediendo a un punto común. Un conmutador que permite la conexión en red y acceder a internet.

Los elementos de red están activos y operando. Su desempeño depende de la capacidad del punto de acceso central, esta estructura permite un fácil mantenimiento y expansión de los equipos que se pueden añadir. Si se va a retirar un equipo o se avería es fácil acceder a él.

La interfaz entre los ordenadores y los cables de red está activada por las tarjetas de red, la cual está preparando, recogiendo y enviando los datos que se están transmitiendo.

Tabla 9. Equipos de red y sus configuraciones.

Configuraciones de los equipos de red				
Equipo	Dirección IP	Mascara de red	Puerta de enlace	DNS
PC 1	192.168.192.101	255.255.255.0	192.168.192.1	192.168.192.1
PC 2	192.168.192.102	255.255.255.0	192.168.192.1	192.168.192.1
PC 3	192.168.192.103	255.255.255.0	192.168.192.1	192.168.192.1
PC 4	192.168.192.104	255.255.255.0	192.168.192.1	192.168.192.1
PC 5	192.168.192.105	255.255.255.0	192.168.192.1	192.168.192.1
PC 6	192.168.192.106	255.255.255.0	192.168.192.1	192.168.192.1
PC 7	192.168.192.107	255.255.255.0	192.168.192.1	192.168.192.1
IP P. Enlace	192.168.192.1			
IP Publica	186.46.213.3			
Enlace:	2 MB Compartido 2 a 1			Proveedor Wifinet

Nota: Se muestra las direcciones de red asignadas a cada máquina del cyber xpress y las direcciones del enlace que permite ver la organización de la red.

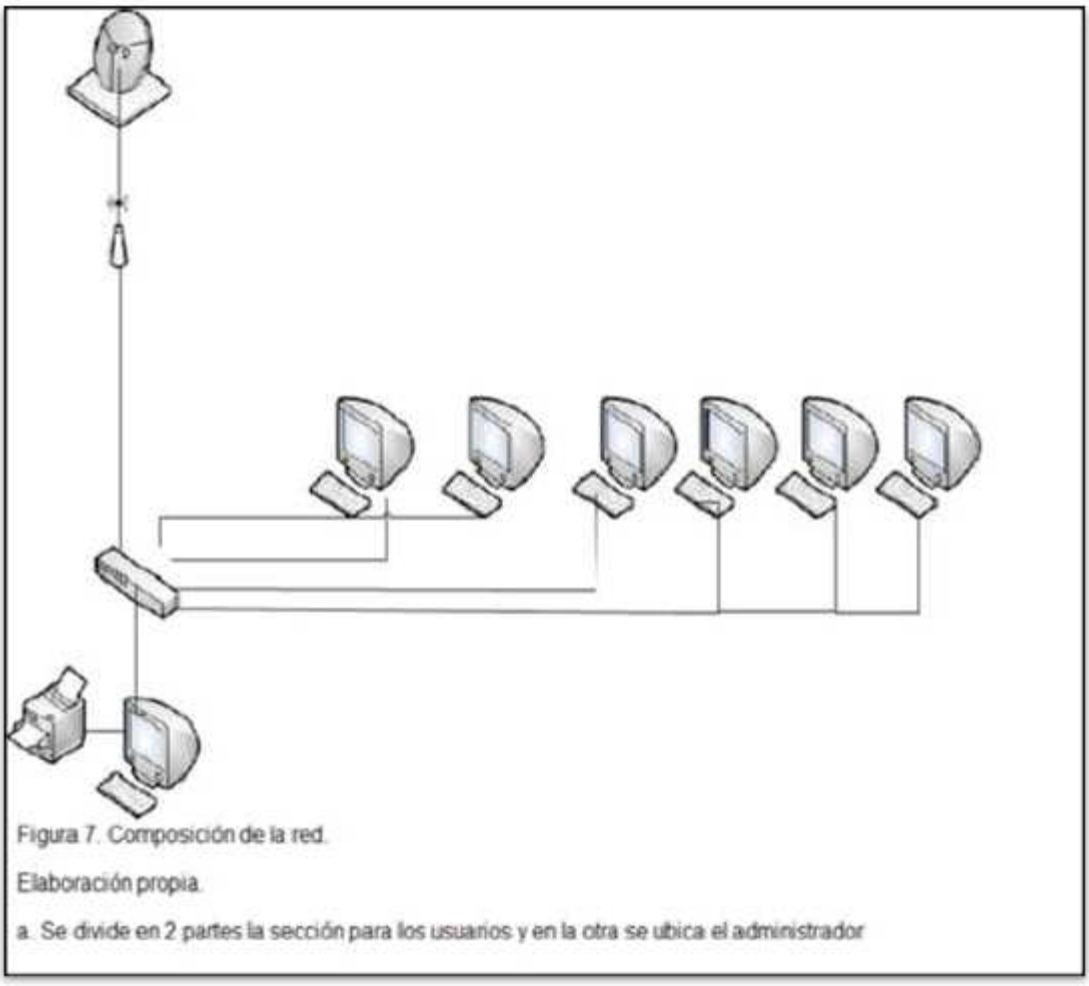


Figura 7. Composición de la red.

Elaboración propia.

a. Se divide en 2 partes la sección para los usuarios y en la otra se ubica el administrador

2.9.3 Estado actual de los elementos que conforman la red.

Los elementos de la red se encuentran operando normalmente en sus respectivas funciones, el estado de cada componente en particular se detalla a continuación:

Tabla 10. Estado de los elementos de la red.

	Detalle de los elementos
Equipos PCs:	Ubicados de forma continúa para mantener un control de estos y están en funcionamiento.
Cableado horizontal:	Cableado UTP categoría 5.
Cableado vertical:	Es un cable UTP categoría 6e que conecta el modem satelital que recibe la señal del ISP con el switch.
Switch:	Opera en modo repetidor.
Firewall:	Esta activo el de Windows que posee cada máquina.
Router:	No disponible
Access Point:	Punto de acceso que recibe la señal wifi y opera como guía de sistema de distribución wireless que capta una señal desde el Exterior.
Internet:	Acceso a través de la antena satelital vía wifi.
Impresoras:	Compartidas en red y funcionando.

Nota: Se enlista los factores de operatividad y características de los equipos del cyber xpress.

2.9.3.1 Disponibilidad del software contra ataques.

Tabla 11. Estado del software.

Software	Estado
C.cleaner:	Activo
Mcafee security scan plus:	Activo
Usb disk security:	Activo
Congelamiento de las maquinas.	Activo
Firewall Windows	Activo
Firewall De terceros	No disponible
Avast Free antivirus	Activo

Nota: Se enlista la disponibilidad de hardware de la red cyber xpress.

2.9.3.2 Disponibilidad del hardware contra ataques.

Tabla 16. Estado del hardware.

Hardware	Posee
Elemento físico contra ataques por software.	No
Puesta a tierra para descargas eléctricas.	No
Reguladores de voltaje.	SI

Nota: Se enlista los factores de disponibilidad de los equipos de la red cyber xpress.

2.9.3.3 Conformación del entorno en el que se encuentra la red.

Para determinar y explicar las causas que provocan este comportamiento en la red se empleará el razonamiento lógico y un análisis de diagnóstico. Para poder conocer al detalle el entorno de la red y los problemas de esta. Partiendo del conocimiento previo de los factores que la afecta como: la humedad, puesta a tierra incorrecta, ubicación y elementos externos.

La humedad en la red es casi nula, esta puede afectar los componentes de la estructura así como provocar pérdidas en el rendimiento de la red.

La puesta a tierra es una medida de protección que ayuda a corregir descargas eléctricas de los elementos de esta red.

La ubicación de los elementos está orientada a ubicar al cableado, utilizando las partes posteriores e inferiores de la estructura del edificio.

CAPÍTULO III

3 Estudio Realizado.

El conjunto de procedimientos realizados a continuación son determinados, para alcanzar los objetivos que rigen esta investigación, están basados en la norma ISO 27001 y la elección de las actividades que se aplican a esta empresa.

Las herramientas aplicadas para obtener la información, son la observación científica, hechos anecdóticos, listas de chequeo, entrevista, todo esto con el respaldo del administrador de la red.

Basado en la norma ISO 27001 Se realizó el siguiente plan de actividades.

1) Para conocer si el administrador tiene una política de seguridad documentada, se revisa continuamente su política de seguridad y se apoya la seguridad dentro de la organización, además se le realizara preguntas al administrador.
2) Con la visita al sitio se definirá si las responsabilidades de seguridad están dadas para usuarios y administrador.
3) Conocer el establecimiento para estudiar si hay requerimientos de seguridad, que permita Identificar los riesgos que corren los medios de procesamiento de información las computadoras.
4) Efectuar una investigación y estar al tanto de los permisos de acceso a la información por parte de los usuarios así como de los activos del establecimiento.
5) Respaldarse en el administrador para saber si la información recibe un nivel de protección apropiado y conocer responsabilidades o roles de los usuarios su asistente además de su grado de riesgo.
6) Realizar preguntas a los usuarios determina si estos están al tanto de amenazas y responsabilidades sobre la seguridad en el cyber.
7) Hacer una investigación y observación de la estructura de la red, conocer si están establecidos perímetros de seguridad físicos así como cuáles son

los controles de entrada físico y la seguridad en los medios.

8) Consultar al administrador su protección contra amenazas externas naturales.
9) Análisis de los equipos para saber si están bien ubicados y protegidos contra fallas de energía.
10) Analizar y basarse en hechos anecdóticos para saber si la protección del cableado eléctrico funciona contra intercepción o daño.
11) Revisar los equipos o lista de registro, para conocer el mantenimiento que se hace al equipo, además si hay una eliminación segura de los equipos en desuso. Que permita determinar si se tiene una operación correcta de los elementos del establecimiento.
12) Mediante la entrevista al administrador y observación a la estructura del establecimiento, conocer la política y las medidas de control de acceso implementadas. Además de cuál es el mantenimiento de los sistemas de información y estar al tanto de la gestión que se realiza ante eventos e incidentes en la red.
13) Con el apoyo de administrador y revisar, observar, determinar, investigar los planes o aspectos de seguridad para continuar con la actividad comercial, además de basarnos en la normativa de las ISO 27001 para conocer cumplimiento de políticas de seguridad.

3.1 Auditoria física.

3.1.1 Ataques de red físico.

El cyber no dispone de herramientas de seguridad para ataques de nivel de físico, puesto que hasta el momento no ha surgido este tipo de ataques, el administrador de la red no ha visto necesario la instalación de los mismos.

3.1.2 Control de acceso físico al cyber.

El establecimiento cuenta en su estructura con acceso libre a los equipos de los usuarios, sin embargo hay una delimitación con el área de control de la red, esta delimitación es controlada a través de la persona encargada de atender a los usuarios.

3.1.3 Control de acceso a los equipos.

El control físico de acceso a los medios de almacenamiento externos no está implementado, sin embargo la información de estos medios es exclusiva de los usuarios por lo tanto es de su propio interés cuidar estos medios. La información de las maquinas del cyber está disponible para ser copiada sin restricciones.

Se controla periódicamente los dispositivos físicos instalados en la red, así se evita el robo o daño de estos. Por el momento no se ha registrado el robo de algún equipo o elemento.

3.1.4 Control de acceso por áreas.

Un medio establecido como tarjetas magnéticas o control de quien accede y hacia donde no está establecido, por la funcionalidad del cyber no es necesario por el costo de esta implementación en comparación con el beneficio que se puede tener.

3.1.5 Cableado estructurado.

La normativa de cableado esta implementada en ciertas partes de la red mas no está totalmente prevista en todo el centro de cómputo, además no está debidamente ordenado todo el cableado y etiquetado, los puntos de red con sus respectivas direcciones.

3.1.6 Estado tarjetas de red.

La funcionalidad de las tarjetas está estable y cumple con los requerimientos del usuario, por el momento no se ha reportado fallas en ellas.

3.1.7 Condiciones de seguridad del establecimiento.

Las condiciones para tener una seguridad óptima no están implementadas completamente, sin embargo se cuenta con normas de uso de equipos que disminuyen el riesgo de actos ilícitos y emergencias.

En control de ingreso de bebidas, alimentos y tabaco es una medida de control de seguridad implementada que evita que estos elementos puedan dañarlos.

El conocimiento de las actividades que están realizando los usuarios mediante el software que funciona en la máquina de control ayuda a mantener la seguridad.

3.1.8 Dispositivos contra incendios.

No cuenta con detectores de humo que son importantes en caso de un corto circuito que genere fuego.

No implementada señalización en caso de incendio, salida de emergencia no disponible y el establecimiento cuenta con una única salida que en caso de emergencia puede generar problemas.

3.1.9 Dispositivos contra descargas eléctricas.

Cada equipo de cómputo cuenta con un regulador de corriente para evitar que se averíen en una posible falla eléctrica.

No dispone de una planta eléctrica en caso de un corte eléctrico, los equipos no tienen un fluido eléctrico de respaldo. No hay una correcta puesta a tierra que debe tener una varilla de cobre de 3 mts, enterrada bajo el nivel del suelo en tierra húmeda, con sales y carbón.

No se tienen circuitos de cableado eléctrico para cada segmento de equipos de funcionamiento del establecimiento, es decir no hay un cableado exclusivo para las computadoras y otro para la luminaria.

No se cuenta con aire acondicionado que permita bajar la temperatura ambiente de las máquinas y que disminuya el riesgo de averías por sobrecalentamiento.

3.1.10 Plan de evacuación.

No cuenta con un plan de evacuación en caso de una amenaza de seguridad externa natural como un incendio, inundación, terremotos, etc.

3.1.11 Políticas de seguridad para usuarios.

A pesar de que las políticas de seguridad son establecidas por el administrador de la red, no todos los usuarios las conocen y las ponen en práctica.

3.1.12 Responsable de políticas, normas y procedimientos.

El administrador de la red es la persona a cargo de implementar según cree conveniente las políticas, normas y procedimientos de establecimiento.

3.1.13 Definidos responsabilidades y roles.

Los roles y responsabilidades si están definidos en este cyber, además de que el personal está capacitado para cubrir los requerimientos de los usuarios.

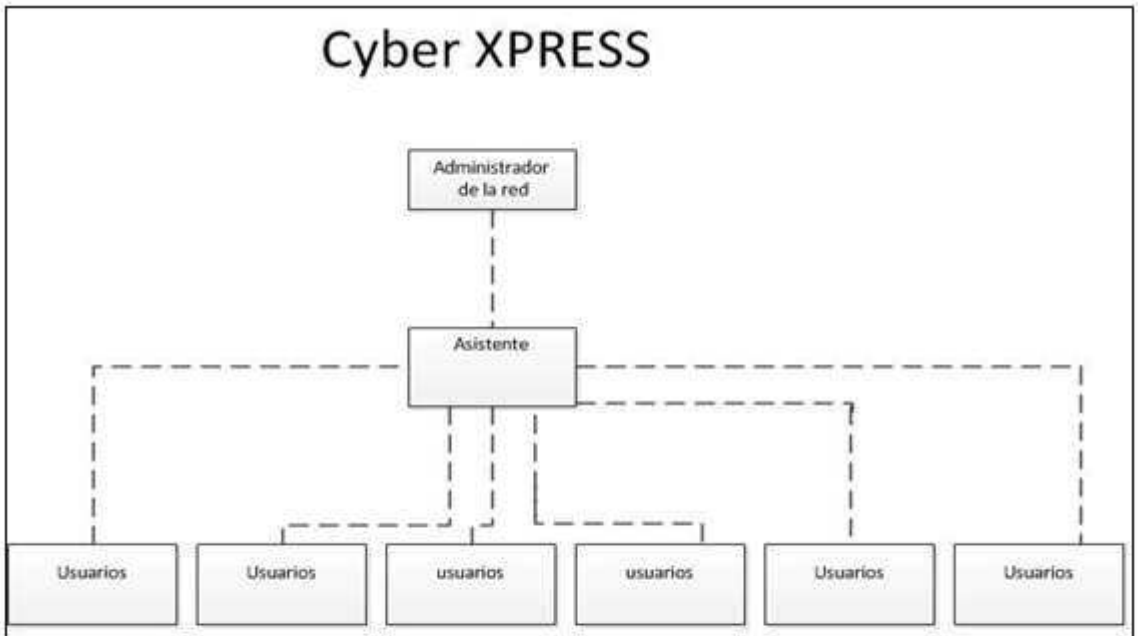


Figura 8. Esquema de composición de la empresa.

Elaboración propia.

a. Muestra como están formados los operadores de la empresa jerárquicamente.

3.1.14 Respaldo de equipos averiados.

Un reemplazo de equipos averiados no se puede realizar inmediatamente después de haber sucedido el percance puesto a que por el momento no se tiene elementos de respaldo, debido a que el costo de tener estos equipos sin trabajar no genera un beneficio para el establecimiento.

3.2 Auditoria lógica.

3.2.1 Ataques de red.

El software de protección para ataques esta implementado en su forma más básica y económica. La utilización de antivirus, *firewall* de *Windows*, *usb disk security*, *c.cleaner* satisfacen las necesidades que hasta el momento ha generado la red.

3.2.2 Contraseñas de acceso.

La utilización de las contraseñas está siendo implementada en el establecimiento esto permite controlar la utilización de los equipos y las contraseñas son implementadas por el administrador de la red.

3.2.3 Respaldo de los datos.

No hay un servidor donde estén respaldados los datos del centro de cómputo y de las maquinas puesto que un computador central está encargado del control de las maquinas a través de software ciber control 4.0.

El respaldo de las maquinas se da a través de la clonación, si se avería una de estas un respaldo clonado la restaurara al modo anterior.

3.2.4 Control de instalación de software.

El control lo realiza el administrador cuya configuración tiene a las maquinas en modo congelamiento. Gracias a esto después de apagarse las maquinas vuelven al estado en el que se encontraban al prenderse. No dispone de un software específico para control de las instalaciones de programas.

Las actualizaciones no están activadas automáticamente y el encargado de hacerlas es el administrador de la red.

3.2.5 Respaldo del software instalado.

Las aplicaciones que utilizan en este establecimiento se encuentran respaldadas en imágenes ISO.

3.2.6 Software licenciado.

El software que posee la empresa es ilegal excepto por los 2 antivirus en sus versiones free:

- *MacAfee security scan plus* antivirus.
- *Avast free* antivirus.

3.2.7 Control de los elementos externos.

El control de los elementos externos esta implementado a través del programa USB Disk Security.

3.2.8 Inventario de los elementos.

No se precisa de un inventario completo y detallado de los equipos disponibles en la red.

3.2.9 Control del mal uso de los equipos.

El control del mal uso del equipo y de las aplicaciones que corren sobre los mismos esta dado a través del programa cyber control 4.0 de administración de tiempos y recursos de la computadoras.

3.2.10 Normas del entorno de la red.

Como el establecimiento está ubicado junto a uno mecánica de enllantado se tiene mucho riesgo de alguna amenaza a la red. Por lo tanto respecto a la ubicación no se tomó como referencia normas de seguridad.

3.2.11 Comercio electrónico seguro.

En el cyber no se puede realizar comercio electrónico seguro dado que las máquinas de los usuarios son controlados en lo que realizan desde la computadora de control y no se tiene privacidad al igual que medidas para una conexión segura.

3.2.12 Monitoreo de seguridad.

El cyber no cuenta con un programa exclusivo para control y monitoreo de los ataques de terceros a la red de información.

No hay implementación de redes virtuales privadas VPNs.

3.3 Mantenimiento de la Red.

3.3.1 Mantenimiento preventivo.

No existe una planificación de mantenimiento preventivo de los equipos, se realiza esporádicamente control de funcionamiento de equipos.

3.3.2 Mantenimiento correctivo.

Cuando surge la necesidad de mantenimiento de los equipos por un daño el administrador de la red se encarga de realizarlo.

3.3.3 Auditoria realizada con anterioridad.

No hay registro de un proceso auditable desde que se formó el establecimiento.

3.3.4 Realizado una evaluación de riesgos.

No se ha realizado una evaluación de las posibles averías y causas que se puedan dar en la estructura de la red.

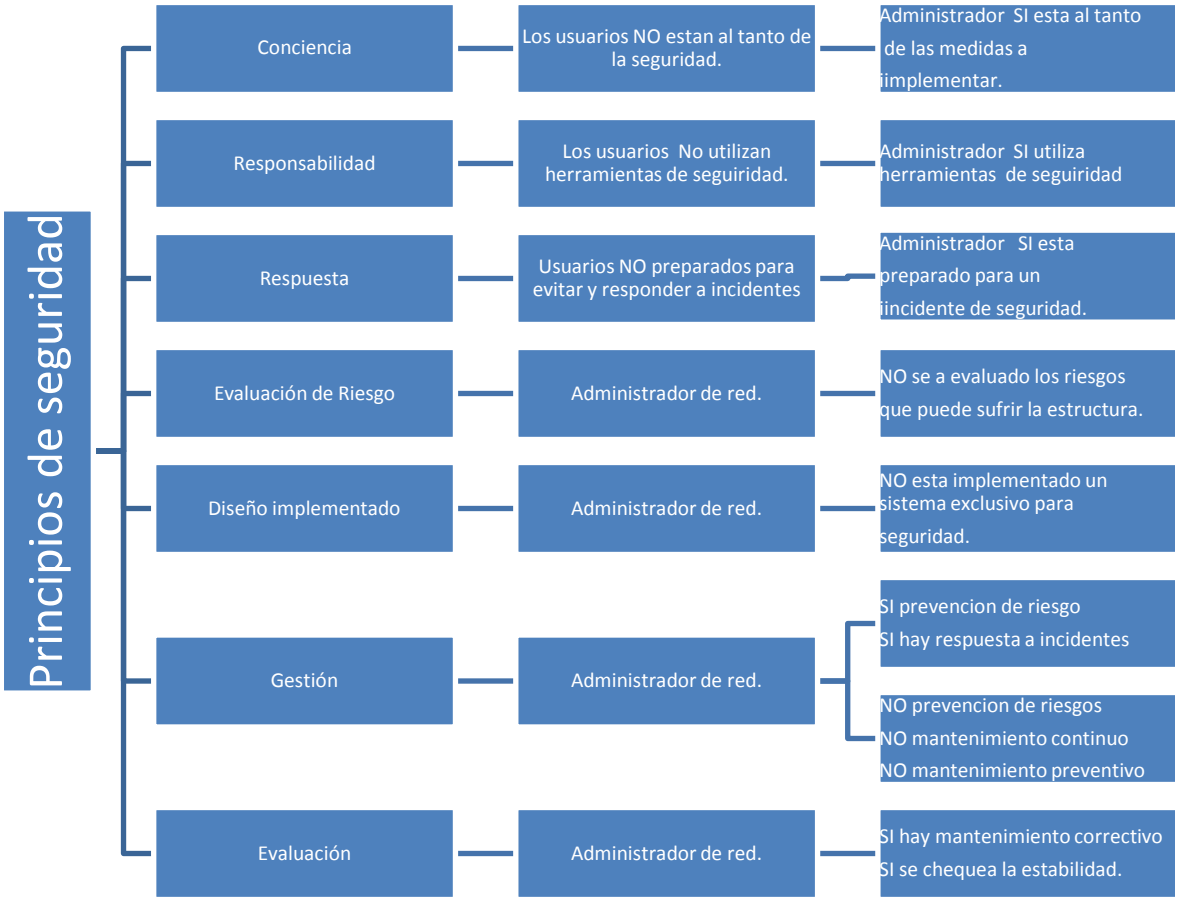
3.3.5 Plan de contingencia.

No existe un plan de contingencia debidamente elaborado indicando los pasos a realizar en caso de una amenaza de seguridad o para recuperarse después de un fallo del sistema.

3.4 Resultados.

Los resultados expuestos a continuación están basados en la norma ISO 27000 y en su norma primera 27001 y sus anexos A y B.

3.4.1 Diagrama 1: Principios de seguridad implementados en el cyber según anexo B:



3.4.2 Listas de resultados de los puntos de control según el anexo A:

Tabla 17. Lista de chequeo de los 10 puntos de control de la red.

	Punto 1	
N :	**Políticas de seguridad.**	**Indicación**
1	Tiene documentos de políticas de seguridad de sistemas de información.	NO
2	Se revisa regularmente la política de seguridad.	NO
3	Hay una persona responsable de las políticas de seguridad.	SI
	Punto 2	
N:	**Organización de la seguridad.**	**Indicación**
1	Existe una dirección clara, apoyo y asignación de responsabilidades.	NO
2	Están siendo coordinadas las actividades de seguridad según el rol del usuario.	SI
3	Existen claramente responsabilidades según las partes del establecimiento.	SI
4	Hay un proceso de control para los nuevos medios de información.	SI
5	Tiene acuerdos de confidencialidad de la información que opera en la red.	NO
6	Se revisa la implementación de controles de seguridad cada cierto tiempo.	NO
7	Existe control acceso a elementos externos.	NO
8	Hay control de seguridad de los activos del establecimiento.	NO

9	Existen contratos sobre la organización de seguridad con empresas externas.	NO
	Punto 3	
N:	**Gestión de activos informáticos.**	**Indicación**
1	Hay un inventario de activos.	NO
2	El inventario detalla la propiedad de los activos del establecimiento.	NO
3	Se implementa reglas para el uso de los elementos del establecimiento.	SI
4	Se dan a conocer las reglas para el uso de los elementos del establecimiento.	NO
5	Hay un responsable de los activos.	SI
6	Está clasificado el acceso a la información de acuerdo al usuario.	SI
7	Hay ordenamientos de etiquetado.	NO
	Punto 4	
N:	**Seguridad de los recursos humanos.**	**Indicación**
1	Están definidas las responsabilidades y roles de seguridad	SI
2	Hay un control sobre el encargado del establecimiento en torno a seguridad.	SI
3	Existen condiciones de seguridad en el contrato de trabajo.	NO
4	Existen procesos de seguridad claros a seguir.	NO
5	Se lleva un registro de los incidentes de forma detallada.	NO
6	Existe información que conozca los usuarios sobre vulnerabilidades.	NO

7	Se les da a conocer los usuarios que no deben de probar vulnerabilidades.	NO
8	Eliminación de derechos de acceso una vez terminada la sesión de un usuario.	SI
	Punto 5	
N:	**Seguridad Física y ambiental.**	**Indicación**
1	Hay elementos de seguridad físicos.	NO
2	Hay controles de entrada físico a las áreas importantes de la red.	NO
3	Hay protecciones contra eventos naturales.	NO
4	Existe control físico al personal que labora en el cyber.	NO
5	Hay protección frente a fallas eléctricas.	NO
6	Hay protección frente a humedad.	NO
7	La ubicación de los equipos permite que estén protegidos.	NO
8	La ubicación de los equipos importantes permite que estén protegidos.	SI
9	La ubicación de los equipos externos tiene seguridad.	NO
10	Hay seguridad sobre el cableado.	NO
11	La ubicación de los equipos previene recalentamientos.	NO
12	Los equipos averiados son reutilizados o sus componentes.	SI
13	Se tiene un control sobre la extracción de los equipos fuera del cyber.	SI
	Punto 6	
N:	**Gestión de comunicaciones y operaciones.**	**Indicación**

1	Están documentados los procedimientos de la política de seguridad.	NO
2	Hay un responsable de los cambios en los equipos	SI
3	Se conocen las responsabilidades en un incidente de seguridad.	SI
4	Está controlado el mal uso de los elementos del cyber por el administrador.	SI
5	Están delimitadas las áreas de la empresa.	SI
6	Hay una entidad externa encargada de la gestión.	NO
7	Se conoce la capacidad de proceso y almacenamiento de la red.	SI
8	Se implementa actualizaciones y modificaciones con criterios de seguridad.	NO
9	Dispone de control sobre software malicioso.	SI
10	Dispone de copias de backup de la información esencia del establecimiento.	NO
11	Hay adecuado manejo y control sobre la red.	SI
12	Se ha identificado y se lleva un registro de los fallos de la red.	SI
13	Hay controles sobre los medios externos USB, CD, ETC.	SI
14	Se utilizan procedimientos para la eliminación de medios informáticos	SI
15	Hay seguridad en la información.	NO
16	Hay acuerdos para el intercambio de información o software.	NO
17	Hay protección sobre los medios físicos de intercambio de información.	NO
18	Tiene medidas de seguridad sobre el comercio electrónico	NO

19	Tienen normas o herramientas para garantizar confidencialidad e integridad.	NO
20	Se pueden realizar transacciones en línea seguras.	NO
21	Se Monitorean el uso de medios de procesamiento de información.	SI
22	Hay registro de una auditoria previa	NO
	Punto 7	
N:	**Control de accesos**	**Indicación**
1	Existe política de control de accesos.	NO
2	Existe control y restricción de acceso.	SI
3	Hay registro de accesos.	SI
4	Se gestiona las contraseñas de usuarios.	SI
5	Se utiliza contraseñas.	SI
6	Existe una autenticación en los puntos de conexión.	SI
7	Hay políticas de uso sobre la red del establecimiento.	SI
8	Existe un control en la conexión de la red.	SI
9	Hay controles de acceso a las aplicaciones.	NO
10	Existe control a la computación móvil y tele- trabajo.	NO
	Punto 8	
N:	**Adquisición desarrollo y mantenimiento de los sistemas de información**	**Indicación**
1	Implementada la seguridad en los sistemas según los requerimientos.	NO

2	Existen herramientas para el correcto funcionamiento de las aplicaciones.	NO
3	Hay controles de protección para la confidencialidad eh integridad.	NO
4	Se garantiza la seguridad de la información.	NO
5	Hay un control de cambios seguros en los procesos que corren en la red.	NO
6	Existe un control para determinar las vulnerabilidades de la red.	NO
	Punto 9	
N:	**Gestión de incidentes en la seguridad de la información**	**Indicación**
1	Se reportan los eventos de seguridad.	NO
2	Se reportan por parte de los usuarios las debilidades de seguridad.	NO
3	Hay procedimientos de respuesta por parte del administrador.	SI
4	Existen definidas las responsabilidades ante un incidente.	SI
	Punto 10	
N:	**Gestión de la continuidad comercial**	**Indicación**
1	Existe un plan de continuidad del negocio.	NO
2	Hay una evaluación de riesgo para una continuidad de negocio.	NO
3	Se implementan planes de continuidad.	NO
4	Esta dentro de un marco la planificación del negocio.	NO
5	Se realiza pruebas, mantenimiento y re evaluación de plan de continuidad.	NO

	Punto 11	
N:	**Cumplimiento con requerimientos legales.**	**Indicación**
1	Existe cumplimiento de la legislación de seguridad	NO
2	Resguardo de la propiedad de la información	NO
3	Hay controles de auditoria.	NO

Nota: Se estudian los puntos de control en el cyber xpress para determinar las medidas de seguridad aplicadas por el administrador de la red.

CAPÍTULO 4

4 Conclusiones y Recomendaciones

4.1 Conclusiones.

- En relación a la operatividad del cyber se puede determinar que brinda un servicio estable y cubriendo los requerimientos básicos de los usuarios, dispone de capacidad ancho de banda suficiente para poder navegar en internet y que opera a velocidades moderadas con bajo porcentaje de errores.
- Utilizado la norma ISO 27001 da como resultado que la seguridad de la red es baja.
- Como amenazas en la parte física se detectó falta de elementos de seguridad, controles de entrada, protección contra eventos naturales.
- La vulnerabilidad en la red es a causa de la falta de políticas de seguridad.
- La estructura y la ubicación de los equipos no los protege.
- El ambiente en el que se encuentran no afecta la operatividad de los equipos.
- Los elementos que componen la red local están funcionando correctamente.
- No dispone de un método de seguridad específico para las acciones accidentales o intencionales de los usuarios que ocasionen daños.
- Conociendo la disposición de los equipos cubren las necesidades de las personas y están ubicados para fácil acceso de los usuarios.
- El personal está capacitado para brindar asistencia en el servicio básico o de ofimática a los usuarios.
- El centro cuenta con recursos de la red compartidos como la impresora, aplicaciones compartidas corriendo establemente como los juegos en red. Se tiene un buen control respecto a la medición de tiempo y cálculos totales a pagar por los usuarios.

- El control de equipos es bajo la regla de bloqueo y desbloqueo automático de equipos, la protección de estos es a través del software de defensa como antivirus Mcafee y Avast. Falta un software de control de acceso a las páginas web, la falta de un mantenimiento preventivo de equipos y cableado sin la normativa completamente correcta. Además no se lleva un registro documentado de aplicaciones instaladas. Los medios extraíbles no tienen un control físico el control de software malicioso se lo hace en su forma más elemental con antivirus y otros además las descargas eléctricas sin un medio de prevención, también de la no protección contra amenazas externa naturales. Corre el riesgo de interferencia por los elementos que disponen los locales adjuntos, así como el daño de los computadores por desconocimiento de los usuarios sobre la correcta utilización de los equipos.
- Si ocurren ataques a nivel físico no dispone de elementos que eviten un daño a la red, la delimitación de áreas en el cyber está dada, por supervisión del asistente y el administrador, sin un medio físico que controle al igual que el acceso de elementos físicos externos.
- Es necesario instalar software o hardware de seguridad y controles necesarios según la normativa.
- La estructura de red tiene capacidad de crecimiento además el acceso al sitio donde se encuentra ubicado el cyber es fácil para los moradores del sector.
- El estado de los componentes de la red es bueno tanto de las tarjetas como los equipos y las conexiones.
- No dispone de un servidor como tal donde se respalde la información, pero si cuenta con un computador central donde se ejecuta el programa de control cyber control 4.0, el control de instalación y actualización de software lo realiza el administrador de la red.
- Si dispone de software de respaldo, mas no se tiene licencias del mismo. No hay un inventario documentado de los elementos informáticos, el control del mal uso de los equipos esta cargo del administrador y del asistente además de que la herramienta de software de control ciber

control 4.0 le permite ver a las maquinas lo que están haciendo. No se ha seguido normas de implementación de la red.

- Se puede realizar comercio electrónico mas no es recomendable por que el sitio no cumple con todas las normas de seguridad indicadas por la ISO 2700, Además no cuenta con un programa exclusivo para control y seguridad de red.
- No se encontró rastro de auditoria previa.
- Mediante esta auditoría se detectó como puntos fuertes: la calidad de servicio brindado es óptima, hay capacidad de crecimiento de la red, el conocimiento del administrador es empleado en beneficio de los usuarios. En puntos débiles se encontró: falta de principios, políticas de seguridad y una organización de seguridad débil.

4.2 Recomendaciones.

- Se necesita dar a conocer a los usuarios sobre los posibles percances que pueden sufrir en la red, dar suficiente información. Es necesario tener una política de seguridad documentada y actualizada conforme lo necesite.
- Es aconsejable que se implemente controles de seguridad de hardware o de software.
- Es necesario que se lleve un inventario documentado de los equipos informáticos.
- Necesario un cableado implementado completamente con la normativa correspondiente y un registro documentado de aplicaciones instaladas, así como el correcto etiquetado de los componentes de la red.
- Se recomienda un control físico de elementos agregados a la red, el control y compra de software con licencia.
- Implementar protección contra amenazas externas naturales y educar a los usuarios sobre la correcta utilización de los equipos.
- Se necesita planificar y realizar un mantenimiento preventivo, una evaluación de riesgos, un plan de contingencia.
- Se requiere implementar condiciones de seguridad, dispositivos contra incendios, descargas eléctricas y un plan de evacuación.
- Se recomienda un servidor como tal donde se respalde la información importante para la red, la elección depende de las posibilidades económicas del cyber.
- Se sugiere implementar un firewall sea físico o por software que permita controlar las conexiones y así proveer de seguridad a la red. Las características de este firewall si está basado en Linux es preferible que el administrador tenga conocimientos previos de este sistema operativo el cual posee desventajas como el conocimiento solo de quien lo implemente, al añadir una nueva regla tendrá que volver a configurar a diferencia del físico que su configuración es más fácil, la elección depende de la inversión del administrador de la red.

REFERENCIAS

Alejandro Corletti Estrada. (2011) Seguridad por niveles. Madrid, España: creative commons.

Andrews. S. Tanenbaum. (2003) Redes de computadoras (4ta edición). Ámsterdam, Holanda: campus.

Carlos Tori. (2008). Hacking ético. Rosario, Argentina: el autor.

http://alberto3003.wikispaces.com (sf) Sistemas de fibra óptica. Recuperado el 6 de febrero del 2013 de: http://alberto3003.wikispaces.com/Sistemas+de+fibra+optica.

http://bryan.bligoo.ec (sf) Cable coaxial. Recuperado el 17 de Septiembre del 2012 de: http://bryan.bligoo.ec/cable-coaxial#.UAmwPWHCpkg.

http://es.wikipedia.org (sf) Carrier sense multiple access with collision avoidance. Recuperado el 6 de septiembre del 2012 de: http://es.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance.

http://materias.fi.uba.ar (sf) Cableado estructurado. Recuperado el 6 de Septiembre del 2012 de: http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf.

http://santydj.blogspot.com. (sf) Quienes somos. Recuperado el 12 de Enero del 2013 de: http://santydj.blogspot.com/p/quienes-somos.html.

http://support.microsoft.com (sf) Soporte. Recuperado 3 de Septiembre del 2012 de: http://support.microsoft.com/kb/103884/es.

http://ticsredesinformaticas.blogspot.com. (sf) Estructura de las redes. Recuperado el 16 de Noviembre del 2012 de: http://ticsredesinformaticas.blogspot.com/2009/07/estructura-de-las-redes-las-redes.html.

http://www.conatel.gob.ec. (sf) Normas del-sector. Comercio electrónico-firmas-electrónicas-y-mensajes-de-datos. Recuperado el 7 de Noviembre del 2012 de: http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=48%3Anormas-del-sector&id=98%3Aley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&Itemid=103.

http://www.derechoecuador.com. (sf) El delito informático. Recuperado el 31 de Octubre del 2012 de: http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426.

http://www.garciagaston.com.ar. (sf) Cableado estructurado. Recuperado el 17 de Octubre del 2012 de: http://www.garciagaston.com.ar/verpost.php?id_noticia=46.

http://www.garciagaston.com.ar. (sf) Cableado estructurado. Recuperado el 20 de Octubre del 2012 de: http://www.garciagaston.com.ar/verpost.php?id_noticia=46.

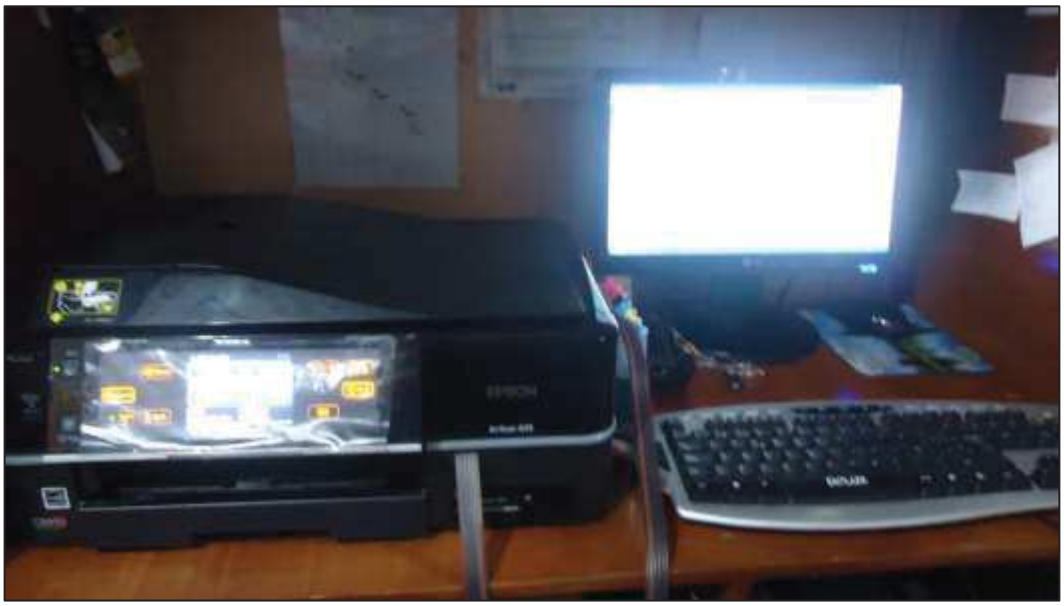
http://www.monografias.com (sf) Cableado. Recuperado el 27 de Septiembre del 2012 de: http://www.monografias.com/trabajos30/cableado/cableado.shtml.

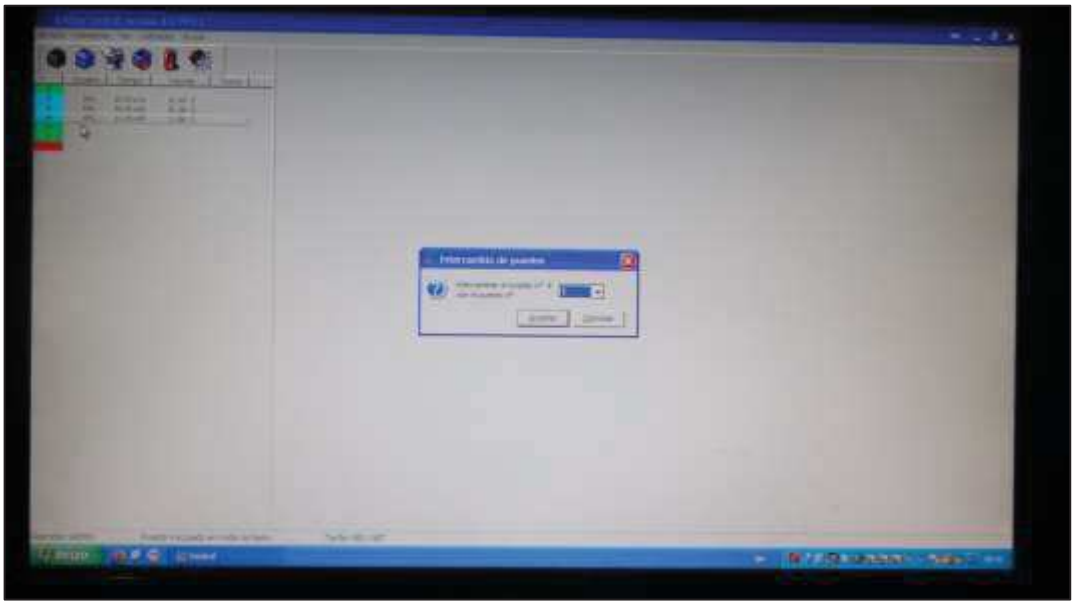
http://www.rnds.com.ar. (sf) Cable de par trenzado. Recuperado el 4 de Octubre del 2012 de: http://www.rnds.com.ar/articulos/052/RNDS_136W.pdf.

http://www.see-my-ip.com (sf) Niveles OSI. Recuperado 3 de Septiembre del 2012 de: http://www.see-my-ip.com/tutoriales/niveles_osi.php.

http://www.utm.edu. (sf) Estándar EIA TIA 568 A y 568 B. Recuperado el 17 de Octubre del 2012 de: http://www.utm.edu/staff/leeb/568/568.htm.

ANEXOS






5
4
3
PARA IMPRIMIR


4
3
2
1
PARA IMPRIMIR
HORARIO DE ATENCION
LUNES A VIERNES


5
PARA IMPRIMIR
4
PARA IMPRIMIR
3
PARA IMPRIMIR
HORARIO DE ATENCI
LUNES A VIERNE
SABADOS, DOMINGOS
FERIADOS
10:00 AM a 6PM


6
PARA IMPRIMIR
5
4
3


6
PARA IMPRIMIR
5
4
3


6
5
4
3
2
1
PARA IMPRIMIR


6
5
4
3
2
1
PARA IMPRIMIR


6
5
4
3
2
1
PARA IMPRIMIR