Diseño e Implementación de una Red de Datos y Control de Acceso Biométrico en el edificio de la Cámara de Comercio de la Ciudad de Otavalo

Autor – Marcela Elizabeth LÓPEZ HUERA

Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Avenida 17 de Julio 5-21 y José María Córdova, Ibarra, Imbabura

melopez@utn.edu.ec

Resumen. *Este proyecto abarca desde el análisis hasta la implementación de la red de datos de la Cámara de Comercio Otavalo, incluyendo un Sistema de Control de Acceso biométrico cuyo objetivo principal fue conseguir una mejora tecnológica en la infraestructura del edificio, lo cual permitió aumentar la capacidad de conexión de los usuarios, con velocidades elevadas, instalación de switches y soporte para los requerimientos actuales y futuros considerando servicios de seguridad.*

Se contempló el estudio de la infraestructura actual con el cual se determinó el enrutamiento del cableado tomando en cuenta la norma ANSI/TIA/EIA 568-B y la norma ANSI/TIA/EIA-569A. Una vez realizado el diseño se ejecutó la instalación y configuración de los equipos de redes y biométricos incluyendo la colocación del cableado, rack, face plates, enrutamiento del par trenzado, segmentación de la red, servidor proxy y manual de políticas de acceso.

Es así que, se logró implementar la Red de Datos y Control de Acceso biométrico en base a los requerimientos planteados, mejorando la infraestructura tecnológica del edificio de la Cámara de Comercio, y proporcionando niveles de seguridad que mejorarán la productividad y eficiencia de sus usuarios.

Palabras Claves

Red de datos, Firewall, TIA 568B, TIA 569A, Otavalo.

Abstract. *This project ranges from the analysis to the implementation of the data network of the Otavalo Chamber of Commerce, including a biometric Access Control System whose main objective was to achieve a technological improvement in the building's infrastructure, which allowed to increase the capacity of Connection of users, with high speeds, installation of switches and support for current and future requirements considering security services.*

It was considered the study of the current infrastructure with which wire routing was determined taking into account ANSI / TIA / EIA 568-B and ANSI / TIA / EIA-569A. Once the design was carried out, the installation and configuration of the network and biometric equipment were implemented, including wiring, rack, face plates, twisted pair routing, network segmentation, proxy server and access policy manual.

Thus, it was possible to implement the Biometric Access Control and Data Network based on the requirements, improving the technological infrastructure of the building of the Chamber of Commerce, and providing levels of security that will improve the productivity and efficiency of its users.

Keywords

Data Network, firewall, TIA 568B, TIA 569A, Otavalo

1. Introducción

La Cámara de Comercio de la Ciudad de Otavalo alberga a empresarios o dueños de negocios pequeños, medianos o grandes que tienen por objetivo incrementar la productividad de sus empresas cuidando sus intereses y teniendo como base la mutua cooperación.

La arquitectura del edificio no fue diseñada para alojar redes de datos ni mucho menos sistemas automatizados; únicamente cuenta con instalaciones eléctricas, ya que su infraestructura existe desde hace más de 40 años.

De igual forma no existen Políticas de Seguridad de Acceso Físico, ni ningún sistema capaz de controlar el ingreso del personal a ciertas estancias o detectar intrusos, siendo este edificio vulnerable a cualquier tipo de inseguridad.

En base a estos antecedentes se plantea como solución la implementación de una Red de Datos lo suficientemente flexible para el lugar, que pueda integrar todas las dependencias de la Cámara de Comercio levantando Políticas de Seguridad de Acceso que permitan brindar conexión a todos los usuarios que la requieran, con un Sistema de Cableado Estructurado apto para transmitir a velocidades GigabitEthernet soportando aplicaciones tales como telefonía, PoE, video on demand o video en alta definición; así como también la instauración de un Sistema de Acceso Biométrico que proporcione seguridad a las personas y bienes que se alojan en el edificio.

2. Normas ANSI/EIA/TIA 568B y 569A

La norma ANSI/TIA/EIA-568-B especifica el Cableado de Telecomunicaciones en Edificios Comerciales. Se divide en ANSI/TIA/EIA-568-B.1, ANSI/TIA/EIA-568-B.2 y ANSI/TIA/EIA-568-B.3

ANSI/TIA/EIA-568-B.1: Requerimientos Generales

De acuerdo a este estándar, el SCE se divide en seis subsistemas: facilidades de entrada, cuarto de equipos, cableado vertical o backbone, cuarto de telecomunicaciones, cableado horizontal y las áreas de trabajo.

Facilidades de entrada (Acometida): se refiere al hardware que se requiere para la interconexión de los proveedores externos de servicio con el SCE del cliente, siendo el punto de demarcación aquel que delimita las responsabilidades entre proveedor y cliente. Este punto puede localizarse en cuartos de otros servicios como por ejemplo agua potable o energía eléctrica.

Cuarto de equipos: constituye el centro de la red, aquí se localizan todos los equipos de telecomunicaciones como: routers, switches, servidores, centrales PBX. Puede incluir áreas de trabajo para los encargados.

Cuarto de telecomunicaciones: concentra las terminaciones del cableado horizontal con los cables de backbone con el objetivo de brindar el servicio a las áreas de trabajo. Se recomienda un cuarto de telecomunicaciones por piso mientras no se sobrepase los 90 metros.

Si se trata de una infraestructura pequeña es posible utilizar montantes de pared o gabinetes encerados.

Cableado vertical o backbone: interconecta los cuartos de telecomunicaciones, los cuartos de equipos y las acometidas de un SCE incluyendo también el tendido de cable entre edificio.

- Los cables reconocidos por la norma son:
- Cable par trenzado 100 ohmios
- Fibra multimodo 50/125micras o 62.5/125micras.
- Fibra monomodo.

En la norma se definen dos niveles de conexión que se evidencian en la figura 1:

- Conexión directa entre cuarto de equipos y cuartos de telecomunicaciones.
- Conexión mediante un cuarto intermedio.

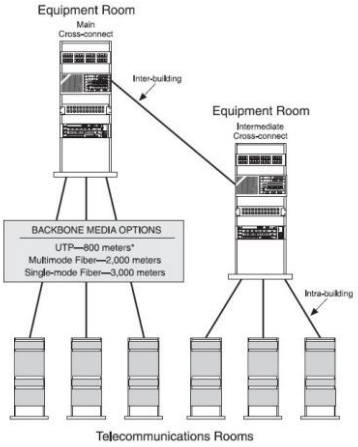

Figura 1. Niveles de conexión entre el cuarto de equipos y el cuarto de telecomunicaciones.

Cableado horizontal: conecta las áreas de trabajo con los cuartos de telecomunicaciones incluyendo patch cords, salidas de telecomunicaciones y las terminaciones en los patch panel con una topología en estrella. Su distancia máxima hasta las salidas de telecomunicaciones es de 90 metros como se observa en la figura 2.

Los cables reconocidos por la norma son:

- Cable de cobre 4 pares UTP 100 ohmios o STP.
- Fibra óptica multimodo de 62,5/125 o 50/125 micras.

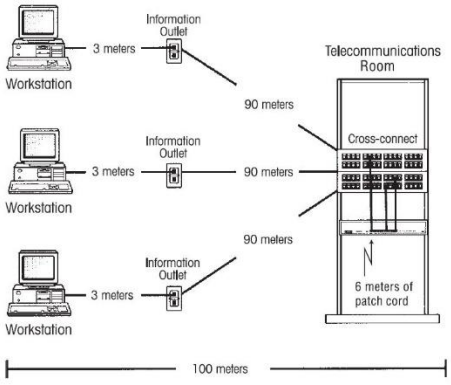

Figura 2. Distancia máxima del cableado horizontal

Área de Trabajo: es aquella que se extiende desde la salida de telecomunicaciones hasta el equipo de trabajo. El cableado en las áreas de trabajo generalmente no es permanente por lo que debe resultar fácil de cambiar. El patch cord empleado en el área de trabajo tiene una longitud máxima de 3m. [1]

Cada área de trabajo deberá tener al menos dos salidas de telecomunicaciones, como lo muestra la figura 20, una para voz y otra para datos. Una salida será cable UTP de 100

ohmios categoría 3 o superior, mientras que la otra será par trenzado o fibras multimodo. [2]

La norma ANSI/TIA/EIA-569-A es el estándar de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales Especifica los siguientes parámetros:

Facilidades de Entrada: deben ubicarse en lugares libres de humedad, cercanos a las canalizaciones de backbone.

Cuarto de Equipos: e debe evitar la humedad y tener fácil accesso para equipos grandes. El tamaño mínimo recomendado es 13.5 metros cuadrados, es decir un espacio de 3.7x3.7 metros. [3]

Canalizaciones de bakcbone: pueden ser internas o externas al edificio. En caso de tratarse de canalizaciones externas se distinguen cuatro tipos:

- Canalizaciones subterráneas: consiste en ductos de 100mm de diámetro mínimo.

- Canalizaciones directamente enterradas: los cables deben tener la protección respectiva ya que quedan totalmente bajo tierra.

- Canalizaciones aéreas: los cables deben contar con protecciones mecánicas para soportar los cambios climáticos.

- Canalizaciones tipo túnel: se crea un túnel exclusivamente para el cableado aislándolo de otros servicios para evitar interferencias.

Ahora bien, si las canalizaciones son internas pueden ser ductos, bandejas, portacables, entre otros. Este cableado puede ser vertical u horizontal.

- Canalizaciones verticales: ductos, bandejas verticales o escalerillas. No se permite la utilización de ductos en ascensores.

- Canalizaciones horizontales: en caso de que los cuartos o armarios de telecomunicaciones no se encuentren alineados se debe usar tramos de cableado horizontal que se pueden localizar debajo del piso, en las paredes o cielorraso.

Cuarto o armario de telecomunicaciones: se recomienda que haya almenos un armario por piso a menos que el área a servir exceda los 1000 metros cuadrados. [4]

• Canalizaciones horizontales

- Su diseño debe soportar los cables especificados en la norma TIA-568B además de estar lo suficientemente distanciados del cableado de energía. Los tipos de canalizaciones pueden ser:

- Ductos bajo el piso: forman parte de la obra civil.

- Ductos bajo el piso elevado: bajo el piso falso es posible instalar el sistema de cableado de telecomunicaciones.

-- Bandejas: estructuras sólidas que generalmente se instalan sobre el cielorraso y pueden o no tener tapa.

- Ductos sobre cielorraso: deben estar fijos al techo.

- Ductos perimetrales: se usan para alcanzar las áreas de trabajo, deben colocarse de forma estética. [5]

Áreas de trabajo: se asume áreas de trabajo de 10 metros cuadrados, es decir 3x3.

3. Diseño de la Red de Datos y Sistema de Control de Acceso

3.1 Requerimientos de usuario

Una red de datos es un activo muy importante dentro de cualquier organización, ya que, para el caso, algunas operaciones que se efectúan en este establecimiento dependen de esta. Sin embargo, al carecer de una red de datos se presentan varios inconvenientes como lo han manifestado sus afiliados y demás personas. Lo que se pretende lograr con el presente proyecto es el acceso a la red por parte de todos sus usuarios, mejorando así su desempeño, por lo que en la tabla 1 se enlistan los requerimientos.

Observación	Requerimiento	Consideraciones
Servicio de compartición de datos ineficiente.	RED DE DATOS ESCALABLE	Puntos de red para los puestos de trabajo actuales y su proyección a futuro. Puntos de red dobles para voz y datos respectivamente.
Conexión mientras hay movilidad	CONEXIÓN MÓVIL	Puntos de red para access points.
Optimizar el acceso a la red.	CONTROL DE CONTENIDOS WEB	Firewall Proxy
Carencia de un método de seguridad de acceso.	SEGURIDAD FÍSICA	Controles de Acceso Biométricos

Tabla 1. Requerimientos de usuario

Análisis de la cantidad de usuarios

Actualmente se necesitarían 31 puntos de red para cada puesto de trabajo, no obstante, considerando el incremento de personal y socios, de los últimos años como se evidencia en la tabla 11, se deduce que, hubo un crecimiento del 1,37% aplicando la fórmula de la ecuación (1), en base a los archivos proporcionados por la Cámara de Comercio que dado que son confidenciales no se los puede publicar.

$$tasa\ de\ crecimiento = \frac{presente-pasado}{pasado} x\ 100\% \quad (1)$$

$$tasa\ de\ crecimiento\_5años = \frac{31-29}{29} x\ 100\%$$

$$tasa\ de\ crecimiento\_5años = 6{,}89\%$$

Elección del medio de transmisión

En primer lugar se descartan categorías inferiores, como UTP CAT-5 puesto que la velocidad de operación 10/100 de estos desaprovecharía las capacidades que tienen los equipos actuales de redes que generalmente son gigabit.

Inicialmente la red no contará con ningún servidor o DMZ, sin embargo, no se descarta la posibilidad de que en un futuro se levanten servicios como: http, voz ip, ftp u otros. Es así que en la tabla 3 y tabla 4 se realiza una estimación de la capacidad que requieren las aplicaciones de mayor uso actualmente y en el futuro; con el fin de conocer el ancho de banda máximo que se podría alcanzar próximamente en caso de implementarse estos servicios. [6]

Requerimientos de ancho de banda actual	**Capacidad requerida (Mbps)**
Navegación	0,20
Actualizaciones en línea de sistemas operativos	0,20
Actualizaciones en línea de sistemas de seguridad	0,20
Acceso a servidores externos de correo	1,00
Transferencia de archivos entre usuarios	25,00
Descargas de videos	5,00
Otros	2,00
TOTAL	33,60

Tabla 2. Requerimientos de ancho de banda pico actual.

Requerimientos de ancho de banda futuro	**Capacidad requerida (Mbps)**
Navegación	0,20
Actualizaciones en línea de sistemas operativos	0,20
Acceso a servidores externos de correo	1,00
Transferencia de archivos entre usuarios	25,00
Descargas de videos	5,00
Servidor de correo electrónico	1,00
Servidor de voz ip	0,06
Servidor HTTP	0,05
Aplicaciones futuras de administración	20,00
Otros	15,00
TOTAL	67,71

Tabla 3. Requerimientos de ancho de banda pico futuro.

Del análisis se obtiene que con una proyección a futuro se requerirá un ancho de banda de 67,71 Mbps, pero con el fin de evitar encolamientos o colisiones se necesitarán equipos y el medio de transmisión del doble de la capacidad calculada, es decir 135,42Mbps. De esta manera, el cable a escoger deberá soportar este valor así como también la velocidad del puerto de los equipos.

De acuerdo a las cifras numéricas de ancho de banda que presentan los pares trenzados 5, 5e, 6 y 6A, que serían los posibles a utilizarse; se recomienda utilizar cable utp categoría 6A, por lo menos en el enlace de backbone, puesto que, los enlaces de cada host convergen en uno solo hacia el firewall y hacia el router; si son en total 75 puntos de red, de los cuales se descartan los puntos de voz (estos solo tendrían acceso a puertos de voz SIP e IAX) y su tráfico ya está tomado en cuenta en las tablas 12 y 13 quedan en total 40 usuarios, siendo que cada uno genera 135,42 Mbps se obtiene entonces 5416,8 Mbps o 5Gbps de tráfico en dichos enlaces, en donde el cableado UTP CAT 5e no abastecería el enlace puesto que en condiciones óptimas llegaría a 1Gbps. Por tal motivo se recomienda utilizar el cable CAT-6A que puede alcanzar hasta 10Gbps.

Sin embargo, para los requerimientos actuales, el cable UTP categoría 5e resulta suficiente ya que certifica 100Mbps, pudiendo alcanzar una tasa de transferencia superior, con los conectores adecuados llegando hasta el GigabithEthernet como máximo.

Si la red diseñada no debiera expandirse la implementación con una categoría superior sería subutilizar el cable dado que, el tráfico en megabits por segundo (Mbps) calculado, resultaría ínfimo en comparación al gigabit que ofrece un cable categoría 6, desperdiciando casi 900 Mbps.

Topología de la red

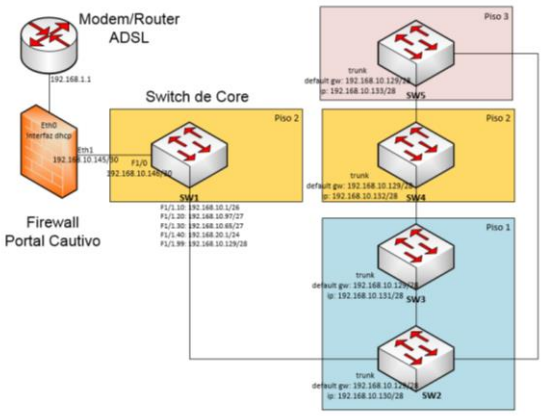

Figura 3. Topología de red propuesta.

Direccionamiento IP

Si se toma en cuenta que un sistema de cableado estructurado debe ser escalable al menos hasta 10 años se calcula que al término de este deberá tener capacidad para alojar a 36 usuarios según la tasa de crecimiento del 1,37% calculada anteriormente, además de que cada uno tendrá su

salida de telecomunicaciones para voz y datos, siendo en total 80 puntos de red solamente para áreas de trabajo.

Es por esto que, se ha tomado la dirección 192.168.10.0 con una máscara de 255.255.255.0 perteneciente a una dirección IP privada de clase C, a la cual se procederá a dividir en subredes mediante el proceso de VLSM para dar cobertura a las vlans de voz y datos, según el número de hosts requeridos que se evidencian en la tabla 12, dado que un /24 permitirá asignar subredes en rangos válidos para los enlaces troncales y dejar espacio disponible para la creación de subredes en caso de ampliar la red con servidores; mientras que, la vlan para usuarios inalámbricos se creará con la dirección de red 192.168.20.0/24 de tal modo que resulte más fácil identificar cuando los usuarios se encuentren con conexión al a wlan, además de que se tendrá una dirección full class con capacidad para 254 hosts.

Cableado estructurado

Para el cableado estructurado de la planta baja se consideró la utilización de un rack de pared por la poca cantidad de puntos de red, a partir del cual se distribuirán los cables para las estaciones de trabajo, siguiendo una topología tipo estrella como se muestra en la imagen de la figura 4.

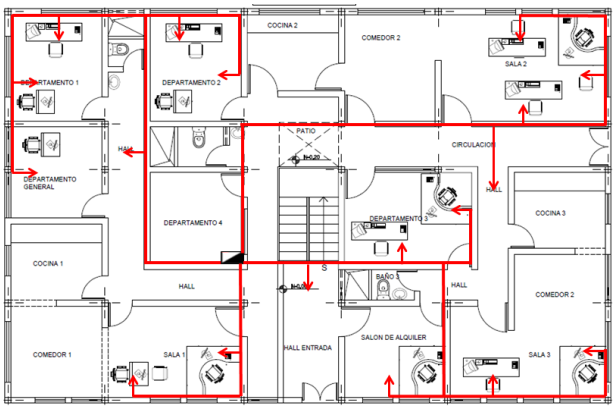

Figura 4. Esquema de distribución de puntos de red Planta Baja

En el cableado horizontal del primer piso se siguió la misma topología tipo estrella, considerando que el rack principal se ubicará dentro de la oficina presidencial, al cual se conectará el cableado de backbone como se indica en la figura 5.

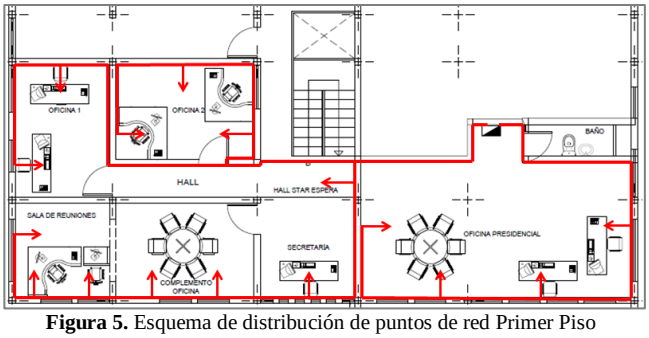

Figura 5. Esquema de distribución de puntos de red Primer Piso

Para el cableado horizontal del segundo piso se considerará la instalación de 9 puntos de red, dado que solamente existe un salón y el pasillo que se pueden observar en la figura 6, por lo que con un rack de pared ubicado en el salón máximo será suficiente.

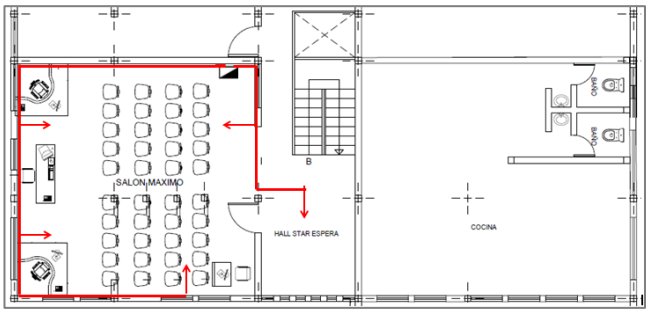

Figura 6. Esquema de distribución de puntos de red Segundo Piso

Canaletas

Se utilizarán canaletas plásticas de tres áreas diferentes, de 20x12mm2 para enrutar hacia las áreas de trabajo, de 32x12mm2 y 40x25mm2 de área.

Entonces se procede a calcular el número de cables que caben en éstas, despejando la ecuación de capacidad utilizada anteriormente, que da lugar a la ecuación 4:

$$\#de\ Pares\ Trenzados = \frac{área\ de\ canaleta}{área\ del\ cable\ x\ 40\%} \quad (4)$$

$$\#de\ Pares\ Trenzados\ CAT-5e = \frac{área\ de\ canaleta}{18.86mm^2\ x\ 2.5}$$

$$\#de\ Pares\ Trenzados\ CAT-6A = \frac{área\ de\ canaleta}{29.22mm^2\ x\ 2.5}$$

CANALETA (mm)	ÁREA(mm^2)	NÚMERO DE PARES TRENZADOS CAT-5e (#)	NÚMERO DE PARES TRENZADOS CAT-6A (#)
20x12	240	5	3
32x12	384	8	5
40x25	1000	21	14

Tabla 4. Número de pares trenzados por canaleta.

Seguridad física

Se instalarán controles de acceso biométricos mediante huella digital, con el objetivo de controlar el ingreso del personal a las instalaciones del edificio. El sistema se encargará de almacenar los datos registrados de las personas con parámetros de fecha y hora principalmente.

Las características mínimas de estos dispositivos son:

• Funcionamiento en modo red o independiente: inicialmente se colocará un biométrico en la entrada por lo que este funcionará en modo independiente, pero con el pasar del tiempo se prevé localizar más de estos dispositivos por lo que el dispositivos por lo que este deberá soportar conexión en red.

• Transferencia de registros en tiempo real: los reportes deberán generarse al día por lo que la transferencia debe ser en tiempo real

• Batería integrada en caso de cortes de energía.

• Capacidad de usuarios: 100 mínimo entre huellas dactilares y contraseñas numéricas ya que esta es la cantidad máxima de personas que han llegado al lugar en un determinado día.

• Entrada USB, TCP/IP: para guardar los reportes generados.

Seguridad lógica

La seguridad lógica estará a cargo del servidor proxy firewall. Para determinar los requerimientos del sistema se utilizó la norma ISO/IEC/IEEE 29148:2011 que especifica los Requerimientos de Software, a través de una serie de parámetros que se deben tomar en cuenta al momento de seleccionar determinado sistema; corresponde a una actualización de la norma IEEE Std 830, para lo cual supone llenar un esquema con la información requerida.

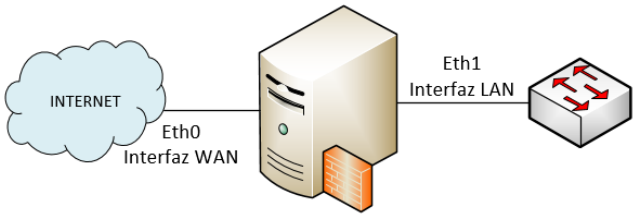

Figura 7. Interfaces del servidor firewall.

El acceso a internet es considerado un derecho humano, así lo establece la Organización de las Naciones Unidas en el artículo 19 de la Declaración Universal de los Derechos por lo que es importante proteger el acceso a Internet ya que "facilita enormes oportunidades para la educación asequible e inclusiva a nivel mundial" [7]. Es así que resulta inadmisible la suspensión total de este servicio sea para cual fuere su fin. Entonces se plantean las políticas acorde a la tabla siguiente:

POLÍTICA	DIRIGIDA A	DENEGAR/PERMITIR
Acceso a facebook, twitter y youtube	Directivos	PERMITIR sin restricciones
	Socios	PERMITIR con control de ancho de banda
Descargas	Directivos	Permitidas
	Socios	Permitidas en determinado horario
Acceso al servidor FIREWALL	Encargado de la red	PERMITIR
	Resto de usuarios	DENEGAR
Acceso a páginas pornográficas, drogas o alcohol	Todos los usuarios	DENEGAR

Tabla 5. Políticas del servidor firewall.

Manual de políticas de seguridad

La creación de políticas de seguridad en una empresa es vital para el resguardo de la información, de tal manera que, basado en las buenas prácticas proporcionadas por la norma ISO-27002 para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, [8] y acorde a lo que la Cámara de Comercio requiere se plantea un manual con los dominios correspondientes a la Cámara de Comercio. La norma ISO-27002 cuenta con catorce dominios, que abarcan desde la seguridad del personal hasta la seguridad ambiental, sin embargo estos parámetros se han descartado puesto que el manual engloba únicamente políticas de acceso. [8]

4. Implementación

Para el ponchado del cable se consideró la norma T568B y T568A para cada extremo respectivamente, logrando cables cruzados cuya configuración se muestra en la tabla 40. Se debe considerar que para las canalizaciones del cableado horizontal, uno de los extremos es RJ-45 macho que se conectará hacia el pacth panel mientras que el otro extremo es el Jack RJ-45 o conector hembra que se ubicará en el faceplate que conecta a las áreas de trabajo.

El cable que se utilizó es categoría 5e aunque se dejó la recomendación de realizarse con categoría 6A; pero dado que el costo fue uno de los requerimientos se ajustó el proyecto al par trenzado UTP Cat-5e.

Figura 8. Ponchado del par trenzado

Se instalaron faceplates dobles y simples de la marca DEXSON sobre la pared, que comprenden un cajetín blanco de 10x6 centímetros de color blanco, en los cuales se colocaron los jacks RJ-45 propuestos inicialmente con colores azul y rojo pero finalmente todos son blancos que contarán con su etiquetado.

Lo primero que se realizó fue perforar el cajetín dejando el espacio pertinente para que pase el cable UTP y luego atornillarlo hacia la pared como se ilustra en la figura

Figura 9. Instalación de faceplates

Los puntos de voz de esta red, no se encuentran inicialmente destinados a telefonía IP, por lo que, a ellos se conectarán teléfonos analógicos pudiendo cambiarse esto a futuro, sin embargo se presentó un inconveniente dado que los conectores de estos son RJ-11, que si bien, se adaptan al jack RJ-45, no es recomendable forzarlo debido a que es posible que se obstruyan los pines 1 y 8 de este último, por lo que se optó por modificar el conector de los enlaces telefónicos de RJ-11 a RJ-45 (véase figura 10); no obstante en el mercado existen conversores pero por facilidad de costos esta opción no resulta viable.

Figura 10. Reemplezo del conector RJ-11 por un RJ-45

El rack principal se localiza en la oficina presidencial y es el rack es el más importante de la red puesto que aquí se encuentra el switch central en donde se concentran las conexiones de los switches de acceso. (véase figura 11).

En el diseño realizado se propuso conectar los puntos de voz hacia una vlan voz en el switch, sin embargo con el fin de aprovechar las centrales telefónicas que ya tenía la Cámara de Comercio, no se realizó este procedimiento, puesto que estos dispositivos son analógicos, por lo tanto, los enlaces provenientes de los puntos de voz implementados se conectaron directamente desde el patch panel a esta central que fue alojada en el rack.

Figura 11. Rack principal

Por último, es importante realizar pruebas de funcionamiento en un ambiente real, para determinar su buen desempeño puesto que asegura su correcta instalación, ya que no basta que la información se transmita de un extremo a otro, sino que lo haga óptimamente.

Es así que, se verificó el acceso a internet desde cada uno de los equipos, a través de diferentes navegadores así como también utilizando el comando ping que constituye el método más fácil para probar la conectividad TCP/IP

5. Conclusiones

•Se implementó la Red de Datos y Control de Acceso biométrico en base a los requerimientos obtenidos y basados en las normas ANSI/TIA/EIA 568-B y 569-A mejorando así la infraestructura tecnológica del edificio de la Cámara de Comercio.

•Se realizó el estudio de la situación actual para determinar los requerimientos de usuario y así plantear el diseño óptimo.

•Las características de infraestructura del edificio y las exigencias de los usuarios fueron los parámetros que definieron la implementación final del proyecto, no obstante, para el diseño del presente trabajo de grado se cumplió con los puntos descritos en las normas de cableado estructurado ANSI/TIA/EIA 568-B y 569-A; sin embargo sí existieron variaciones mínimas al momento de la implementación debido a características físicas propias de la infraestructura.

•En el edificio de la Cámara de Comercio se necesitaban 33 puntos de red para las áreas de trabajo que se están ocupando, sin embargo tomando en cuenta la expansión futura y como resultado del estudio de la situación actual se pudo determinar que el número de puntos de red requeridos son 75, distribuidos en todo el edificio, incluyendo puntos de red requeridos para los puestos de trabajo, puntos de red adicionales en base a la dependencia en metros cuadrados y al porcentaje de crecimiento de usuarios en un período de 10 años; y puntos de red en los pasillos para una posible implantación de puntos de acceso inalámbricos.

•La segmentación de la red en pequeñas redes lan virtuales (vlans) que se realizó en la red de la Cámara de Comercio implicó un procedimiento efectivo para prevenir la congestión de tráfico, haciendo un uso eficiente del ancho de banda además de que proporciona seguridad en la red, por lo que, en el diseño realizado se planteó este mecanismo como solución para reducir el dominio de broadcast hasta en un 60% dependiendo del envío de paquetes.

Referencias Bibliográficas

[1] U. Black, Redes de computadores: protocolos, normas e interfaces, 1997.

[2] W. Stallings, Data and computer communications, vol. 10, Madrid: PearsoN Education, 2014.

[3] EIA, «Electronic Industry Association,» 2016. [En línea].

[4] A. Reid y J. Lorenz, Networking para el hogar y pequeñas empresas, Madrid: CISCO Systems, 2016.

[5] Anixter, «Wire & Cable,» 2015. [En línea]. Available: https://www.anixter.com/en_us/services-and-solutions/solutions/building-technologies/enterprise.html.

[6] F. Lamus, «Global News Room Cisco,» 2014. [En línea]. Available: http://globalnewsroom.cisco.com/es/la/press-releases/cisco-ocupa-el-primer-lugar-en-el-mercado-de-segur-1156779.

[7] ONU, Declaración Universal de los Derechos Humanos, 2016.

[8] ISO27000, «Estándar ISO27000 en español,» 2016. [En línea]. Available: www.iso27000.es.

[9] ANSI, «ANSI: Standards activities,» 2016. [En línea]. Available: https://www.ansi.org/standards_activities/overview/overview?menuid=3.

Sobre el Autor...

Marcela López nació en Quito, Provincia de Pichincha el 28 de febrero de 1994. Realizó sus estudios primarios en la Escuela Ana Luisa Leoro de la ciudad de Ibarra y los estudios secundarios en el Colegio Nacional “Ibarra”, donde finalizó en el año 2011, obteniendo el título de Bachiller en Ciencias Especialización Físico Matemático. Actualmente, está realizando su proceso de titulación en Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte – Ecuador.