Dom. Cien., ISSN: 2477-8818
Vol. 4, núm. 2, abril, 2018, pp. 123-137

DOI: 10.23857/dc.v4i2.781

Número Publicado el 05 de abril de 2018

Ciencias de la computación

Artículo de investigación

Diseño e implementación de una red de datos segura para la Pontificia Universidad Católica del Ecuador, Santo Domingo

Design and implementation of a secure data network for the Pontificia Universidad Católica del Ecuador, Santo Domingo

Concepção e implementação de uma rede de dados segura para a Pontifícia Universidade Católica do Equador, Santo Domingo

Carlos V. Galarza-Macancela [I]

gmcv@pucesd.edu.ec

Recibido: 15 de octubre de 2017 * **Corregido:** 21 de noviembre de 2017 * **Aceptado:** 16 de enero de 2018

[I] Magister en Seguridad Informática Aplicada, Diploma Superior en Sistemas de Información Empresarial, Ingeniero en Sistemas e Informática, Pontificia Universidad Católica del Ecuador, Santo Domingo, Ecuador.

Resumen

El estudio presenta el diseño e implementación de una red de datos segura para la Pontificia Universidad Católica del Ecuador para la sede Santo Domingo. Se realizó el respectivo levantamiento de información, se analizó e identificó las vulnerabilidades de los equipos de conmutación de capa 2, para posteriormente proceder con la implementación de los correctivos con sus correspondientes pruebas de funcionamiento. Con la implementación de las configuraciones correctivas de seguridad en la infraestructura de red de datos de capa 2, se consiguió mejorar los niveles de seguridad como una medida preventiva de acceso no autorizado a los diferentes recursos. La implementación de los correctivos en la infraestructura de red de datos segura, permitió reducir la explotación de vulnerabilidades de capa 2, y de esta manera se contribuyó con la integridad, disponibilidad y confidencialidad de la información.

Palabras clave: LAN; seguridad; confidencialidad; integridad; disponibilidad.

Abstract

The study presents the design and implementation of a secure data network for the Pontifical Catholic University of Ecuador for the Santo Domingo site. The respective information survey was carried out, the vulnerabilities of the layer 2 switching equipment were analyzed and identified, and then the corrective measures were implemented with their corresponding operational tests. With the implementation of the corrective security configurations in the layer 2 data network infrastructure, it was possible to improve security levels as a preventive measure of unauthorized access to the different resources. The implementation of the corrections in the secure data network infrastructure allowed the exploitation of layer 2 vulnerabilities to be reduced, thus contributing to the integrity, availability and confidentiality of the information.

Keywords: LAN; security; confidentiality; integrity; availability.

Resumo

O estudo apresenta a concepção e implementação de uma rede de dados segura para a Pontifícia Universidade Católica do Equador para o site Santo Domingo. O respectivo levantamento de

informações foi realizado, as vulnerabilidades dos equipamentos de chaveamento da camada 2 foram analisadas e identificadas, e as medidas corretivas foram implementadas com os respectivos testes operacionais. Com a implementação das configurações de segurança corretivas na infraestrutura de rede de dados da camada 2, foi possível melhorar os níveis de segurança como uma medida preventiva do acesso não autorizado aos diferentes recursos. A implementação das correções na infra-estrutura de rede de dados segura permitiu que a exploração das vulnerabilidades da camada 2 fosse reduzida, contribuindo assim para a integridade, disponibilidade e confidencialidade das informações.
Palavras chave: LAN; segurança confidencialidade; integridade; disponibilidade.

Introducción

La Pontificia Universidad Católica del Ecuador Sede Santo Domingo (PUCE SD), considera en su misión el desarrollo del conocimiento con aperturidad, veracidad, rigurosidad y sentido crítico, en sus diferentes expresiones y disciplinas. Para dar cumplimiento a su misión, la Institución de Educación Superior (IES) emprendió un proceso de cambios tecnológicos, entre estos la implementación de un Data Center moderno, creando conexiones mediante fibra óptica entre los diferentes edificios y el Data Center.

En los últimos años, se ha venido cambiando progresivamente de forma escalable los equipos activos de capa 2 de la red de datos, por unos dispositivos más robustos de marca CISCO que puedan brindar la oportunidad de diseñar una red de datos segura. Actualmente toda la infraestructura de red de capa 2 dispone de equipos administrables CISCO, con un total de 25 switches CISCO y 1 Router CISCO distribuidos por todo el campus.

Se han creado algunas políticas de seguridad en cuanto al acceso del personal en áreas sensibles, como también se ha definido las funciones y criterios de seguridad en el Departamento de Tecnología de la Información (DTI) para la administración de los equipos tecnológicos, sin embargo, hasta el momento no se ha considerado incorporar elementos de configuración de seguridad en cuanto a los equipos activos CISCO de capa 2.

Con la introducción de las computadoras y el uso de aplicaciones para automatizar la información, se volvió evidente la necesidad de implementar sistemas de seguridad sobre la información. Según Katz (2013), los factores más importantes que se deben cubrir dentro de la administración de la red son en orden de prioridad, la funcionalidad, seguridad y rapidez. La seguridad en redes está directamente relacionada con la continuidad de los negocios de una organización, por tanto, una brecha en la seguridad puede causar la pérdida de datos, o afectar la privacidad de las personas y comprometer la integridad de la información. (Watkins & Wallace, 2008)

Para transportar la información desde un computador a otro por medio de la red de datos se requiere crear medidas de seguridad para proteger los datos con el objetivo de garantizar niveles mínimos de integridad, disponibilidad y confidencialidad de la información, referidos a menudo como la triada CIA. (Stallings, NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS, 2011). Lo expuesto, lleva a plantearse como objetivo disminuir las vulnerabilidades existentes en la infraestructura de red de datos de la PUCE SD en sus dispositivos de capa 2 CISCO, la misma que ponen en riesgo la seguridad de la información de la comunidad universitaria.

Materiales y métodos

Entendiendo que un modelo de defensa en profundidad se define en cuatro niveles; Seguridad informática, seguridad de la red, seguridad del servicio, seguridad de las aplicaciones. (Tiller, 2004). El estudio se corresponde al nivel de la seguridad de la red, específicamente en equipos de red de capa 2, por tanto, para la implementación de la red de datos segura, se ejecutaron las siguientes etapas o procesos:

- Diagnóstico
- Análisis
- Diseño
- Implementación y;
- Pruebas

En la etapa de diagnóstico se realizó el levantamiento de la información, como es el registro de los diferentes servicios tecnológicos que brindan a la comunidad universitaria, la topología física y lógica de la red de datos, el inventario de los equipos activos intermedios y la documentación de las configuraciones de los equipos CISCO capa 2.

En la fase de análisis con los insumos obtenidos en el diagnóstico, se identificaron las vulnerabilidades existentes en las configuraciones de los equipos activos de capa 2 con sus respectivos correctivos.

En la fase de diseño se realizó la topología lógica de la red de datos, considerando los resultados obtenidos en la fase de análisis, con la finalidad de minimizar las vulnerabilidades identificadas en el diseño de la red.

En la fase de Implementación se incorporaron los correctivos identificados en la red. Para la implementación de las nuevas configuraciones de capa 2 se las realizó de acuerdo a las políticas de seguridad de acceso a los equipos de red, definidos en el DTI.

En la fase de pruebas, se procedió con la validación del correcto comportamiento de la red con las nuevas configuraciones de la red de datos, para lo cual se diseñó un escenario adecuado para su validación.

De acuerdo a políticas de seguridad, las pruebas no se realizaron directamente en la red de producción, sin embargo, se trabajó en equipos reales para las validaciones en una topología creada de manera temporal. Para este proceso se trabajó con el personal designado del área de Redes.

Resultados y discusión

De acuerdo a lo detallado en el apartado anterior, se procede a la presentación de los resultados en cada etapa.

Diagnóstico de la problemática de la red de datos

El levantamiento de la información, permitió determinar los diferentes servicios que se brindan a través de la red de datos de la PUCE SD que se detallan en la tabla 1:

Tabla 1: Servicios de la red de datos

N°	APLICACIÓN	BASE DE DATOS / APLICACIÓN	SISTEMA OPERATIVO	MODELO SERVIDOR
1	Sistemas Informaticos de Producción	Oracle 10G	Windows Server	IBM System X3650
2	Sistemas Informaticos de Producción Pruebas II	Oracle 10G	Linux	IBM System X3250 M2
3	Página Web	Apache, PHP, Mysql, Joomla	Linux	IBM System X3250 M2
4	Sistema Biblioteca	SIABUC 9, PostgreeSQL	Windows Server	Lenovo Thinkcentre M57
5	Sistema Para Control de Personal Biometrico	SQL Server	Windows Server	IBM System X3200
6	Sistema Administrador de Personal RRHH	Apache, PHP, Mysql	Linux	Clon
7	Archivos Principal	SMB	Linux	IBM System X3200
8	Archivos Principal Backup	SMB	Linux	Clon
9	Proxy	Httpd, iptables, squid, squidguard	Linux	IBM System X3200
10	Servidor DHCP	Servicio DHCP	Windows Server	Clon
11	Antivirus	Antivirus - Consola Esent Endpoint Server	Windows Server	Lenovo Thinkcentre M92p
12	Inventario OCS	Apache, Mysql, PHP, OCS	Linux	Clon
13	Monitoreo Cactic	Mysql, CACTI, SNMP, PHP, Apache	Linux	Clon
14	Micro-PC	Ncomputing	Windows	Lenovo Thinkcentre M92p
15	Servidor Cámaras IP	Software Administrador Cámaras IP	Windows	Clon

El levantamiento de la infraestructura física, permitió construir la topología de la red de datos física, la misma que se detalla en la figura 1:

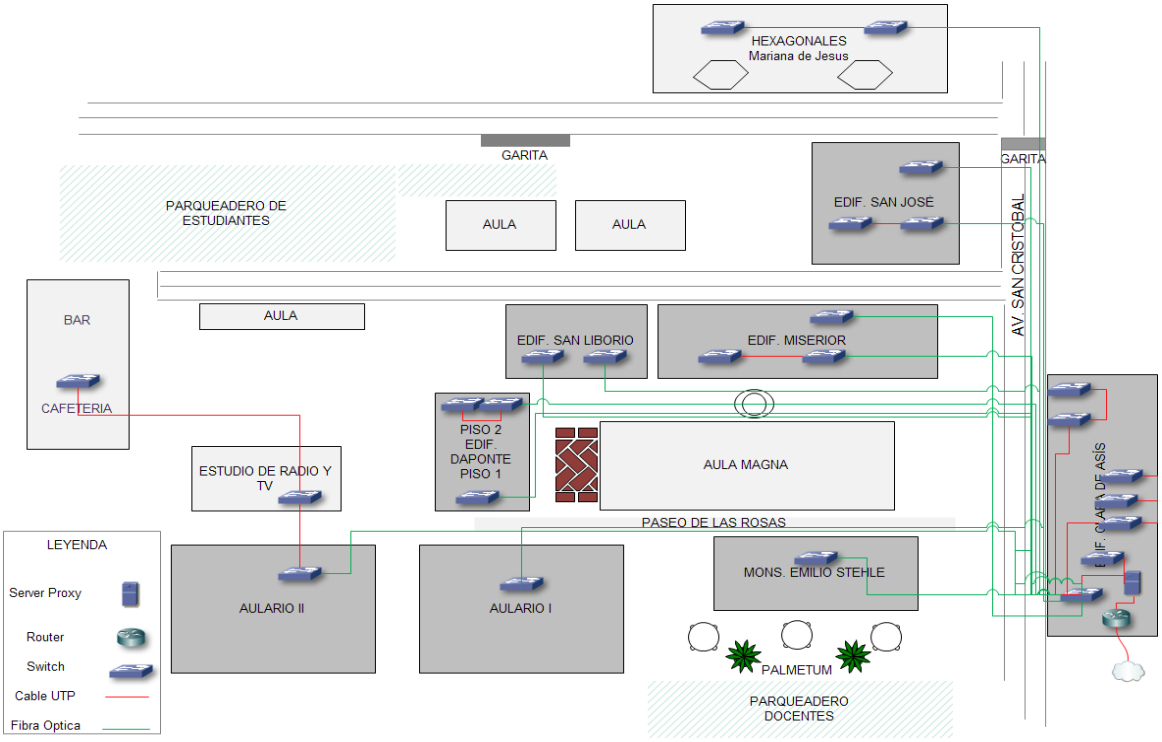

Figura 1: Topología física de la red de datos

Fuente: elaboración propia.

La topología presenta una estructura donde los enlaces desde el edificio Clara de Asís se conectan con todos los edificios de forma directa, por medio de un enlace de fibra óptica monomodo, a excepción de los enlaces entre el edificio de "Estudio de Radio y TV" y la "Cafetería", mismo que se conectan por medio de un enlace de cable UTP, desde el aulario II, conformado en su conjunto una topología de estrella extendida.

Como resultado de la investigación de campo, se logró diagramar la topología lógica de la red de datos, la misma se aprecia en la figura 2:

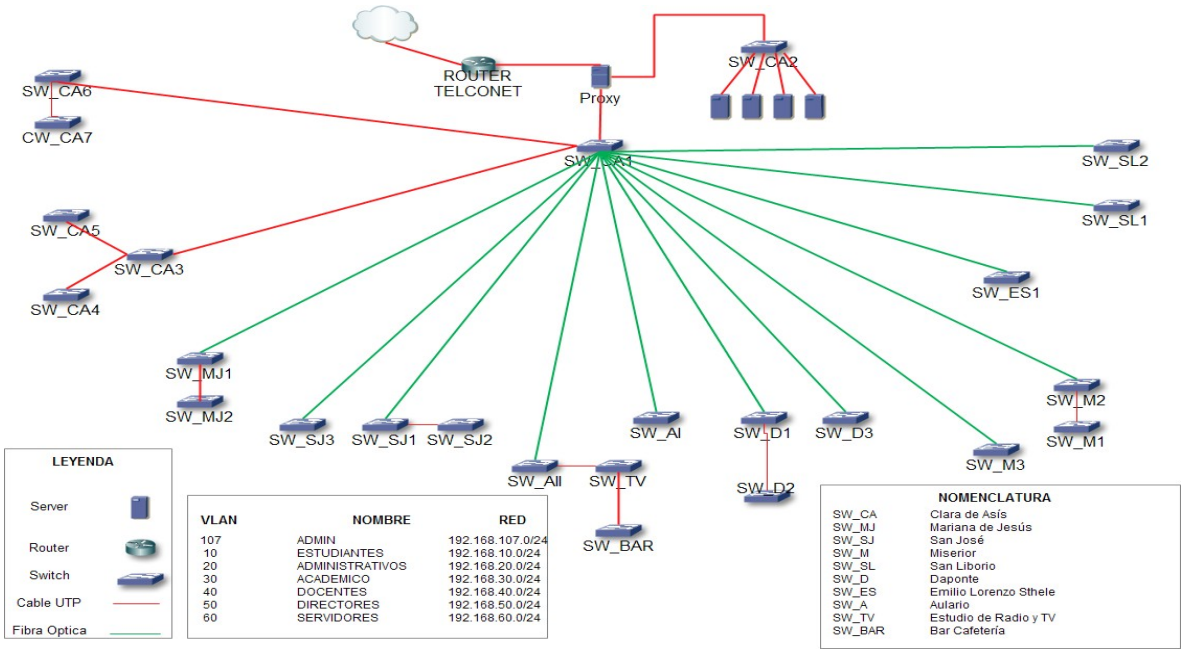

Figura 2: Topología lógica de la red de datos

Fuente: elaboración propia.

Se definió una nomenclatura para la documentación de los switches de la infraestructura de red, considerando las iniciales de los edificios como nombres de los switches, también se documentó las VLANs existentes.

Para el levantamiento del inventario de equipos activos, se consideró únicamente los switches CISCO de la infraestructura de red, sin considerar la red wireless, ya que ésta se encuentra fuera del alcance de la investigación. Se encuentra compuesta por 25 switches CISCO de la serie 2960.

Se documentó las configuraciones de los diferentes switches de la infraestructura de red de datos de la PUCE SD. Debido a un acuerdo de confidencialidad se procede a presentar de forma general las características de configuración encontradas en todos los switches:

- Todos los puertos se encuentran habilitados para permitir la conectividad de cualquier dispositivo de red.

- Las conexiones remotas están habilitadas con el protocolo Secure Shell (SSH).
- Cada colaborador del área de redes tiene asignado un usuario y una contraseña para la administración remota de los switches.
- Tiene creadas 7 VLANs utilizando el protocolo VTP para su aprendizaje en la red.
- Está configurada la encriptación de contraseñas en todos los switches.
- La topología de red tiene implementado el protocolo Spanning Tree (STP).
- Se encuentra creadas siete VLAN para la comunicación de los diferentes tipos de usuarios, incluida una VLAN para la conexión remota.
- Los puertos que se encuentran utilizados están asignados a su respectiva VLAN dependiendo del tipo de usuario, y los puertos que no se encuentran en uso, están en la VLAN por defecto.

Análisis, diseño e implementación de correctivos de vulnerabilidades

La capa 2 se puede considerar la más importante del modelo OSI ya que si es vulnerada, permitiría subir a capas superiores afectando la seguridad de la información. Posteriormente se realizó el analices de las configuraciones documentada de los equipos de capa 2 y se identificaron las vulnerabilidades de la red de datos.

- **Configuración vulnerable 1:**

Todos los puertos se encuentran habilitados para permitir la conectividad de cualquier dispositivo de red.

Análisis: Los puertos en estado activo de forma predeterminada pueden provocar que se conecten dispositivos de red no autorizados, induciendo dificultades para llevar un adecuado control sobre la administración de los dispositivos de la red de datos de la PUCESD.

La configuración predeterminada permite que se puedan presentar los siguientes problemas:

Se pueden realizar ataques de saturación MAC o ataques de desbordamiento de la tabla CAM, el cual consiste en una sobrecarga al switch con direcciones MAC falsas, hasta que se llene la tabla de direcciones MAC, lo que provoca que el switch entre en estado denominado "fail-open", que provoca que el switch adquiera un comportamiento similar al de un hub.

Al tener habilitado por defecto el protocolo de descubrimiento de cisco (CDP) permitiría compartir información de otros equipos cisco que se encuentren directamente conectados, permite obtener información útil, creándose de esta manera una brecha de seguridad. El CDP se encuentra habilitado por defecto, sin embargo, no se está considerando su utilidad en las actividades de monitoreo por parte del área de redes, por tal motivo se debería deshabilitar el protocolo.

La configuración por defecto permite que en un puerto se puedan conectar diferentes dispositivos finales, con autorización o sin la misma, esto como consecuencia por la falta de implementar un límite al número de direcciones MAC que pueden conectar a un puerto. Por otro lado, la configuración actual permite que se conecten dispositivos intermedios, dando espacio a brechas de seguridad en la infraestructura de red, al cambiar la topología de la red por personal no autorizado.

Configuración correctiva: se deshabilitaron todos los puertos que no se encuentran utilizados, para evitar el acceso no autorizado. Se deshabilito la búsqueda de DNS. Para evitar o prevenir el ataque de saturación MAC o ataques de desbordamiento de la tabla CAM, como el acceso a equipos no autorizados o dispositivos intermedios como switch o router, se habilitó la seguridad de puerto (port security) detallada en la vulnerabilidad 5.

Se deshabilitó el protocolo de descubrimiento de cisco (CDP)

- **Configuración vulnerable 2:**

Tiene creadas 7 VLANs utilizando el protocolo VTP para su aprendizaje en la red.

Análisis: el protocolo VTP facilita la creación de VLANs de forma automática y centralizada por medio de la configuración de un switch en modo servidor y los otros switches en modo cliente. Al validar previamente la contraseña de configuración del protocolo VTP entre los diferentes dispositivos

intermedios, se está garantizando que el acceso no autorizado no pueda afectar las configuraciones a través de mensajes con un número de revisión más alto.

Para la creación de contraseñas seguras tienen definidos criterios en el departamento; mínimo 8 caracteres, debe incluir letras mayúsculas, minúsculas, incluir números y caracteres especiales.

Configuración correctiva: Con la configuración de contraseñas seguras definidas en el departamento DTI, y con las configuraciones implementadas de acuerdo a la vulnerabilidad 1 y 5, se minimiza la posibilidad de algún ataque al protocolo VTP.

- **Configuración vulnerable 3:**

La topología de red tiene implementado el protocolo Spanning Tree (STP) para garantizar una red libre de bucles o lazos de capa 2.

Análisis: el protocolo Spanning Tree Protocol (STP) o 802.1d, está diseñado para prevenir bucles dentro de la red. Antes de llegar a una convergencia, STP debe pasar por una serie de estados antes de que el puerto sea capaz de transmitir información del usuario. Este proceso puede tardar entre 30 y 50 segundos.

Un ataque podría modificar la topología o estructura de árbol establecida a través del STP, a través de la selección de un nuevo dispositivo como puerto raíz, falsificando de esta manera al puerto raíz original o real. El atacante debe realizar un broadcast de BPDUs hasta conseguir una prioridad menor, forzando de esta manera el cambio en la topología y logrando tener acceso a tramas o información que anteriormente no tenía acceso.

Configuración correctiva: la red de datos tiene habilitado el protocolo STP, sin embargo, en la topología física no existen enlaces redundantes, por lo cual, para evitar que cualquier puerto transmita BPDUs TCN que es el que envía información de cambios en la topología, se realizó la siguiente configuración en todos los puertos de los switches de la red de datos.

Se configuró en todos los puertos de acceso de cada switch el PortFast con el comando spanning-tree portfast default. También el bpduguard en todos los puertos de acceso y en los que se encuentran sin utilizar destinados para puertos de acceso, en caso de presentarse una conexión de un dispositivo intermedio provocará que el puerto se deshabilite al recibir una BPDU.

- **Configuración vulnerable 4:**

Se encuentra creadas siete VLAN para la comunicación de los diferentes tipos de usuarios, incluida una VLAN para la conexión remota.

Análisis: para la administración de la red se han incrementado 7 VLAN, de estas 1 (ESTUDIANTES) es para el control de todas las salas de computo (SC1 a la SC6) y la VLAN de administrativos esta compartida con las impresoras de toda la universidad, lo que provoca un inadecuado control del uso de la red de datos.

Para mantener una mejor administración del ancho de banda y manejo de usuarios, no debe mantenerse en una misma VLAN todos los laboratorios, tampoco se debería compartir una misma VLAN entre las impresoras y usuarios administrativos.

Configuración correctiva: se remplazó la VLAN estudiantes por 6 VLANs para las salas de computo (SC1, SC2, SC3, SC4, SC5, SC6) y de la VLAN de Administrativos se sacó a las impresoras y se creó la VLAN Impresoras.

- **Configuración vulnerable 5:**

Los puertos que se encuentran utilizados están asignados a su respectiva VLAN dependiendo del tipo de usuario, y los puertos que no se encuentran en uso, están en la VLAN por defecto.

Análisis: el mantener los puertos en la VLAN por defecto, genera una brecha de seguridad sobre la información de administración. Al existir otra VLAN creada para la administración de los switches, es recomendable tener inhabilitados todos los puertos que no se están utilizando.

Configuración correctiva: se configuró todos los switches con seguridad a los puertos, para lo cual se configuró port-security. La interfaz no debe estar en modo dinámico ya que esto no permitiría habilitar la seguridad en una interfaz. Asimismo, el modo restrict, esta configuración de violación a la restricción del puerto provoca que al conectarse otro dispositivo que viola la seguridad del puerto, permanezca la interfaz activa, pero elimina los paquetes. Sólo se permite tráfico de la MAC registrada inicialmente.

Diseño de la red de datos segura

En el nuevo diseño lógico de la red de datos de la PUCE SD se consideró incorporar 7 VLANs adicionales para segmentar de mejor manera los grupos de usuarios como diferenciar los estudiantes por salas de cómputo, logrando de esta manera llevar un mejor control en cuanto al uso de la red. En la figura 3 se aprecia los cambios realizados.

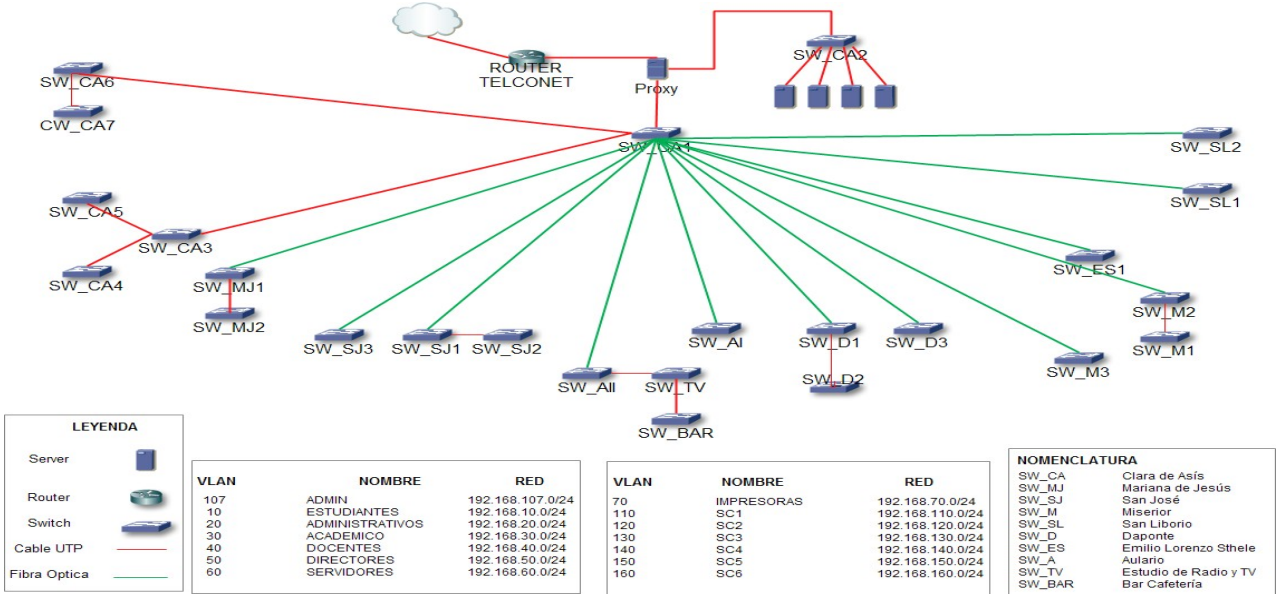

Figura 3: Diseño de red de datos segura

Fuente: elaboración propia.

Implementación de configuraciones en la red de datos

Para la implementación de las configuraciones correctivas en cada switch de la infraestructura de red de la PUCE SD se realizaron los siguientes procesos:

1. Socializar las vulnerabilidades identificados con el personal técnico del área de redes del DTI.
2. Explicar la función de las configuraciones correctivas a ser implementadas.
3. Implementar las configuraciones correctivas en cada switch en presencia de un técnico del área de redes, ya que por políticas internas del DTI, solo personal del área de redes puede acceder a los equipos de la infraestructura de red.

Pruebas de funcionamiento

Después de realizar las pruebas respectivas del comportamiento de la red, se registraron los siguientes resultados, comprobándose los resultados esperados como se aprecia en la tabla 2:

Tabla 2: Pruebas en la red de datos

VULNERABILIDADES		PRUEBAS		
N°	DESCRIPCIÓN	Respuesta obtenida		DESCRIPCIÓN
		SI	NO	
1	Todos los puertos se encuentran habilitados para permitir la conectividad de cualquier dispositivo de red.	X		Los puertos no utilizados se observan fisicamente apagados.
		X		Al ingresar intencinalmente un comando incorrecto, no realiza la busqueda de un servidor DNS.
		X		Al realizar las consultas sobre información a través del protocolo CDP presenta el mensaje ""% CDP is not enabled".
2	Tiene creadas siete VLAN's utilizando el protocolo VTP para su aprendizaje en la red.	X		Se conectó a la red un switch con VTP configurado con un número de revisión mayor. El puerto se mantiene deshabilitado.
3	La topología de red tiene implementado el protocolo Spanning Tree (STP) para garantizar una red libre de bucles o lazos de capa 2.	X		Se conectó una PC en un puerto configurado con PortFast y el puerto se habilitó en un menor tiempo.
		X		Al desconectar de un puerto de la red una PC y conectar en su remplazo un switch, el puerto se deshabilita.
4	Se encuentra creadas siete VLAN para la comunicación de los diferentes tipos de usuarios, incluida una VLAN para la conexión remota.	X		Al realizar la consulta con el comando "show vlan brief", se visualizan las vlans: SC1, SC2, SC3, SC4, SC5, SC6, impresoras. No se visualiza la vlan estudiantes.
5	Los puertos que se encuentran utilizados están asignados a su respectiva VLAN dependiendo del tipo de usuario, y los puertos que no se encuentran en uso, están en la VLAN por defecto.	X		Los puertos destinados para dispositivos finales se encuentran configurados en modo de acceso.
		X		Al ejecular el comando "show running-config" se verificó que todos los puertos de acceso se encuentren configurados con el port-security
		X		Al desconectar de un puerto de la red una PC y conectar otra PC en su remplazo, el puerto se deshabilita.

Conclusiones

- La red de datos segura de capa 2 mantiene un mejor control de acceso de los diferentes dispositivos en la infraestructura de red, permitiendo identificar los dispositivos de red en los cuales se han presentado problemas de accesos no autorizados, y de esta manera identificar oportunamente su origen.
- El nuevo diseño de la red de datos de la IES, permitió mejorar la administración, funcionamiento, y control de ancho de banda debido a la segmentación de las VLANs.
- Gracias al nuevo diseño de la red de datos de la IES, se ha mejorado la administración, funcionamiento, y control de ancho de banda debido a la segmentación de las VLANs.
- Se logró reducir notablemente los riesgos de seguridad de la información de la comunidad universitaria; la integridad, disponibilidad y confidencialidad.
- Las configuraciones realizadas permitieron a los técnicos del área de redes, considerar dentro de la administración de la red, criterios de seguridad.

Referencias bibliográficas

KATZ, M. D. (2013). Redes y Seguridad. México: Alfaomega.

WATKINS, M., & WALLACE, K. (2008). CCNA Security Official Exam Certification Guide. EEUU: Cisco Press.

STALLINGS, W. (2011). Network security essentials: applications and standards. EEUU: Prentice Hall.

TILLER, J. (2004). The Ethical Hack: A Framework for Business Value Penetration Testing. EEUU: Auerbach.