Diseño orientado a elevar la seguridad en la red troncal de la Dirección Territorial Cienfuegos de ETECSA

MSc. Denis Morejón López, Adm.or de la Red, DT Cienfuegos; Ing. Emir Sánchez Peña, Esp. Dpto. Servicios Móviles, DT Camagüey; MSc. Félix Javier Álvarez Herrera, Esp. Dpto. Servicios Móviles, DT Villa Clara; Ing. Luis Castellanos Carrión, Jefe de Grupo de Infraestructura y Soporte de la Red, VP Tecnología de la Información, ETECSA; MSc. Alexis Gómez Domínguez, Prof. Facultad de Informática, Universidad de Cienfuegos; Ing. Ricardo Fernández Cañizarez, Jefe de Brigada de Electricidad, Comunicaciones y Alarmas, CIMEX Cienfuegos
denis@cfg.etecsa.cu, emir@cmg.etecsa.cu, felix.alvarez@etecsa.cu, luis.castellanos@etecsa.cu, alexis@ucf.edu.cu, rfdezc@cimex.com.cu

I Introducción

Las redes de campus o redes troncales LAN —*Local Area Network* / Redes de Área Local— constituyen el núcleo fundamental de la red telemática de cualquier empresa o institución. Su diseño repercute, directamente, en muchos aspectos que pueden afectar o elevar su desempeño, rendimiento, fiabilidad, estabilidad y seguridad. Este último elemento se ha convertido en uno de los principales objetivos de la mayoría de las organizaciones modernas [1].

Cada vez más las empresas están usando aplicaciones que son determinantes para el funcionamiento y productividad de sus acciones. El éxito de las compañías y su supervivencia dependen de estas aplicaciones y de la productividad que pueden obtener implementándolas. De esta manera, la disponibilidad, la confiabilidad y la integridad de los datos son fundamentales.

Por otra parte, las aplicaciones y sistemas operativos desarrollados tienden aún más al uso de los servicios de redes. En consecuencia, el empleo de sistemas distribuidos, las aplicaciones remotas, los servidores centralizados aumentan considerablemente. El protagonismo se mueve, de modo significativo, desde las estaciones y redes locales hacia las redes troncales. De acuerdo con esta situación, los modelos empleados en el diseño de redes y las tecnologías utilizadas han evolucionado con rapidez y han convertido a la red en el soporte de las estrategias de seguridad y gestión de las empresas.

El presente trabajo es parte de un proyecto liderado por el Departamento de Gestión de la Seguridad Informática de ETECSA y enfocado a mejorar la seguridad en su red de gestión (GESNET). En él se describe el desarrollo de una investigación sobre los modelos de diseño y tecnologías empleadas en las infraestructuras de redes troncales, orientado primordialmente a elevar sus niveles de seguridad, estabilidad, confiabilidad, no repudio y escalabilidad. Con esto se garantizaría minimizar las afectaciones ante errores humanos y brindar a los administradores de sistemas un mayor control y supervisión de los eventos que puedan ocurrir, así como una mayor independencia en la configuración de los dispositivos y servicios de red local.

Además, disponer de una infraestructura de red troncal acorde a los requerimientos actuales —que abarque el nivel físico, topológico y funcional—, garantizaría en gran medida el cumplimiento de los objetivos de las instituciones con una dependencia elevada de la red telemática. Un ejemplo concreto lo constituyen las empresas proveedoras de servicios de telecomunicaciones —como es el caso de ETECSA— que, en general, cuentan con una red denominada Corporativa orientada, principalmente, al intercambio de información, comunicación y soporte de muchas aplicaciones que se emplean en el trabajo de oficina, facturación, atención a clientes, etc. Este tipo de empresa dispone de una Red de Gestión que se ocupa de la configuración y monitoreo de los servicios de telecomunicaciones, interconectando elementos tecnológicos como las centrales telefónicas, equipos de transmisión, equipos de acceso y las estaciones encar-

gadas de controlarlos. Estas dos redes por sus características deben estar separadas; pero, a la vez, deben permitir algunos flujos de información en sentido y sólo para usuarios definidos.

En el contexto nacional, específicamente, en la red troncal de la Dirección Territorial de ETECSA en Cienfuegos, el diseño actual no cumple con varios de los requisitos de diseño utilizados con más frecuencia; además, presenta serios problemas de seguridad y operatividad a causa de:

- Problemas de seguridad debido a la ausencia de un mecanismo que filtre o limite los tráficos que provienen de las redes externas o los generados internamente.
- Los sistemas detectores de intrusos existentes no abarcan todos los segmentos de red.
- Imposibilidad de tener un monitoreo y control sobre todos los flujos de información en la red.
- Vulnerabilidad ante fallos físicos en los enlaces por falta de redundancia.
- Imposibilidad de expansión de la red territorial con el equipamiento existente y con un adecuado ancho de banda.
- La falta de privilegios administrativos sobre el enrutador existente obstaculiza la gestión dinámica de cualquier cambio en la red.
- Imposibilidad de una administración y gestión centralizada de toda la red.

Estas dificultades frenan, en gran medida, las posibilidades de operación y comprometen la seguridad de esta red. En consecuencia, se detectó como problema principal: la carencia de un diseño de la red troncal que contemplara los elementos de seguridad y garantizara la realización de las operaciones de supervisión y control, además de brindar posibilidades de configuración, adaptación y expansión de la red de acuerdo con las necesidades de la Empresa.

Para buscar una solución al problema, se tomó en cuenta un grupo de aspectos, por ejemplo, las diferentes tecnologías que pueden utilizarse para elevar el nivel de seguridad en la red troncal de esta Entidad; el diseño a desarrollar e implementar; y la forma de validar, posteriormente, su ejecución final.

El propósito general fue implementar una nueva infraestructura de red troncal para la DT Cienfuegos a partir de modelos y tecnologías que eleven sus niveles de seguridad. En específico, se realizó una revisión de la bibliografía técnico-especializada para conocer el estado del arte referente a las tecnologías empleadas en las redes de campus: sus modelos y diseños; se seleccionaron las tecnologías de interconexión de redes y los modelos de diseños más efectivos que permitan alcanzar los niveles de seguridad esperados; se realizaron pruebas y se utilizaron aplicaciones con la finalidad de reunir elementos para la definición de las técnicas y mecanismos de seguridad a emplear, y la simulación de situaciones reales en escenarios de pruebas; finalmente, se validó la implementación mediante el empleo de herramientas de software y el análisis del comportamiento del sistema.

2 Desarrollo

Comúnmente cuando se habla de diseño de redes, se hace referencia a una u otra metodología de diseño que especifica una serie de etapas de obligatorio cumplimento para alcanzar los niveles de funcionalidad de la red esperados. Con este trabajo no se pretende hacer un diseño total de la red de esta Dirección Territorial, debido a que implicaría un análisis mucho más profundo. No obstante, teniendo en cuenta que se realizarán grandes cambios al diseño existente —encaminados a aumentar los niveles de seguridad de la red lo que incluye elevar los niveles de estabilidad, disponibilidad, confiabilidad y no repudio de origen o destino—, se abordarán modelos y diseños de redes de campus con elementos fundamentales para la solución propuesta.

2.1 Análisis de los diseños empleados en redes de campus

Una red de campus es una red de empresa que se compone de muchas Redes de Área Local en uno o más edificios, todos conectados y, usualmente, en la misma área geográfica [1]. Las siguientes secciones presentan varios modelos de redes que pueden ser empleados para clasificar y diseñar redes de campus.

Diseño Jerárquico de Red

Se puede estructurar la red de campus de una forma jerárquica. Cisco —empresa proveedora de equipamiento de interconexión de redes, líder a nivel mundial en esta materia—, por ejemplo, tiene clasificado un acercamiento jerárquico para el diseño de redes que permite a los diseñadores crear lógicamente una red definiendo y usando Capas de Servicios. La red resultante es eficiente, inteligente, escalable y administrable fácilmente. El modelo jerárquico fracciona una red de campus en 3 capas de servicio diferentes. Estas capas son:

- Capa de Acceso
- Capa de Distribución
- Capa de Núcleo

Cada una de ellas tiene atributos que suministran tanto funciones de red físicas como lógicas en el punto apropiado en la red de campus. La comprensión de cada capa y sus funciones o limitaciones es importante para aplicar correctamente la capa en el proceso de diseño [1].

Diseño de Red Modular

Diseñar una red de campus utilizando el modelo jerárquico de tres capas puede ser un poco confuso. Una aproximación más cercana a las necesidades reales del diseño es utilizar una manera lógica según el Método Modular. En este método cada capa de un diseño jerárquico de red puede ser dividida en unidades básicas funcionales. Estas unidades o módulos son dimensionados apropiadamente y conectados juntos, dejando un margen para un futuro crecimiento y expansión de la red [1].

Una red de campus de empresa puede dividirse en los siguientes elementos básicos:

- Bloque de conmutadores: es un grupo de conmutadores de capa de acceso junto con sus conmutadores de distribución.
- Bloque de Núcleo: es el *backbone* de la red de campus.

Existen otros elementos relacionados con este diseño, pueden ser designados por separado y añadidos al diseño de red. Estos elementos son los siguientes:

- *Server Farm Block* —Bloque de Granja de Servidores—: un grupo con sus servidores de empresa junto con sus conmutadores (capa) de distribución y acceso.
- *Management Block* —Bloque de Administración—: un conjunto de recursos de administración de red junto con sus conmutadores de acceso y distribución.
- *Enterprise Edge Block* —Bloque de Frontera de la Empresa—: es una colección de servicios relacionados con el acceso externo de la red, junto con sus conmutadores de acceso y distribución.
- *Service Provider Edge block* —Bloque de Frontera con el Proveedor de Servicio—: son servicios externos de red contratados o usados por la red de la empresa, donde estos son los servicios con los cuales hace de interfaz.

2.2 Red Troncal de la Dirección Territorial Camagüey

La red de ETECSA en Camagüey constituye el primer antecedente de diseño de red local orientado a la seguridad en la Empresa a nivel nacional. Sus subredes, enfocadas a funciones específicas y Listas de Control de Acceso —del inglés, *Access Control Lists* (ACL), empleadas en equipos de interconexión de redes para filtrar paquetes y establecer reglas que permiten o no el intercambio de información— que regulan el flujo de información entre ellas, y garantizan una compartimentación capaz de evitar accesos no autorizados [2]. En la figura 1 se muestra un diagrama lógico de esta red.

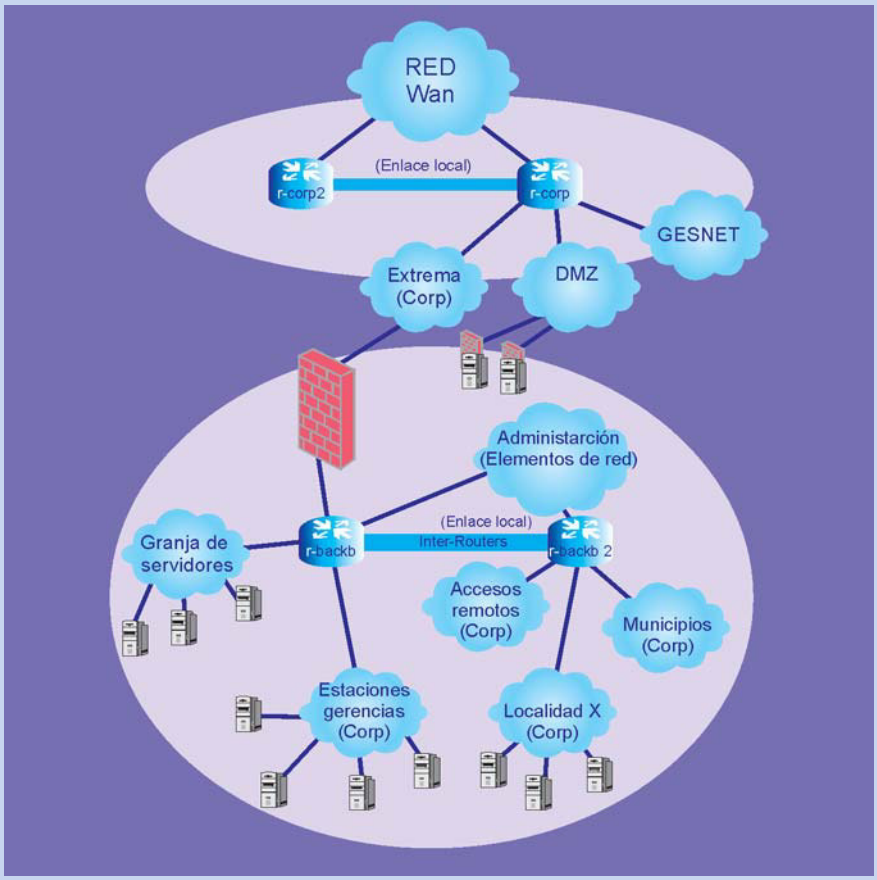

Figura 1 Esquema de la red Camagüey. (Fuente: elaboración propia).

2.2.1 Descripción

Primero es necesario aclarar la ubicación física de los equipos y subredes:

- La red WAN —*Wide Area Network* / Red de Área Extensa— es la única que se ubica fuera de la provincia; particularmente, se refiere a la red WAN de ETECSA que interconecta a todas las direcciones territoriales.
- Los 4 enrutadores se encuentran en el mismo local.
- Las redes Accesos Remotos, Localidad X y Municipios están como se infiere fuera del edificio donde se concentran los equipos anteriores.

La red LAN es conectada a la red WAN a través de 2 enrutadores —r-corp, r-corp2— que emplean distintos enlaces, con distintas tecnologías, hacia esta última. Estos enrutadores realizan prácticamente la misma función de encaminar paquetes hacia y desde la WAN, de manera que garantizan una redundancia en ese nivel. Uno de los enlaces puede sufrir avería y la comunicación se man-

tiene a través del otro enrutador. Si uno de los enrutadores se avería, el otro pudiera asumir sus funciones provisionalmente. Esa fue una decisión de los especialistas y directivos de la WAN para reforzar la disponibilidad de algunos territorios del país que constituirían centros regionales.

Es importante aclarar que cada subred de este diseño se aísla físicamente mediante el uso de la tecnología VLAN —*Virtual Local Area Network*—. En la Empresa existen 2 categorías o tipos de redes: Red GESNET y Red Corporativa. La primera es una red de gestión que engloba a los equipos de telecomunicaciones y las estaciones con acceso a ellos. La segunda abarca al resto de las estaciones y servidores, y posee servicios como el correo electrónico, sitios web, sistemas contables y de facturación, etc. En esta red trabaja el personal que no está involucrado con la operación de los equipos de telecomunicaciones.

Por norma, estas redes deben estar aisladas con un punto común de contacto que sería la red Zona Desmilitarizada —del inglés, *Demilitarized Zone* (DMZ)— donde se ubica la información necesaria para el trabajo de ambas redes [3]. Por lo tanto, en el enrutador r-corp existen reglas que impiden el acceso directo entre la Red GESNET y la Red Corporativa.

La Red Externa, que es de tipo Corporativa, se ideó con el objetivo de situar allí a las personas de la Empresa que vienen a visitar el territorio y, de ese modo, accedan con mayor facilidad a los servicios empresariales —de la WAN— que a los internos —de la LAN—. Esta facilidad se refiere al hecho de que existen reglas configuradas en el enrutador rbackb que regulan el tráfico de información entre las distintas subredes. El cortafuegos que se divisa en la figura 1 entre la Red Externa y el enrutador r-backb es una representación gráfica de estas reglas; no, un equipo independiente. Entonces, el resto de las redes podrían clasificarse como redes internas.

En la red Granja de Servidores, como su nombre indica, están situados los servidores territoriales. Existen, también, un grupo de reglas en r-backb que determinan cuáles puertos pueden ser accedidos o cuáles subredes pueden acceder allí.

La red Estaciones Gerencia es de tipo Corporativa que se ubica en el edificio principal. A esta se conectan la mayoría de los usuarios.

La red Administración se compone de los elementos de red como conmutadores, enrutadores, etc. que garantizan la gestión de la LAN exclusivamente por parte de los administradores de la red. Para ello sus interfaces de red tienen configuradas sub-interfaces dentro de la red Administración y sub-interfaces dentro de la red Estaciones Gerencia, porque necesitan comunicación con las redes externas.

Las redes Accesos Remotos Localidad X y Municipios son de tipo Corporativa y se conectan mediante el enrutador r-backb2 que posee las interfaces necesarias para comunicarlas.

2.2.2 Valoraciones del diseño

Las redes locales de la mayoría de las provincias poseen un diseño en extremo sencillo. Cuentan con apenas un enrutador sin la posibilidad de administrarlo en el territorio. Eso limita la capacidad de respuesta del territorio, en plazos prudenciales, ante las necesidades cambiantes de requisitos de seguridad y cambios topológicos que no dependan del Nivel Corporativo. Lo único estandarizado, a nivel nacional, es la presencia del segmento de Red DMZ que posibilita la comunicación entre la redes aisladas de gestión y corporativa. Dentro de este escenario, la idea de introducir elementos de capa 3 —administrados localmente, para configurar reglas, cambiar la forma en la que se concebía la función de los administradores en las redes territoriales cada vez más complejas y eliminar características del diseño de la red que hacían más sencillo a un trabajador o personal mal intencionado acceder a elementos o servicios vitales para el funcionamiento de la red— resulta un aporte importante en aras de mejorar la funcionalidad y la seguridad de las redes territoriales.

2.2.3 Aspectos positivos del diseño

- La red posee dos enlaces redundantes de salida hacia la WAN.
- Se define una subred para los equipos de interconexión Administración con reglas que la aíslan del resto de las redes.
- Se define una subred para los servidores Granja de Servidores que posibilita, en lo fundamental, diferenciar las reglas del filtrado de puertos respecto al resto de las redes que no proveen servicios a los usuarios.
- Se define una subred Externa para los invitados.
- Se mantiene el estándar de la empresa GESNET-DMZ-Corporativa para la comunicación entre las redes de GESNET y Corporativa.

2.2.4 Observaciones

- Se estructuran las redes de tipo Corporativa y no se hace en la red de GESNET que por su importancia lo amerita. De este modo, quedan mezclados, por ejemplo, los equipos de telecomunicaciones con sus estaciones gestoras, aún cuando no todos los gestores tienen que acceder a todos los equipos. Esto constituye un elemento muy importante porque la red de GESNET es un punto vital en el funcionamiento de la Empresa.
- Los administradores de red deben crearse sub-interfaces en sus estaciones para acceder a la red Administración. Si después se pretende que los administradores puedan tener libre acceso a otras subredes, habría que adicionarles una sub-interfaz en cada una de sus máquinas por cada una de las subredes a las que necesiten

acceder sin restricciones. Una forma más flexible y escalable pudiera ser crear una pequeña subred aparte para los administradores a la que se le establezcan las reglas que necesitan.

2.3 Análisis de la red de la Dirección Territorial Cienfuegos

A continuación se describirá la topología de la red troncal, sus elementos de interconexión, subredes, etc. Luego se hará un análisis crítico de la misma donde se resaltarán sus principales deficiencias.

2.3.1 Descripción de la red troncal existente

Actualmente existen 3 tipos de subredes en el entorno local:

- Red Corporativa
- Red GESNET
- Red DMZ

Las subredes Subred-1, Subred-2, Subred-Municipios son de tipo Corporativa. La Subred 3 es de tipo DMZ y la Subred 4 de tipo GESNET. Estas se conectan a la WAN por medio de un enrutador CISCO 3640. El enrutador posee 4 interfaces Ethernet (10 Mbps), 3 de ellas para conectar las subredes locales y la cuarta para conectar la red WAN. Las subredes 1 y 2 se conectan a la misma interfaz física al definirse en ellas dos sub-interfaces lógicas. Cada sub-interfaz lógica fue concebida para servir de *gateway* —es decir, se refiere a la puerta de enlace para la subred correspondiente— a su subred correspondiente.

Por ejemplo, si las subredes tienen la siguiente numeración IP:

Subred-1: 192.168.12.0/24

Subred-2: 192.168.105.0/24

Las sub-interfaces configuradas para cada subred pudieran ser:

Subinterfaz-1: 192.168.12.1

Subinterfaz-2: 192.168.105.1

La red WAN se compone de subredes de tipo Corporativa y GESNET que se ubican en las otras provincias. Estas subredes se conectan a una misma interfaz física del enrutador de igual modo que lo hacen las subredes 1 y 2. Las subredes 3 y 4 se conectan a las 2 interfaces Ethernet restantes.

La subred Municipios se conecta a través del nodo de transmisión de datos con una interfaz serial del enrutador usando el protocolo *frame-relay* —retransmisión de tramas, se emplea en redes WAN—. Esta subred se compone de las subredes que se encuentran en los municipios.

Existen sistemas de seguridad que se ejecutan sobre una PC con el objetivo de supervisar el tráfico entre la red LAN y la WAN —Snort, ARPWatch, Ntop, es decir, aplicaciones de software de libre distribución—. Estos intentan ofrecer a los administradores información sobre los eventos que ocurren en la periferia de la red local. Esta PC se conecta a un puerto espejo del conmutador de las subredes 1 y 2. El conmutador fue configurado de modo tal que dirige hacia ese puerto los tráficos que pasan a través de la interfaz conectada al enrutador para que sean supervisadas ambas subredes. En el enrutador están configuradas las Listas de Control de Acceso que garantizan el aislamiento entre las redes GESNET y Corporativa

2.3.2 Análisis de la red troncal existente

La red troncal actual presenta las siguientes insuficiencias:

1-Los técnicos del territorio carecen de privilegios administrativos sobre el enrutador. Este enrutador es administrado de manera centralizada por los técnicos de la Empresa en Ciudad de La Habana. Esta es la causa fundamental por la que no se realizan un grupo de tareas que pudieran mejorar la gestión de seguridad en la red.

2-No hay un mecanismo para supervisar el tráfico entre la red WAN y todas las subredes locales. Es cierto que existen los sistemas de seguridad perimetral; pero, estos no logran abarcar todas las subredes locales. La subred Municipios, la subred DMZ y, principalmente, la subred de GESNET, no desvían sus tráficos hacia la PC donde corren dichos sistemas. Por lo tanto, una parte importante de nuestra red queda sin supervisión perimetral. Por ejemplo, si un técnico con conocimiento de algunos controles de acceso, accediera a algún módulo de la planta digital situada en la red local de GESNET y, por error humano o intencional, desconfigurara o inhabilitara alguna funcionalidad, no habría trazas disponibles de su conexión a través de los elementos de red. Es necesario aclarar que existen en la planta, tanto controles de acceso por usuarios como sistemas de bitácora para archivar estos accesos, pero son insuficientes para alcanzar los niveles de seguridad que este caso requiere.

3-No existen reglas de control de acceso que regulen el tráfico entre las subredes o hacia determinadas estaciones individuales del territorio.

Ejemplo 1: la Red DMZ local —de gran importancia estratégica debido a su comunicación directa con la Red GESNET— puede ser accedida desde cualquier punto de ETECSA en el territorio nacional. Esta es una situación no deseada cuando los servicios que yacen en ella sólo son para pasar información entre la Red GESNET local y la Red Corporativa local.

Ejemplo 2: una estación de trabajo local pudiera estar brindando servicios no autorizados de páginas Web o mensajería electrónica por sus puertos habituales a algunos usuarios de la WAN. De este caso, se pueden derivar dos problemas: el de tramitar o difundir información ajena a los intereses de la Empresa y la vulnerabilidad asociada a mantener servicios sin la debida configuración de seguridad que rigen los administradores de una red y los responsables de seguridad informática. La inexistencia de ACLs impide establecer los servidores oficiales de estos servicios. De manera general, sin el empleo de ACLs es difícil compartimentar un escenario de red local.

Ejemplo 3: si aparece un nuevo gusano —tipo de código malicioso que afecta la seguridad en la red— en Internet, que se propague a través de un determinado puerto no sería posible bloquear dicho puerto en la entrada de la red territorial.

4-La red troncal es poco escalable porque no puede aumentarse el número de subredes debido a que sólo se disponen de 4 interfaces Ethernet en el único enrutador existente. El número total de estaciones es aproximadamente 300 y este número crece cada año, así como crece el número de minipuntos y centros de atención a la población. Otros números IP son otorgados a elementos de red como conmutadores, enrutadores y equipos de telecomunicaciones.

5-No existen subredes asociadas a determinadas funciones que posibilite la compartimentación dentro de la red local.

Ejemplo: un equipo de telecomunicaciones situado en la Red GESNET local puede ser accedido por cualquier técnico o supervisor de dicha red aún cuando no le corresponda trabajar con ese equipo. Se aclara nuevamente que siempre hay un control de acceso básico en dichos equipos. El problema radica en que los equipos de telecomunicaciones no debieran estar en la misma subred en la que están sus operarios.

Por las razones anteriormente expuestas, el diseño actual de la red troncal de ETECSA en Cienfuegos no reúne los requisitos de seguridad necesarios para alcanzar los niveles de seguridad que pretende tener la Empresa.

2.4 Descripción de la solución

Para afrontar los problemas existentes en la topología actual de la red troncal, es preciso diseñarla de nuevo. Este diseño debe regirse por modelos y estándares establecidos mundialmente; además, tener en cuenta otras experiencias como las descritas en este trabajo.

En la figura 2 se muestra el esquema topológico que se propone. El diseño incluye:

1-Inserción de un Conmutador Capa-3 entre el enrutador y el resto de los conmutadores de capa 2 existentes.

2-Creación de subredes para distintas funciones, que estén separadas mediante VLANs comunicadas por las rutas establecidas en el Conmutador Capa-3.

3-Creación de ACLs que controlen el tráfico entre las distintas subredes.

4-Mecanismo para almacenar trazas del tráfico entre las diferentes subredes.

5-Traslado de la subred Municipios que está conectada al enrutador para el Conmutador Capa-3, para que pueda ser supervisada tanto por el mecanismo de almacenamiento de trazas como por el sistema de seguridad perimetral.

6-Extensión de las subredes creadas hacia las áreas principales de la Empresa que se encuentran geográficamente dispersas —Centro de Gestión y Planta Telefónica—.

7-Implementación de protocolos para automatizar el manejo de enlaces redundantes dentro de la red troncal.

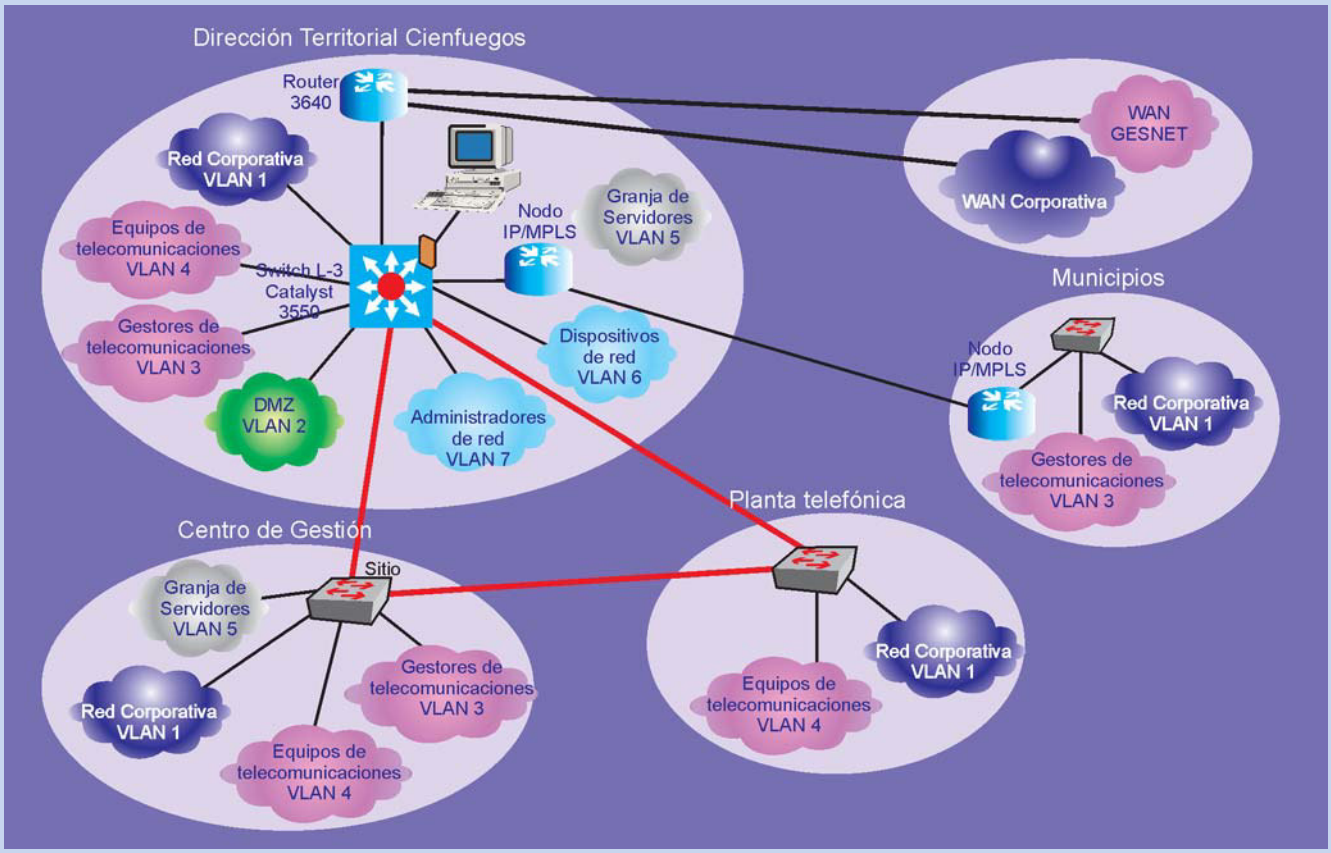

Figura 2 Esquema físico-topológico de la red territorial ETECSA Cienfuegos. (Fuente: elaboración propia).

A continuación se justificarán algunas de estas acciones, siguiendo el mismo orden en que fueron expuestas.

1-Según el modelo de diseño jerárquico, en redes de mediana complejidad deben existir uno o varios elementos que distribuyan y controlen los tráficos entre las subredes internas —Capa de Distribución—. La inserción de un Conmutador Capa-3 con 24 ó 48 interfaces Ethernet pudiera cumplir esta labor. De este modo, el enrutador existente quedará sólo para conectar la red territorial con el proveedor de servicios de conectividad —Departamento de Operaciones de la Red de la Empresa— para que este se encargue de la conexión con la red WAN empresarial.

El enrutador quedaría liberado de ejecutar ACLs y otras configuraciones que responden a intereses territoriales de Cienfuegos, incluso, pudieran cambiar con alguna periodicidad.

Hay otras razones organizativas que conllevan a tomar esta decisión. Es responsabilidad de la Dirección de Infraestructura y Soporte de la Red de la Empresa, ubicada en la capital, mantener la conectividad entre los territorios que conforman la WAN; en ese sentido, no sería prudente compartir los privilegios administrativos en el enrutador entre técnicos que se subordinan a distintos departamentos con diferentes misiones. Por ejemplo, la misión principal de esta Dirección consiste en que exista conectividad entre el enrutador y la WAN. La misión principal de los técnicos en la red territorial es garantizar la conectividad y seguridad de la red interna.

2- Según lo establecido por el diseño modular de redes, el establecimiento de bloques —o subredes— asociados a determinadas funciones garantiza una compartimentación en la red interna que evita accesos no

autorizados a determinados servicios, elementos de red, estaciones, datos, etc.

Se proponen las siguientes subredes:

a-**Subred Corporativa**: en esta subred se encuentran la mayoría de los usuarios del territorio y desde ella se accede a los servicios telemáticos comunes —correo, acceso a Internet, transferencia de archivos, etc.—.

b-**Subred de gestores de GESNET**: aquí se encuentran los gestores de telecomunicaciones que atenderán los equipos ubicados en GESNET. Cada gestor tendrá acceso a los equipos que atienda específicamente y no a todos los equipos de la subred por igual.

c-**Subred de equipos de telecomunicaciones**: se encuentran los equipos que soportan los servicios de transmisión, conmutación, datos, etc.

d-**Subred DMZ**: esta subred sirve de puente (enlace) entre las subredes de GESNET y Corporativa; por las características de compartimentación de la Empresa mencionadas no pueden comunicarse directamente.

e-**Granja de Servidores**: en esta subred están ubicados todos los servidores que hospedan los diferentes servicios a los que acceden los usuarios de la red.

f-**Subred de Administradores**: se ubican las PC de los administradores para evitar la configuración de subinterfaces que pertenezcan a esa subred.

g-**Dispositivos de Red**: se sitúan los dispositivos como conmutadores, enrutador, etc. con posibilidades de gestión remota.

h-**Subred Municipios**: se refiere al enlace con algunos municipios que antes se conectaban con *frame-relay* al enrutador 3640 y ahora se conectan al Conmutador Capa-3 y posibilita la supervisión de estos tráficos.

3- Se implementarán ACLs que permitan en cada caso controlar el acceso entre subredes. Para ello se considerarán las direcciones IP de origen y destino así como los puertos utilizados por los servicios existentes, teniendo en cuenta habilitar la funcionalidad de *logging* —se refiere a la posibilidad de tener un registro de los eventos que se configuren— para algunas reglas.

4-Se configurará un sistema de almacenamiento de trazas centralizado con el empleo del protocolo *syslog*, en particular la implementación syslog-ng, se configurará un servidor central con GNU/Linux y se habilitará en los dispositivos de red el envío de las trazas hacia este [3-4].

6-Se implementará el Estándar IEEE 802.1Q para la extensión de las VLANs configuradas para cada subred [5].

7- Se habilitará un enlace redundante activado automáticamente mediante el empleo del Protocolo de Árbol Expandido —del inglés, *Spanning-Tree Protocol* (STP)— que será previamente configurado en el conmutador, eliminando el procedimiento manual existente [5].

2.5 Implementación

Para la implementación final del diseño, se decidió dividir los trabajos en 2 etapas, de acuerdo con su complejidad y las posibles afectaciones que pudieran surgir. Además para su completa terminación, es necesaria la participación de técnicos de distintas áreas y la reestructuración de algunos servicios.

Con el propósito de describir la primera etapa, puede utilizarse como referencia la figura 3.

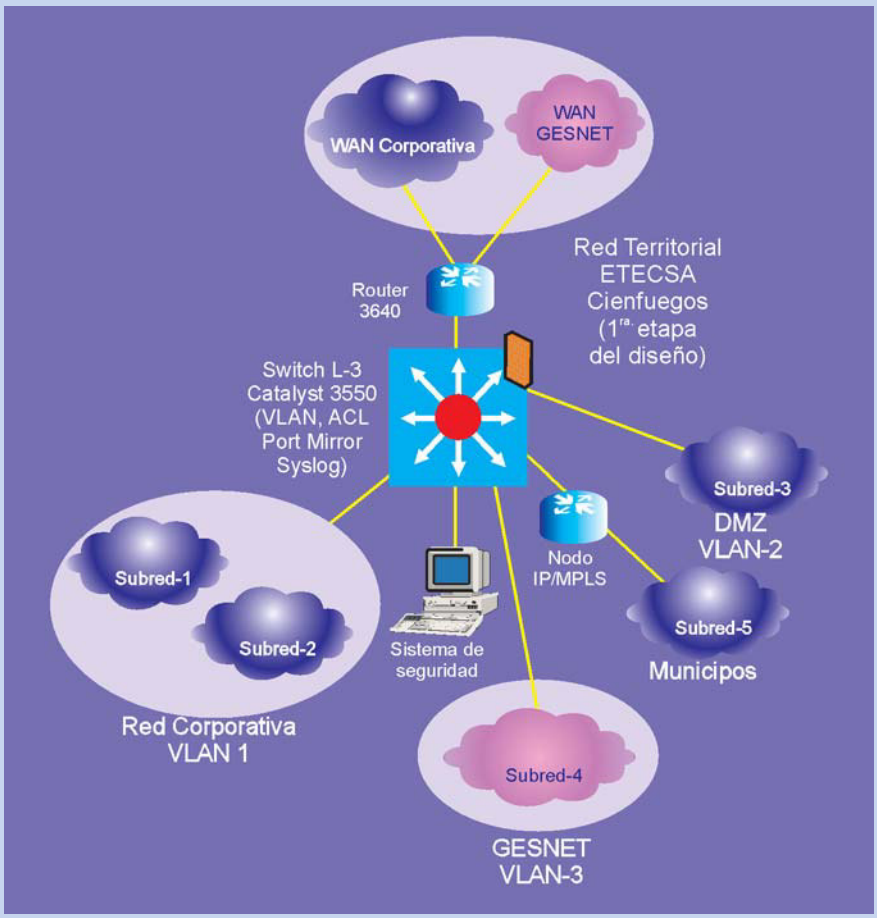

Figura 3 Esquema de la red territorial ETECSA Cienfuegos en su 1ra etapa. (Fuente: elaboración propia).

Por otra parte, también puede observarse la implementación de las acciones siguientes:

Acción	Cumplimiento
1	Se cumple completamente
2	Se efectúa parcialmente, pues sólo se implementan 3 VLANs
3	Se cumple completamente para lo implementado en esta etapa
4	Se efectúa completamente
5	Se realiza completamente
6	Se pospone para una segunda etapa
7	Se pospone para una segunda etapa

Tabla 1 Estado de cumplimiento. (Fuente: elaboración propia).

Durante la implementación de esta etapa se realizaron pruebas en escenarios reales con equipos similares a los empleados en la solución final, así mismo se validó la implementación utilizando aplicaciones de software, por ejemplo, Nmap, Ntop, comando *ping* de ICMP —Internet Control Messages Protocol / Protocolo de Control de Mensajes de Internet—, Traceroute y chequeo de las trazas generadas por los dispositivos y enviadas al servidor syslog.

3 Resultados y discusión

Es importante destacar que el costo de la implementación propuesta depende, fundamentalmente, del equipo de Capa-3 y este varía según las prestaciones exigidas. Por ejemplo, un switch Cisco Catalyst 3550, similar al empleado en el trabajo realizado, puede costar aproximadamente 3500 CUC. Sin embargo, los beneficios obtenidos son significativos, sobre todo, al valorar las pérdidas ocasionadas por las afectaciones, tanto por errores humanos como por acciones mal intencionadas, de los equipos de telecomunicaciones que brindan el soporte tecnológico de la Empresa, por ejemplo, la planta telefónica digital—. En ese sentido, la variante propuesta elimina, en gran medida, estas posibilidades al proteger los equipos vitales y supervisar el acceso a los mismos.

Un ejemplo concreto en relación con las inversiones que se necesitan sería: una avería de 24 horas en la Central Digital de la DT Cienfuegos le cuesta a ETECSA alrededor de 6000 CUC y 60000 pesos cubanos, que equivalen a 8400 CUC en total, esto sin tener en cuenta el tiempo de trabajo especializado requerido para lograr una solución. No obstante, el impacto social sería incalculable pues se afectarían, en alguna medida, los principales servicios de información, llamadas de urgencias tanto del servicio de emergencias y ambulancias de los hospitales y centros de atención como los de la PNR, MININT, bomberos y otros servicios no menos importantes relacionados con trámites de diversa índole.

Además otro elemento que realza la viabilidad de esta propuesta consiste en utilizar, en todo momento, aplicaciones de software libre y de gratis distribución.

4 Conclusiones

El nuevo diseño de la red troncal de la Dirección Territorial de Cienfuegos en ETECSA, descrito en este trabajo, logra eliminar las deficiencias existentes y permite, además, elevar los niveles de seguridad, estabilidad, confiabilidad, no repudio y escalabilidad de la red, con la garantía de minimizar las afectaciones ante errores humanos y aumentar la operatividad de la red.

Teniendo en cuenta los objetivos planteados, puede concluirse que:

1-Como resultado del trabajo realizado se logró el diseño de una nueva infraestructura de red troncal para la DT Cienfuegos, estructurado en 2 etapas de implementación.

2-Se culminó la primera etapa de implementación descrita en este trabajo.

3-Se realizó una revisión de la bibliografía técnico-especializada que permitió conocer el estado del arte referente a las tecnologías empleadas en las redes de campus, modelos y diseños empleados en las mismas.

4-Se seleccionaron las tecnologías de interconexión de redes y los modelos de diseños más efectivos que permitieron alcanzar los niveles de seguridad esperados.

5-Se realizaron pruebas prácticas y se utilizaron aplicaciones que permitieron definir las técnicas y mecanismos de seguridad empleados, simulando situaciones reales en escenarios de pruebas.

6-Se validó la implementación mediante el empleo de herramientas de software y el análisis del comportamiento del sistema.

5 Recomendaciones

A pesar del avance alcanzado en este trabajo, que concluyó el diseño de una nueva infraestructura de red troncal para esta Entidad, y con la implementación de la primera etapa descrita, existen una serie de recomendaciones en aras de completar la implementación final, mejorar los niveles de seguridad y operatividad de la red, además de posibilitar su ejecución en redes con características similares. Estas recomendaciones son las siguientes:

1-Realizar las acciones necesarias que permitan culminar satisfactoriamente la implementación de la segunda etapa del diseño descrita en este trabajo.

2-Validar la implementación final mediante el estudio y análisis de su comportamiento en situaciones reales de la operación de la red, por un periodo no menor de 3 meses que facilite mejorar algunos detalles propios de su funcionamiento estable.

3-Explotar al máximo las posibilidades de control y supervisión que ofrece la nueva infraestructura de la red troncal.

4-Mejorar la implementación final teniendo en cuenta los resultados de la validación final; las sugerencias de sus administradores de la red y operadores o usuarios finales; y las nuevas exigencias que puedan surgir por parte de la dirección de la Empresa.

5-Que con la consecución de las 4 primeras acciones pueda obtenerse una versión mejorada que permita su implementación en las redes territoriales de ETECSA.

6 Referencias bibliográficas

[1] Hucaby, David. *CCNP BCMSN Exam Certification Guide*. USA: Cisco Press Indianapolis, 2004, pp. 632.

[2] Odom, Wendell. *CCNA ICND Exam Certification Guide*. USA: Cisco Press Indianapolis, 2004, pp. 626.

[3] Santos, Omar. *End-to-End Network Security Defense-in-Depth*. USA: Cisco Press Indianapolis, 2008, pp. 444.

[4] Mann, Scott and Mitchell, Ellen L. *Linux System Security*. USA: Prentice Hall PTR, 2000, pp. 564.

[5] Donahue, Gary A. *Network Warrior*. USA: O'Reilly, 2007, pp. 599.