DISEÑO DE UNA ZONA DESMILITARIZADA (DMZ) PARA LA FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

ANDRÉS FELIPE SÁNCHEZ RESTREPO
BRAYAN DAVID HERRERA PINTO

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2018

DISEÑO DE UNA ZONA DESMILITARIZADA (DMZ) PARA LA FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

ANDRÉS FELIPE SÁNCHEZ RESTREPO
BRAYAN DAVID HERRERA PINTO

Trabajo de grado como requisito parcial
para optar el título de Ingeniero de Sistemas

Director
LUIS EDUARDO BAQUERO REY
Magíster en Seguridad Informática

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2018

NOTA DE ACEPTACIÓN

JURADO

JURADO

Bogotá D.C., marzo del 2018

RESUMEN

El presente documento tiene como propósito brindar un modelo de red de datos, que ayude a incrementar la seguridad de la información de la Fundación Universitaria Los Libertadores (FULL), para esto se ha desglosado el contenido en una base teórica en la cual se exponen los elementos más importantes de la seguridad dentro de una red de datos, la cual puede estar constituida por diferentes elementos tales como router, switches, hub entre otros elementos. Estos componentes deben ser distribuidos en un orden que garantice el funcionamiento continuo de la red de datos en general.

Para esto, se planteó una problemática general que tienen las instituciones de nivel superior para las redes de datos y se planteó un diseño de zona desmilitarizada (DMZ) con una configuración pertinente que ayudara a elevar la seguridad que actualmente posee la FULL. Dentro de este documento se encontrará un marco teórico que ayudara a conocer el concepto de una DMZ, como lo son las zonas de seguridad y defensa perimetral, detección de intrusos, filtrado de contenido entre otras. Se encontrará información sobre las leyes y estándares que son aplicados al uso de recursos tecnológicos.

En el desarrollo de este documento se realizó un levantamiento de información de la FULL con los cuales se pudo realizar un diseño de mejoramiento de la red de datos, teniendo en cuenta las políticas de seguridad será omitida una parte de la información suministrada por el personal administrativo del área de sistemas de la FULL. Finalmente se llevó a cabo una serie de cambios en los diseños que actualmente posee la red de datos de la FULL y se establecieron recomendaciones que se sugiere aplicarse para el buen funcionamiento de los diseños propuestos.

PALABRAS CLAVE: DMZ, seguridad informática, seguridad perimetral, seguridad en redes.

ABSTRACT

The purpose of this document is to provide a data network model that will help to increase the security of the information of the Fundación Universitaria Los Libertadores (FULL), for this the content has been broken down into a theoretical basis in which the most important elements are exposed of security within a data network, which can be constituted by different elements such as router, switches, hub among other elements. These components must be distributed in an order that guarantees the continuous operation of the data network in general.

For this, a general problem that university institutions have at the level of data networks was raised and a demilitarized zone design (DMZ) with a relevant configuration was proposed that will help to raise the security that FULL currently has. Within this document there will be a theoretical framework that will help to know the concept of a DMZ, such as the perimeter security and defense zones, intrusion detection, content filtering, among others. You will find information about the laws and standards that are applied to the use of technological resources.

In the development of this document, an information survey of the FULL was carried out with which it was possible to design a data network improvement, taking into account the security policies. Some of the information provided by the administrative staff will be omitted. of the systems area of the FULL. Finally, a series of changes were carried out in the designs that the FULL data network currently has and recommendations were established that are suggested to be applied for the proper functioning of the proposed designs.

KEYWORDS: DMZ, computer security, perimeter security, network security.

INTRODUCCIÓN

El presente trabajo hace referencia a la implementación de buenas prácticas en el diseño esquematizado de redes, los cuales deben contener elementos optimizados que permitan mejorar la conectividad entre los elementos tecnológicos que componen la topología de red de datos. En este documento se encuentra información de la Fundación Universitaria Los Libertadores (FULL), para la cual fue realizado este proyecto.

Los diferentes cambios que ha sufrido la tecnología a través de los tiempos, hacen que nuevas ideas o nuevos conceptos surjan y puedan ser utilizados e implementados en cualquier topología de red, para esta investigación se habla de las zonas seguras, zonas perimetrales o la llamada zona desmilitarizada. Las cuales elevan la seguridad de cualquier topología de red de datos que quiera trabajar este diseño dentro de su red interna, este tipo de soluciones son aplicadas principalmente para separar los componentes que no deben tener accesos hacia la internet, de los componentes que si deben navegar o intercambiar información con la internet, es decir que crea un tipo de segmentación personalizado que protege o incrementa el nivel de seguridad en la información que debe ser pública a la información que no debe tener acceso público.

Durante el desenlace del contenido principal de este proyecto se encuentra información de los componentes de una red datos y estructuración de la misma, se brinda información sobre elementos de última tecnología que se encuentran actualmente en el mercado. El objetivo principal es identificar los elementos que pueden ser mejorados a nivel tecnológico y proponer mejores elementos tecnológicos que puede ser utilizado dentro de la red datos que utiliza la FULL.

TABLA DE CONTENIDO

Pág.

LISTADO DE TABLAS

Pág.

TABLA GRÁFICOS

Pág.

ANEXOS

Pág.

1. EL PROBLEMA Y SU CONTEXTO

1.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad se hace necesario que todas las empresas e instituciones cuenten con una conexión de red segura, para esto utilizan diversos controles que garanticen que el intercambio de información a través de la red tenga un buen nivel de seguridad. Por esto, en la Fundación Universitaria Los Libertadores, los sistemas de seguridad debe ser una necesidad obligada para proteger la información de la institución. Aunque los sistemas de seguridad no brindan una seguridad total (100%), si se puede lograr que la información tenga niveles más altos en su seguridad, para esto se crea configuraciones locales en la red de datos, conocidas como DMZ, la cual proporcionar un nivel seguridad más alto de red de datos en la institución y permite establecer límites en los datos que deben ser públicos, de los privados.

Resaltando así que toda red de datos puede ser vulnerable y que cada día surge un nuevo malware o una nueva forma de acceder a las redes datos y más aún con el último acontecimiento ocurrido en el 2017 (Ransomware, Wannacry), es bueno estar a la vanguardia tecnológica a nivel de seguridad en las redes de datos. Como tal los ataques que han sufrido la FULL no han sido de gran relevancia, ante toda la comunidad estudiantil es importante tener en cuenta que aun así no están exentos de sufrir dichos ataques y más aún cuando esta red maneja datos personales y bancarios que pertenecen a la FULL. La institución tiene la obligación de implementar y elevar la seguridad en toda la red de datos para así estar prevenidos para cualquier ataque que se pueda presentar. Tal como se muestra en la tabla 1, cifras de ataques informáticos en américa latina, se plantea este proyecto para establecer nuevas medidas de seguridad en la red de datos para la Fundación Universitaria Los Libertadores (FULL).

Tabla 1. Cifras de ataques informáticos en américa latina

Sectores	Ataques por día	Porcentaje	Tendencia a futuro
Financiero	6.600.000	75,29%	Aumentarán
Gobierno	925.600	10,56%	Aumentarán
Comunicaciones	737.200	8,41%	Se Mantendrán
Energía	325.347	3,71%	Descenderán
Industria	173.900	1,98%	Aumentarán
Comercio	3.600	0,05%	Aumentarán
Total	**8.765.647**	**100%**	

Obtenida de www.csiete.org, fecha publicación marzo 2017 cifra de ataques informáticos en América latina.

Siendo usuarios del sistema, se evidenciaron caídas del sistema, lo cual perjudico el correcto funcionamiento de las actividades académicas, aunque estos logs no fueron proporcionados por el área de sistemas se tienen conocimiento que por parte de asignaturas en la carrera de ingeniería de sistemas se llevaron a cabo laboratorios de denegación de servicio en los servicios ofrecidos por la FULL.

1.2 FORMULACIÓN DEL PROBLEMA

La interrogante más importante en el entorno empresarial, es la cantidad de recursos tecnológicos que se necesitan para conformar una red de datos y las configuraciones necesarias para el aprovechamiento del hardware.

¿Cuál es el diseño adecuado de una DMZ para la red de datos de la Fundación Universitaria Los Libertadores?

El punto de acoplar un diseño de arquitectura de red DMZ, es poder elevar la seguridad frente a la distribución que existe en los elementos que constituyen la red de datos de la Fundación Universitaria Los Libertadores, y así poder brindar continuidad en los servicios ofrecidos.

1.3 JUSTIFICACIÓN

Las diferentes topologías de red de datos conocidas en el mundo globalizado del internet, hace que cada vez sea mayor el nivel de ataques e incidencias de seguridad en las diferentes redes, tanto a nivel global, como a nivel local, por consiguiente, hace que la información que es trasmitida posea riesgos de seguridad, los cuales permite que la información confidencial sea utilizada por personas inescrupulosas.

Este proyecto cuenta con una configuración de seguridad más adecuada, gracias a una tecnología llamada DMZ, con la cual se garantiza que la información pública estará separada de la información privada, con una correcta configuración de políticas de seguridad y diseño adecuado de la red de datos en la FULL, la institución podrá contar con una configuración de protección de la información mucho más alto.

1.4 OBJETIVOS

1.4.1 Objetivo general

Diseñar una arquitectura DMZ en la red de datos para la Fundación Universitaria Los Libertadores y así incrementar la seguridad en los diferentes servicios que se ofrece a través de ella.

1.4.2 Objetivos Específicos

- Identificar qué servicios son los que no debe tener acceso público y deben separarse aplicando un modelo DMZ.
- Establecer reglas de seguridad sobre los elementos que componen la DMZ para la FULL.
- Diseñar mejoras de la arquitectura de red de datos con la que cuenta la FULL.

1.5 ALCANCE

El presente trabajo brinda una nueva propuesta de mejora para la red de datos, de la Fundación Universitaria Los Libertadores, donde se toma la información de la red interna que existe actualmente, se realiza un análisis sobre los elementos que la conforman y así proporcionar recomendaciones y mejoras que se pueden aplicar en red de datos actual.

1.6 LIMITACIONES

- La falta de acceso a las políticas de seguridad que se tienen actualmente en la institución.
- No tener implementada la certificación ISO27000 en la institución.
- No tener acceso al servidor de pruebas para realizar laboratorios de vulnerabilidades.
- No tener los medios para presentar el diseño detallado de la DMZ y aplicar los análisis de vulnerabilidad que se requieren.

1.7 LÍNEA DE INVESTIGACIÓN

Siendo la ingeniería de sistemas el engranaje de los métodos sistemáticos y herramientas encaminados a la seguridad en las redes, donde establecen los procesos basados en mejores prácticas e impartiendo calidad al proceso desarrollado, la Fundación Universitaria Los Libertadores, ha establecido semilleros e investigación en el área de seguridad informática, con el fin de sembrar en la comunidad educativa, actitudes de carácter investigativo que ayudará en un mediano y largo plazo en el crecimiento de los estudiantes. Estos semilleros investigativos hacen parte del grupo de investigación y desarrollo de nuevas tecnologías de la información y telecomunicación (grupo de investigación GUIAS, antes llamado GRIDNTIC) establecida a nivel nacional la cual da el sello de buenas prácticas en las propuestas investigativas.

2. MARCO REFERENCIAL

2.1 ESTADO DEL ARTE – ANTECEDENTES

Estado del arte puede definirse como una recopilación de información sobre un conocimiento de lo ya existente en un área de saber, para este caso se diseñó el siguiente gráfico 1 el cual describe como se aplicará la investigación que se llevará a cabo.

Gráfico 1. Concepto del estado del Arte

Nota: Este grafico es diseñado para uso de este documento, por los estudiantes de la FULL.

Cuando se analiza la defensa en profundidad en el ámbito informático se deben tener en cuenta los siguientes puntos; en el ámbito de la seguridad informática, está presente en el hecho de que siempre existirán nuevas formas de ataque (actualmente la defensa no tiene la iniciativa).

La información: va a permitir, en particular, la disminución de la incertidumbre sobre las acciones enemigas confirmando o refutando las hipótesis y ayudará a evitar los ataques por sorpresa. La información no debe estar disociada de la planificación.

El origen de las amenazas

- En la seguridad informática se encuentra el aspecto global del ataque que proviene del interior y del exterior. la profundidad del dispositivo de protección deberá, por lo tanto, definirse en varias dimensiones. Esto significa que la profundidad de la defensa deberá contemplar la organización, la implementación y las tecnologías, sin contentarse con una simple defensa perimétrica frente al "exterior" del sistema.

Para que exista defensa en profundidad se requiere como mínimo:

- Varias líneas de defensa independientes en el sentido en que cada una sea capaz de defenderse sola contra todos los ataques. Cooperación entre las líneas de defensa, sino el concepto es llevado únicamente a simples barreras sucesivas cuya resistencia no depende de la anterior (entonces pueden ser atacadas sucesivamente).
- La pérdida de una línea debe permitir reforzar la defensa y no debilitarla.

2.2 ANTECEDENTES

En un primer trabajo denominado IMPLANTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL de (Carlos Diaz, SEPTIEMBRE 2013). Este proyecto está basado en un diseño e implementación de un sistema de seguridad perimetral. Para ello, establecieron los principales elementos de seguridad que lo conformaría, este documento está dividido en dos partes; en la primera parte se exponen los elementos más importantes de la seguridad perimetral, haciendo parte los elementos como lo son el Firewall, IDS/IPS, Antivirus, Proxy, Gestores de ancho de banda, etc. en segundo lugar se tiene en cuenta los distintos firewalls usados y configuraciones que estos poseen para la seguridad perimetral.

En un segundo trabajo sobre: DISEÑO DE ASEGURAMIENTO REDES UTILIZANDO DMZ de (Hector Rodolfo, MAYO 2009). Este proyecto está basado en la construcción de un diseño utilizando DMZ para la seguridad en una organización. En donde se deja en claro por qué es importante la seguridad informática y como esta clase arquitectura de red es una muy buena opción para el resguardo de información sensible dentro de una empresa.

2.3 ZONA DE SEGURIDAD Y DEFENSAS PERIMETRALES

La arquitectura de seguridad tiene como objetivo la defensa del perímetro de red (DMZ). El perímetro es el punto o puntos de separación de la red interna confiable para la organización, que se encuentra en contacto con otras redes no fiables (Elizabth D. Zwicky). Estas redes no fiables no sólo son la red de Internet, sino otras redes de usuarios o extranet relacionadas con la organización con las que se tenga conexión. El perímetro se delimita a través del uso de líneas de cortafuegos que actúan a modo de barrera separando de forma lógica las diferentes zonas de seguridad.

Las zonas externas engloban todos aquellos servicios y redes que realizan un uso intensivo de Internet y por tanto se caracterizan por un alto nivel de exposición frente a ataques o incidentes de seguridad al tener interconexión directa a la red pública de Internet. La parte interna engloba todos los sistemas internos, redes de usuarios internas y la interconexión con otras intranets y extranet, relacionada con la organización.

2.3.1 Defensa de red

Al tener una red DMZ no se debe descuidar las redes internas frente a posibles ataques cuyo origen pueden ser las propias redes externas, para esto, se llevan a cabo segmentaciones de redes para evitar la visibilidad directa entre las mismas (Carlos Diaz, SEPTIEMBRE 2013), su actuación a frente a posibles ataques o comportamientos. La inclusión de protocolos de cifrado IPsec/SSL para el transporte seguro de los datos a través de redes no confiables como internet o entre las propias redes internas identificadas.

2.3.2 Detección de intrusiones

La previa monitorización de las redes más expuestas a ataques, se realizan a través de sistemas de prevención intrusiones (Villalon). Los cuales se encargan de analizar el tráfico de red en busca de posibles ataques o patrones de ataques previos. Los comportamientos de dichos sistemas pueden ser solo informativos, se realizan a través del envió de alertas o mediante la detección y terminación de los distintos ataques.

2.3.3 Características de una DMZ

Entre las características más comunes dentro de las DMZ se pueden encontrar las siguientes:

- Filtrado de paquetes
- NAT, mapeo bidireccional
- Colas de tráfico y prioridad
- Filtrado de contenido

2.3.4 Filtrado de paquetes

La acción de filtrar paquetes es bloquear o permitir el paso de datos en forma selectiva, según van llegando a una interfaz de red. Los criterios que se usan para inspeccionar los paquetes, son tomados de la información existente en la capa 3 (IPv4, ICMP, IPv6) y en la capa 4 (TCP, UDP, ICMP, y ICMPv6) de las cabeceras de los paquetes. Los criterios que más se utilizan son los de la dirección de origen y de destino, el puerto de origen y de destino, y el protocolo. Las reglas de filtrado especifican los criterios con los que debe concordar un paquete y la acción a seguir, bien sea bloquearlo o permitir que pase, que se toma cuando se encuentra una concordancia.

Las reglas de filtrado se evalúan por orden de secuencia, de la primera a la última. La última regla que concuerde será la que dictamine qué acción se tomará con el paquete. Al principio del grupo de reglas de filtrado hay un pass all implícito que indica que,

si algún paquete no concuerda con ninguna de las reglas de filtrado, la acción a seguir será dejarlo pasar, o sea permitirle el acceso.

La traducción de direcciones de red, o NAT (Network Address Translation) es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP que han asignado hacia una red externa es inferior a la cantidad de equipos que accedan a dicha red. Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT (Elizabth D. Zwicky). La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

- Invertir los cambios en los paquetes devueltos.
- Asegurarse de que los paquetes devueltos pasen a través del firewall y no sean bloqueados.

2.3.5 Colas de tráfico y prioridad

Poner algo en cola es almacenarlo en orden, a la espera de ser procesado (Hector Rodolfo, MAYO 2009). Dentro de una DMZ, cuando se envían paquetes desde un servidor, éstos entran en un sistema de colas en el que permanecen hasta ser procesados por el sistema.

2.3.6 Filtrado de contenido (Caching)

La ventaja del caching consiste en que cuando varios clientes solicitan el mismo objeto, este puede proporcionárseles desde el caché (Carlos Diaz, SEPTIEMBRE 2013). De este modo, el cliente obtiene los datos de una forma más rápida y se reduce al mismo tiempo el volumen de transferencias en la red.

Además del caching, ofrece múltiples prestaciones tales como:

- La definición de jerarquías de servicios para distribuir la carga del sistema.
- Establecer reglas de control de acceso para los clientes que quieran acceder.

- Permitir o denegar el acceso a determinadas páginas web con ayuda de aplicaciones adicionales.

2.3.7 Proxy cache Web

Un proxy generalmente proporciona una cache para las páginas web y los contenidos descargados, que son compartidos por los equipos de la red, al mismo tiempo esto libera de carga hacia los enlaces de Internet.

Funcionamiento de un proxy cache web:

- El cliente realiza una petición (E.J. navegador web) de un recurso de internet (página web) especificado por una URL.
- El proxy recibe la petición, busca la URL resultante en su cache local. Si es correcta, devuelve el documento, si no lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su cache para futuras peticiones.

Los proxys son también usados para filtrar webs, dichos filtrados se realizan mediante listas de URLs prohibidas, que puedes estar clasificadas según al tipo que pertenezcan, como son las redes sociales (Facebook) entretenimiento, videos, etc. (Elizabth D. Zwicky). De esta manera se restringe el acceso a determinadas web que se considere perjudicial para el buen funcionamiento, o incluso para la distracción y el mal aprovechamiento del tiempo de trabajo.

Como principales ventajas se tienen las siguientes afirmaciones:

- Ahorro de Tráfico: Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
- Velocidad en Tiempo de respuesta: El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.

- Demanda a Usuarios: Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- Filtrado de contenidos: El servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- Modificación de contenidos: Basándose en la misma función del filtrado, y llamado proxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Como principales desventajas se tienen las siguientes afirmaciones:

- Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché. Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.
- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.
- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

2.3.8 Servidores DNS

Son utilizados para proveer a las computadoras de los usuarios un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando este está bien configurado (Villalon).

Los usuarios generalmente no se comunican con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (ej navegadores, clientes de correo, aplicaciones que usan internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo, comprueba si la respuesta se encuentra en la memoria cache. En el caso de que no se encuentre, la petición se enviara a uno o más servidores DNS.

2.3.9 Gestor de ancho de banda

Los gestores de ancho de banda ayudan a establecer un mínimo y máximo para un tipo concreto de tráfico. El ancho de banda (Traffic control o traffic shaping) de la red puede garantizarse para los servicios esenciales durante los periodos de alta congestión (Elizabth D. Zwicky). Por lo tanto, en caso de saturación, ese tipo de tráfico disfruta del ancho de banda asignado y no nota esa congestión. Es recomendado asegurarse que las aplicaciones y los recursos críticos reciben una cantidad garantizada del ancho de banda disponible.

La gestión del ancho de banda tiene como objetivos responder las siguientes preguntas:

- ¿Quién debería obtener un determinado nivel de servicio para ciertas aplicaciones?
- ¿Qué nivel de prioridad debería asignarse a cada tipo de tráfico?
- ¿Para qué tipo de tráfico debe garantizarse su entrega?
- ¿Qué cantidad de ancho de banda debe ser reservada para garantizar un correcto funcionamiento?

2.3.10 Sistema de monitorización de equipos

Un sistema de monitorización es una solución que permite ayudar a controlar cualquier equipo de una arquitectura de red implantada. Es decir, se puede saber en todo momento el estado de la maquina monitorizada, así como el estado de cualquier servicio que dicha maquina proporciona, pudiendo actuar de manera inmediata en el caso de que se produjera algún tipo de fallo. En caso de producirse cualquier fallo, se podrá optar por varias maneras de advertir el hecho, ya sea reportándolos vía email, SMS, y/o solucionándolos automáticamente antes de que el cliente o usuario final pueda darse cuenta de los mismos (Leonardo Barrera, 17/10/2012).

Hay tres valores técnicos fundamentales a la hora de elegir un sistema de monitorización adecuado para nuestro entorno, independientemente del precio o facilidad de instalación y de utilización. A continuación, se especifican los tres valores técnicos:

- Forma de presentar los datos, las alarmas y gráficos para su estudio. Estos han de ser lo más eficientes posible y ofrecer una idea de los problemas de un solo vistazo.
- Ubicación, distancia entre equipos y tipo de conexión (velocidad y rendimiento). A más distancia y cantidad de equipos, así como con conexiones lentas, es conveniente utilizar agentes locales que reporten a un servidor central.
- Sistemas operativos que se monitorizan.

2.3.11 Bastionado de equipos

Pese a la efectividad de las barreras de seguridad perimetral, no nos ofrecen soluciones en servicios expuestos a redes públicas por requisitos del servicio (como es el caso de servidores Web, SMTP, etc.) (Hector Rodolfo, MAYO 2009). Para estos activos se utilizara los medios a nuestro alcance el reducir al mínimo las posibilidades de intrusión, su impacto y propagaciones resto de elementos de la infraestructura.

Como herramienta básica para lograr este fin, se dispone del bastionado o configuración segura de dispositivos, sistemas operativos y aplicaciones.

Cada sistema requiere de un procedimiento de bastionado distinto en función de los elementos que incluya, con lo que escapa a la finalidad de este documento, no obstante, si podemos esbozar las directrices básicas del proceso de bastionado y configuración segura que se deberían aplicar a cada uno de los sistemas a implantar.

Reducción y control de puntos de acceso a los sistemas:

- De forma remota.
- De forma local.

Prevención frente a ataques comunes:

- A nivel de comunicaciones de red.
- A aplicaciones.
- Por configuraciones por defecto o innecesariamente permisivas.
- Por revelación de información sensible de forma innecesaria.

Reducción y control de permisos:

- A usuarios.
- A aplicaciones.
- Información y recursos

Protección mediante reglas:

- Mostrado de condiciones de uso.
- Tratamiento de la información.

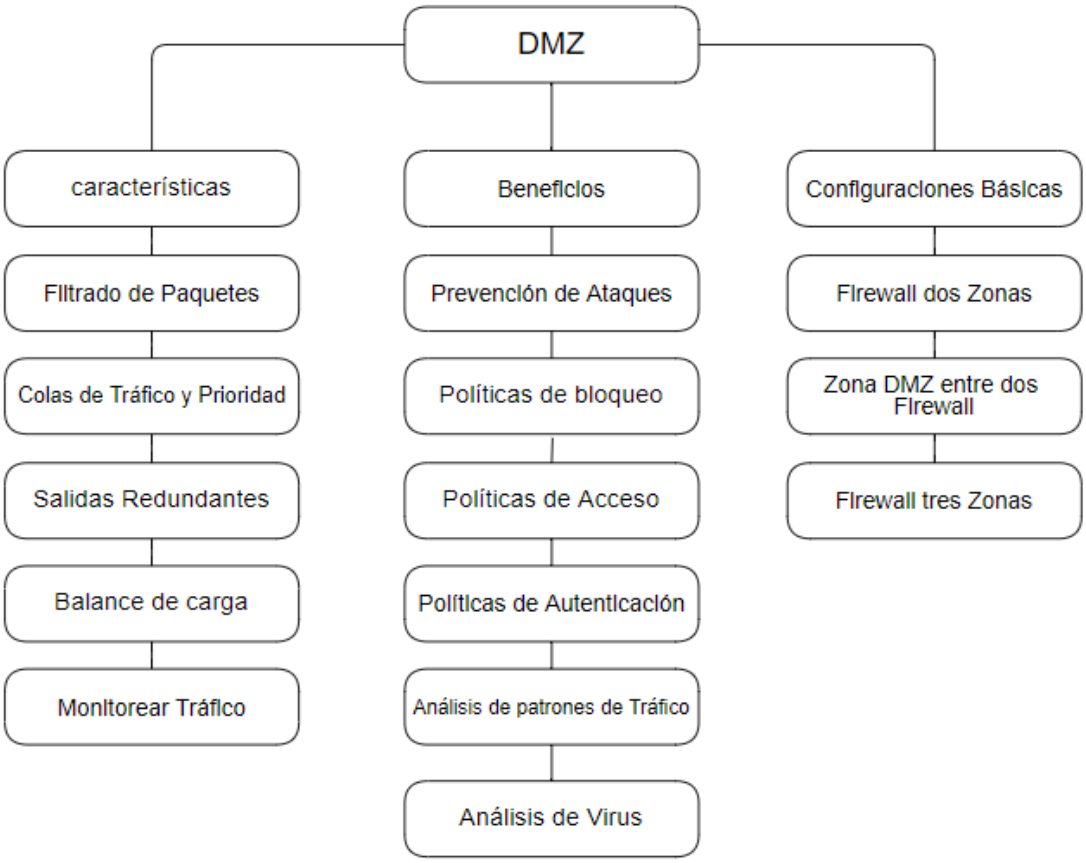
Activación de la monitorización de los sistemas:

- Acceso al sistema.
- Acceso a aplicaciones.
- Acceso a la información y recursos.

2.4 MARCO CONCEPTUAL

Las DMZ son usadas habitualmente para ubicar servidores, que es necesario que sean accedidos desde fuera, en la siguiente ilustración podremos ver las distintas características, beneficios y configuraciones que una DMZ brinda.

Gráfico 2. Diseño Marco Conceptual



Nota: Este Gráfico es diseñado para uso de este documento, por los estudiantes de la FULL.

2.5 MARCO LEGAL

2.5.1 Legislación Colombiana

En la LEY ESTATUTARIA 1581 DE 2012 octubre 17 Articulo 5 se habla sobre los datos sensibles, por los cuales se entienden datos que afecten la intimidad del titular o cuyo mal uso pueda generar discriminación, tales como, convicciones religiosas o filosóficas, que revelen el origen racial o étnico, la orientación política, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Leonardo Barrera, 17/10/2012).

- Cuando el titular haya dado su autorización explícita a dicho procedimiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- Cuando el tratamiento de los datos es necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorga su autorización.
- Cuando el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- Cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando el tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

El tratamiento de datos personales de niños, niñas y adolescentes salvo aquellos datos que sean de naturaleza pública (Leonardo Barrera, 17/10/2012).

En donde es tarea del estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes y tutores sobre los eventuales riesgos sobre el tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás

2.5.2 Estándares

La implementación de estándares internacionales como los son la ISO/IEC 27001 el cual está diseñado con la intención de proporcionar un modelo el cual permita implementar, operar, monitorizar, revisar y mantener un sistema de se seguridad de la información, para una organización, la implementación de esta norma supone un paso de calidad en lo que respecta a su trabajo. A la hora de implementarla, los objetivos, tamaño y estructura de la organización, marcara la rigurosidad de las medidas a aplicar.

Otra de las normas que es importante mencionar es la ISO/IEC 27002 la es una norma con carácter internacional que ofrecen consejos y recomendaciones de cara a la gestión de la seguridad de la información. Está dirigida a los responsables de mantener la seguridad en una organización. El objetivo de la misma es disponer de una base a través de la cual implementar normas de seguridad en una empresa sea un proceso sencillo, eficaz y práctico (www.iso.org).

3. LA INSTITUCIÓN

3.1 RESEÑA HISTÓRICA

El 14 de mayo de 1982 es una de las fechas más importantes para la Comunidad Libertadora, pues ese día se firmó el Acta de Constitución de una de las instituciones educativas más promisorias del país. Se conformó el primer Consejo Directivo y la Asamblea nombró al Doctor Hernán Linares Ángel como su primer gestor y representante. Días después, la Resolución 7542 del 18 de mayo de 1982, expedida por el Ministerio de Educación Nacional, le dio vida jurídica a la Fundación Universitaria Los Libertadores. Así, nuestra institución quedó legítimamente constituida, iniciando labores formalmente de 26 de agosto de ese mismo año.

Desde sus inicios, el Proyecto Educativo Institucional Libertador (PEI) recogió y sistematizó el espíritu que infundieron los fundadores: ser una comunidad académica que genere espacios para el desarrollo integral de las personas y de la sociedad, y vivir bajo los valores fundamentales de la vida y obra de nuestros Libertadores: Simón Bolívar, Francisco de Paula Santander y Antonio Nariño.

El crecimiento de la Fundación Universitaria Los Libertadores ha sido constante y evidente durante estas más de tres décadas, y se refleja en el desarrollo de los programas académicos, de pregrado y posgrado, que utilizan metodologías presenciales, a distancia y virtuales. El desarrollo institucional, además, se percibe en la expansión de la infraestructura física, en la adquisición de recursos variados y suficientes para el cumplimiento de sus pretensiones misionales, y en el cada vez mayor número de estudiantes, colombianos en busca de su formación profesional y humana.

Parte importante de la identidad institucional está basada en respetar el legado histórico que la antecede. Al mismo tiempo, se enfrenta y adapta a los retos de la educación contemporánea. Las tecnologías de la información, por ejemplo, plantean preguntas importantes que la Institución ha sabido encarar, incorporando estas nuevas herramientas a las lógicas educativas. Ese mismo sentido de innovación se ha utilizado para entender y enfrentar las cambiantes dinámicas económicas, sociales y

culturales de la sociedad colombiana. La capacidad de adaptación nos pone a la vanguardia de la oferta educativa nacional.

Por todo esto, la Fundación Universitaria Los Libertadores escribe la historia de la educación superior en Colombia mediante su visionario sentido de pertenencia e innovación (Los Libertadores, s.f.).

3.2 DIRECTRICES INSTITUCIONALES

3.2.1 Misión

Formar integralmente profesionales y ciudadanos críticos con amplio sentido de lo social, ético, estético y político; competentes, investigativos, innovadores y con espíritu emprendedor, mediante la cualificación permanente del proyecto pedagógico, curricular y administrativo, que estén en concordancia con los avances de la ciencia, la tecnología y sustentados en el desarrollo económico, político, social, educativo y cultural de los ámbitos local, regional, nacional e internacional (Los Libertadores, s.f.).

3.2.2 Visión

La Fundación Universitaria Los Libertadores se proyecta como una organización social de educación superior con liderazgo en el uso de las tecnologías como mediadoras en los procesos de formación integral en los campos social, económico, cultural, político, humanístico y científico, mediante estrategias presenciales, a distancia y virtuales, con propuestas de formación permanente, uso de metodologías innovadoras adecuadas al contexto de la educación superior local, nacional e internacional, para contribuir al desarrollo de la sociedad colombiana (Los Libertadores, s.f.).

3.3 SISTEMA DE GESTÓN DE CALIDAD

La Institución recibió del Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) la renovación y ampliación del certificado de calidad SC 5677-1, que es otorgada por el diseño y desarrollo de programas académicos y servicios de educación universitaria en programas de pregrado y posgrado en la modalidad presencial, virtual y a distancia. La recertificación y ampliación de nuestro sistema de gestión de calidad confirma el cumplimiento frente a los requisitos de la NTC-ISO 9001/2008 (Los Libertadores, s.f.).

3.3.1 Política de Calidad

La Fundación Universitaria Los Libertadores forma integralmente a sus estudiantes mediante el cumplimiento del Proyecto Educativo Institucional Libertadores (PEIL). Este documento contiene los objetivos, los compromisos, retos y proyecciones de la Institución, lo que incluye su apuesta por un alto nivel educativo.

Desde 1985, la Institución implementó el Primer Modelo de Evaluación Institucional, pensando en la mejoría permanente. De 1999 a 2001 se inició el seminario institucional permanente de acreditación, con el objetivo de analizar la situación en vías de este proceso. Siete años después, tras procesos sustanciales de análisis, se reglamentó la organización y el desarrollo del proceso de acreditación de alta calidad.

Actualmente, la dirección de aseguramiento de calidad y acreditación es la encargada de guiar, desarrollar y monitorear estos importantes procesos en toda la institución, con el fin último de lograr la acreditación institucional (Los Libertadores, s.f.).

Objetivos de Calidad:

- Asegurar las competencias del talento humano.
- Gestionar los recursos necesarios para el desarrollo de las actividades definidas en los procesos.

- Incrementar los niveles de satisfacción de los miembros de la comunidad libertadora.
- Mejorar de manera continua la gestión y el aseguramiento de la calidad.

3.4 ESTRUCTURA ORGÁNICA

En el anexo 1 se puede ver la estructura organizacional de la Fundación Universitaria Los Libertadores. Con la cual podremos evidenciar las distintas áreas, con las cuales relacionaremos el tipo de proyecto y el impacto que este tendrá dentro de la organización (Los Libertadores, s.f.).

3.5 GERENCIA DE TECNOLOGÍA

Gerencia de Tecnología es la dependencia encargada de dirigir la planeación, la ejecución y el control de las actividades relacionadas con los equipos de comunicación y de cómputo, dispositivos móviles, aplicativos y sistemas de información, que prestan servicios, apoyan y soportan la información requerida por la Universidad en función de garantizar su operación, desarrollo y crecimiento (Los Libertadores, s.f.).

4. DISEÑO METODOLÓGICO Y PROPUESTA

4.1 TIPO DE INVESTIGACÓN

La investigación propuesta y que se acopla a necesidad planteada en el punto 1.1 Descripción del Problema, es la investigación descriptiva. Esta investigación permitirá realizar un estudio directo de los elementos tecnológicos que posee actualmente la red datos de la FULL, detallar la arquitectura implantada en la FULL y según los resultados obtenidos de dicha investigación tomar las decisiones del caso para iniciar con la construcción lógica de la DMZ.

4.2 FASES DEL PROYECTO

Teniendo en cuenta el tipo de investigación se realizaron las siguientes fases para el desarrollo del proyecto.

Levantamiento de la información.

- Entrevista.
- Conocimiento de la institución (Las respuestas de la entrevista).
- Políticas de seguridad.
- Para que funcionan las políticas en una entidad.
- Topología de red.

Análisis información.

- Análisis en los elementos de infraestructura.
- Análisis Políticas de seguridad.
- Análisis de la Topología de red.

Propuesta.

- Elementos a utilizar.
- Diagrama de red.
- Elementos a utilizar en la DMZ.
- Diagrama de DMZ.
- Consideraciones generales y aclaraciones de la propuesta.

4.3 LEVANTAMIENTO DE LA INFORMACIÓN

4.3.1 Entrevista

Se realizó una reunión entre las partes interesadas en la ejecución de este proyecto y se desarrolló de la siguiente manera.

Participantes:

Por parte de La Fundación Universitaria Los Libertadores.

Christian López (Oficial de Seguridad de la Información).

Julio Cesar Ramírez (Ingeniero de Redes y Comunicaciones).

Por parte de los estudiantes.

Andrés Felipe Sánchez Restrepo (Estudiante).

Brayan David Herrera Pinto (Estudiante).

Desarrollo de la entrevista

El desarrollo de la entrevista por parte de los estudiantes Andrés Felipe Sánchez Restrepo y Brayan David Herrera Pinto, con la coordinación del profesor Luis Eduardo Baquero Rey, se realizó el día 15 de junio del 2017 en el segundo piso de la sede Santander con el acompañamiento por parte del Oficial de seguridad Christian López, y el Ingeniero de Redes y Comunicaciones Julio Cesar Ramírez.

Durante el tiempo en el que se realizó dicha entrevista, se suministró información acerca de las redes, infraestructura y seguridad de la Fundación Universitaria Los Libertadores, en la cual se dejó detallado por parte de los ingenieros de la FULL será solo con fines académicos. Dicha información será analizada por parte de los estudiantes para la realización de un plan de mejoramiento de una Zona Desmilitarizada (DMZ). La presente entrevista se desarrolló clasificando cada uno de los partes encargados de la arquitectura, por esta razón se decidió entre las partes dividir en dos, infraestructura y seguridad.

Es importante aclarar que los ingenieros que participaron en esta entrevista manifestaron que existía información la cual no se podría tener acceso, así que por normas internas de la FULL el cuestionario aplicado tuvo que ser delimitado frente a las políticas de seguridad implementadas en la institución.

4.3.2 Conocimiento del Área

Estructura (Red Datos)

La universidad informó que a nivel estructural poseen las siguientes características:

- 2 canales. Un canal principal de 250Mb y un canal para Wi-fi de 50Mb.
- Dentro de (Multiprotocol Label Switchintg) MPLS son 7 sedes (Cartagena, sede H, Córdova, Nariño, Policarpa, bienestar y Santander). Conectadas a Santander están Bolívar, Ricaurte y Caldas.
- 7 sedes conectadas por MPLS y el resto por LAN.
- Topología en estrella MPLS y LAN. Wi-fi en estrella centralizado con una Controladora.
- Por cada Sede hay 6 vlans para cada segmento de red (Administrativo, académico, intervlan, voip, impresoras y Access point). Ver adjunto segmentación vlans.
- Por cada Sede hay 6 vlans para cada segmento de red (Administrativo, académico, intervlan, voip, impresoras y Access point).
- Cada segmento en DHCP tiene una máscara de 24 bits ampliable a 23. Varían entre 100 y 500 máquinas conectadas por cada segmento de red.
- 2 Firewall sonicwall: 1 firewall interno sonicwall 5500 y UN firewall externo sonicwall 6600.
- 2 redes (Administrativa y académica), cada una con un. witch core cisco 3750G, 60 switches conforman la capa de acceso y distribución, equipos cisco en su mayoría.
- 100 servidores entre físicos y virtuales aproximadamente. En su mayoría son máquinas virtuales.
- Página web, correo, servicios administrativos (Iceberg, Aire, portal del trabajador, entre otros). Bases de datos, servidores de acceso. (Ver adjunto listados servidores y servicios).
- Ya que esta información es muy grande se tiene la necesidad de realizar una codificación. (Ver adjunto listados servidores y servicios).
- 20 máquinas dentro de la DMZ.

- Los servidores en su mayoría son virtuales y los ubicados en la DMZ se encuentran en un único segmento de red.

Muchos de los datos recolectados se pueden verificar en los anexos 2,3 y 4, ya que corresponden a los gráficos informados por la Fundación Universitaria Los Libertadores.

Seguridad

La universidad informó que a nivel estructural poseen las siguientes

- En la política hace referencia a los procedimientos.
- Control de accesos.
- Política de seguridad de la información que actualmente está en construcción.
- El procedimiento ya se encuentra construido y en etapa de divulgación.
- Estos registros se deberían quedar en los incidentes de seguridad, Ya se creó un procedimiento que se llama incidentes de seguridad, se encuentra en etapa de divulgación.
- Nivel externo el firewall.
- Nivel interno otro firewall.
- Endpoint con sus reglas firewall Windows.
- La fundación está creando su matriz de activos, para los procesos más críticos para el consejo, con esto se crea la matriz de riesgos para los activos y de esto salen sus controles inherentes.

Por motivos de políticas de seguridad de la información, muchas preguntas formuladas, que se encuentran en el Anexo 2, no fue posible obtener una respuesta ya que se puede incurrir en un incidente de seguridad, por esta razón no es posible contestar dichas pregustas.

4.3.3 Políticas de seguridad

Hoy en día hablar de seguridad en los sistemas de información es tan sencillo como hablar de inversión tecnológica y para esto es necesario que toda entidad que requiere

de seguridad en la información deba conocer los riesgos que pueden presentarse en su operación y así mitigarlos a través de normas que se apliquen en toda la organización.

Una solución recomendada es limitar todo el espectro de seguridad que rodea a la entidad en lo que hace, a plataformas, procedimientos y estrategias, de manera que se pueda controlar un conjunto de vulnerabilidades que, aunque no logran la seguridad total significa que se tendrán cubiertas las principales vulnerabilidades a través de documentos, directrices y recomendaciones que orientan el uso adecuado de las nuevas tecnologías.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, no es posible dar documentos estableciendo que hacer para lograr mayor seguridad informática, pero si se pueden proponer lineamientos generales que se deben seguir parar lograr documentos con estas características.

Para continuar se definirán algunos conceptos aplicados en la definición de un PSI:

Decisión: elección de un curso de acción determinado entre varios posibles.

Plan: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.

Política: definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Meta: objetivo cuantificado a valores predeterminados.

Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Norma: forma en que realiza un procedimiento o proceso.

Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronóstico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé e influirán en los acontecimientos futuros.

Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.

Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso.

Ahora, "una política de seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que esta y que no está permitido en el área de seguridad durante la operación general del sistema" UERTA, Antonio Villalón. Seguridad en Unix y redes.

Es muy importante aclarar que cada uno de los procesos establecidos requiere tener una definición drástica en el ítem implementado dentro de la política, para ellos existen diversas formas de implementar políticas dentro de un sistema red.

Dentro de todas las temas abordados y especificados que componen la red, existen procesos de seguridad que deben tener cierto control para lo cual de manera muy activa, deben tener esquemas severos a nivel cultural, es decir que con una buena implementación y aplicación de la política al proceso seleccionado se podrá tener un control total en cada uno de los elementos que componen el proceso. Una de estas mejores guías o prácticas la podremos encontrar en la siguiente dirección web (URL) https://www.sans.org/security-resources/policies/network-security, donde podremos encontrar documentación concreta de cómo realizar la implementación de una política enfocada a la seguridad de la información y el control de los elementos tecnológicos que la componen.

4.3.4 Análisis web del hosting

La extensión netcraft 1.11.3 se encuentra disponible para los navegadores Google Chrome y Mozilla Firefox, la cual no proporciona datos de las páginas web que son consultadas.

Los siguientes análisis se realizaron bajo la aplicación web netcraft, las cual nos proporciona datos tales como:

Site title	Fundación Universitaria Los Libertadores - Institución Universitaria	**Date first seen**	August 1998
Site rank	178837	**Primary language**	Spanish
Description	Formaci\303\263n de excelentes profesionales, ciudadanos y personas, el lugar donde tus sue\303\261os y metas se hacen realidad | Fundaci\303\263n Universitaria Los Libertadores		
Keywords	*Not Present*		

Obtenida de netcraft.com, 12 de diciembre 2017.

Datos de la primera visita, lenguaje principal usado, rango del sitio, título del sitio, palabras cables del sitio, fecha de apertura de la página web desde su primera visita.

Site	http://www.ulibertadores.edu.co	**Netblock Owner**	COLUMBUS NETWORKS COLOMBIA
Domain	ulibertadores.edu.co	**Nameserver**	ricaute.libertadores.edu.co
IP address	190.242.99.231	**DNS admin**	root@libertadores.edu.co
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	nic.co	**Nameserver organisation**	whois.nic.co
Organisation	*unknown*	**Hosting company**	Liberty Global
Top Level Domain	Colombia (.edu.co)	**DNS Security Extensions**	*unknown*
Hosting country	CO		

Obtenida de netcraft.com, 12 de diciembre 2017.

Datos del sitio tales como nombre de domino, IP, datos de la organización, país del hosting, DNS admin, nameserver.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
COLUMBUS NETWORKS COLOMBIA Bogota	190.242.99.231	-	Apache	23-Mar-2017
Columbus Networks de Colombia Limitada Bogota	190.242.99.231	Linux	Apache	23-Mar-2017
COLUMBUS NETWORKS COLOMBIA Bogota	190.242.99.231	Linux	Apache/2.2.22 Debian	28-Oct-2015
Columbus Networks de Colombia Limitada Bogota	190.242.99.231	Linux	Apache/2.2.9 Debian PHP/5.2.6-1lenny8 with Suhosin-Patch	16-May-2015
Telmex Colombia S.A. Bogota	200.26.152.210	Linux	Apache/2.2.9 Debian PHP/5.2.6-1lenny8 with Suhosin-Patch	12-Mar-2011
Telmex Colombia S.A. Bogota	200.26.152.210	Linux	Apache/2.0.50 Unix mod_ssl/2.0.50 OpenSSL/0.9.8 Zend Core/1 PHP/5.1.4	16-Jul-2010
Telmex Colombia S.A. Bogota	200.26.152.210	Linux	Apache/2.2.3 Debian PHP/5.2.0-8etch15	6-Jun-2009
Telmex Colombia S.A. Bogota	200.26.152.210	Linux	Apache/2.0.50 Unix mod_ssl/2.0.50 OpenSSL/0.9.8 Zend Core/1 PHP/5.1.4	2-Jun-2009
Telmex Colombia S.A. Bogota	200.26.152.210	Linux	Apache/2.0.52 CentOS	13-Feb-2008
Diveo de Colombia Ltda Bogota	200.31.79.210	Windows Server 2003	Lotus-Domino	12-Jun-2006

Obtenida de netcraft.com, 12 de diciembre 2017.

Se observan datos históricos del hosting, última ves vistos, nombre del servidor, sistema operativo (OS), dirección IP de los mismos.

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

Obtenida de netcraft.com, 12 de diciembre 2017.

Los SPF son registros de un host que describe quien puede enviar un correo en su nombre bajo una serie de reglas, la configuracion de un registro SPF ayuda a evitar la entrega de correos electronicos falsificados en su dominio se recomienda implentar este tipo de registros en los servidores.

Obtenida gfx.robtex.com, 12 de diciembre 2017.

Se obtienen graficos del protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia informacion entre sistemas autonomos.

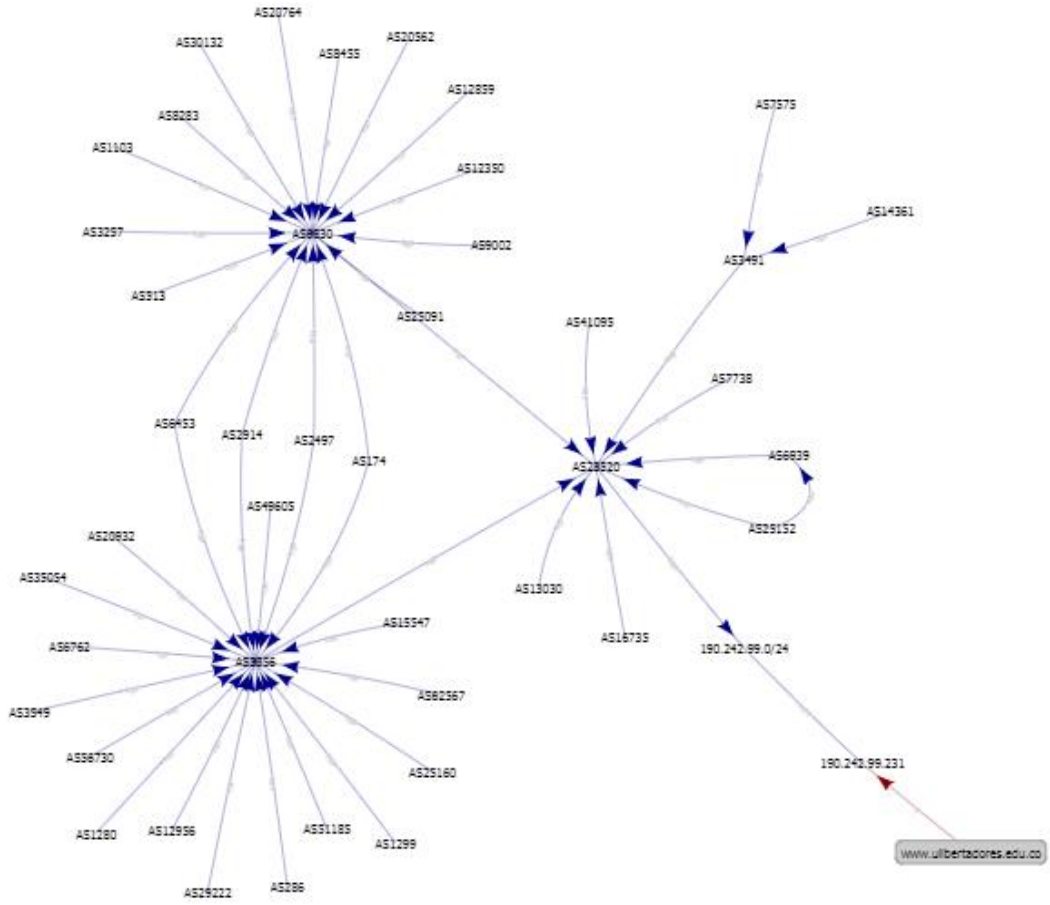
INDEXED PAGES

Title and URL	Domains	Backlinks
...:::Fundación Universitaria Los Libertadores:::... http://www.ulibertadores.edu.co/	99	1,200
Fundación Universitaria Los Libertadores - Valores de Matrícula http://www.ulibertadores.edu.co/index.php/admisiones/valores	2	56
Fundación Universitaria Los Libertadores - Uso de Datos Personales http://www.ulibertadores.edu.co/index.php/uso-de-datos-perso...	2	56
Biblioteca - Universidad los Libertadores http://www.ulibertadores.edu.co:8089/index.php?idcategoria=3...	3	54
Fundación Universitaria Los Libertadores - Proceso de Inscripción Programas Presenciales http://www.ulibertadores.edu.co/index.php/admisiones/proceso...	2	42

Export View full report

Obtenida www.semrush.com, 12 de diciembre 2017.

Autómata de intercambio de información de la red de datos de la FULL.

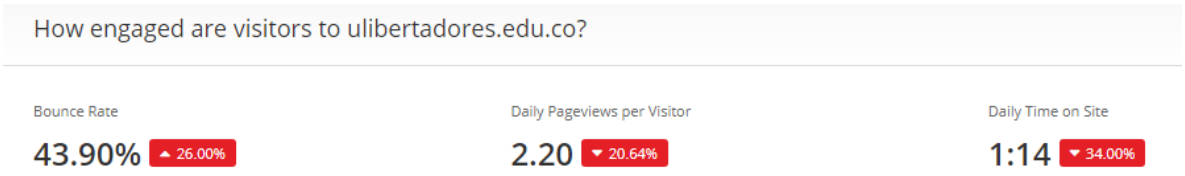


Obtenida www.semrush.com, 12 de diciembre 2017.

Se puede encontrar las paginas idexadas de la pagina web de la universidad, tanto en el dominio como en links externos.

Obtenida www.alexa.com, 12 de diciembre 2017.

En algunas páginas web se obtiene información de que tan popular es la página, que tan visitada es la página web de la universidad, para así medir que tan productivos son los servicios que ofrecen.



Obtenida www.alexa.com, 12 de diciembre 2017.

Se puede observar el tiempo promedio que pasan los usuarios en la página, el número de visitas diarias y su respectivo proveedor de internet.

Obtenida www.alexa.com, 12 de diciembre 2017.

4.4 ANALISIS DE LA INFORMACIÓN

4.4.1 Análisis de los elementos tecnológicos.

Servidores

Después de computar la información recolectada a través de la entrevista se realizó la clasificación de los datos, los cuales se detalla a continuación:

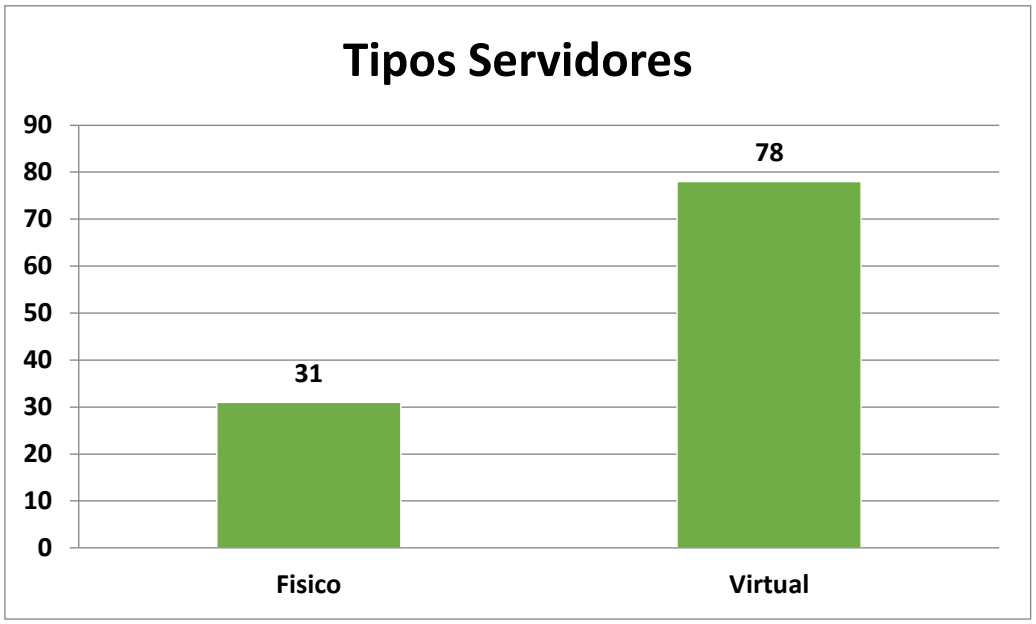


Tabla 2. Tipos de servidores

Conclusiones

A. Se observa que existe un manejo de maquinar virtuales, mayor a las maquinas físicas.

b. este gráfico demuestra que existe un manejo de configuraciones lógicas de servicios tecnológicos y servicios de almacenamiento.

Grupos Red

A continuación, se detalla la cantidad de grupos que se encuentran en la red.

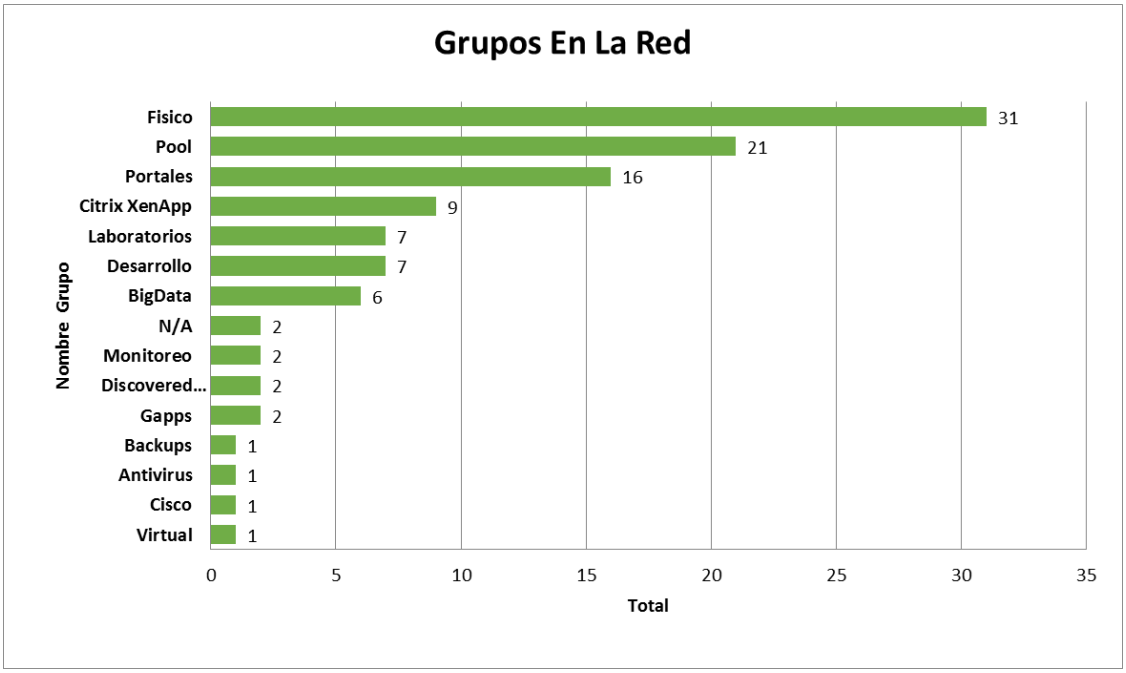


Tabla 3. Grupos En la red

Conclusiones

A. Existen 15 grupos de trabajo que conforman la red.

b. La distribución no está dada con un orden específico, por lo contrario, está basada en la necesidad a suplir.

c. Se demuestra cuantos servicios están configurando en cada uno de los grupos.

Cantidad Sistemas Operativos

El siguiente gráfico detalla la cantidad de sistemas operativos que están siendo utilizados en la actualidad.

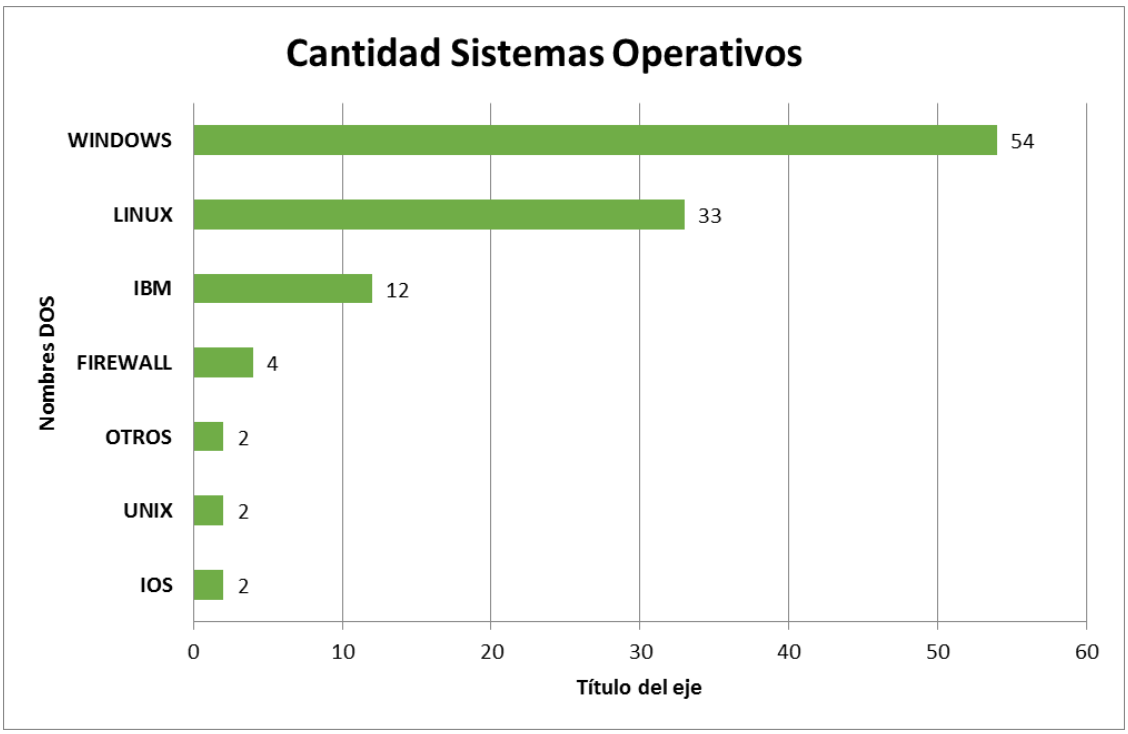


Tabla 4. Cantidad Sistemas operativos

Conclusiones

A. Se Utiliza diversos sistemas operativos para el funcionamiento de la red.

b. Poseen diversos sistemas operativos de código abierto y otros licenciados.

c. Ofrecen servicios internos a través de software y hardware personalizado, tales como los de IBM y los Firewall.

d. El 49 % de los servidores que componen la red son Windows, el otro 51 % están conformados con software de código abierto.

Servidores Windows

A continuación, se detallan la cantidad de servidores que poseen este software:

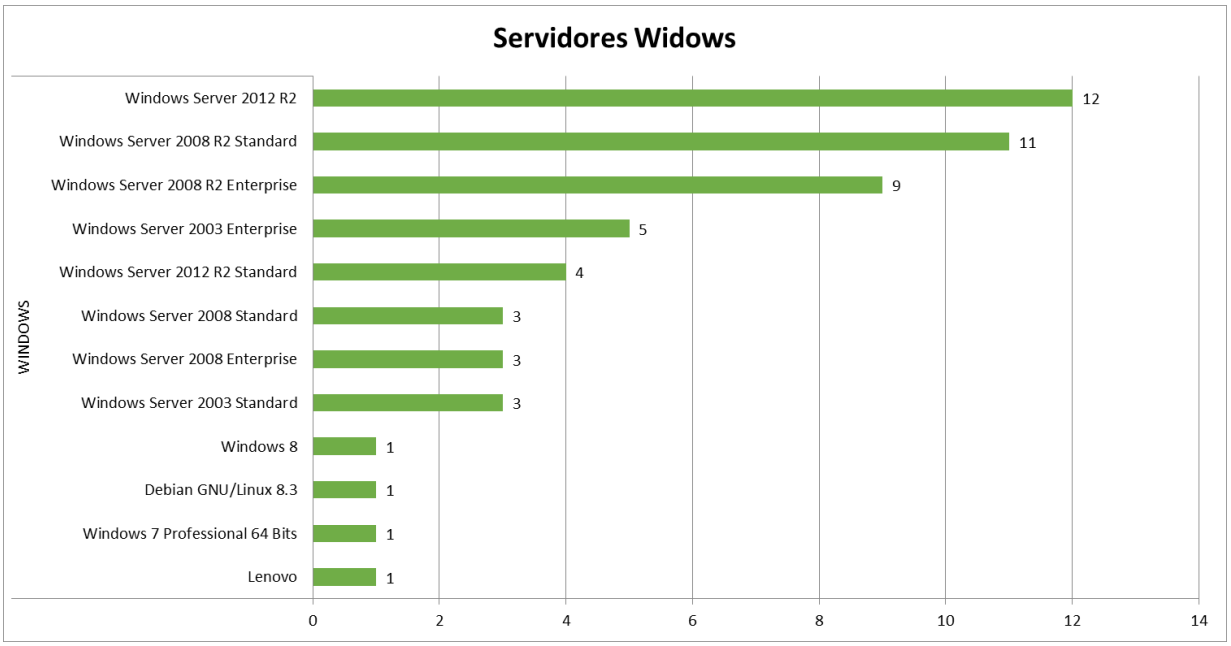


Tabla 5. Servidores Windows

Conclusiones

A. Manejan diferentes versiones de Windows para la administración de servidores.

b. Poseen un software directamente proporcionado con la configuración que requiere el hardware de Lenovo.

c. Manejan diferentes versiones en los servidores y por esta razón pueden presentar incompatibilidad en algunas funcionalidades.

e. El costo de manteamiento en cada uno de este software es alto a comparación de otro software.

Servidores Linux

A continuación, se detallan la cantidad de servidores que poseen este software:

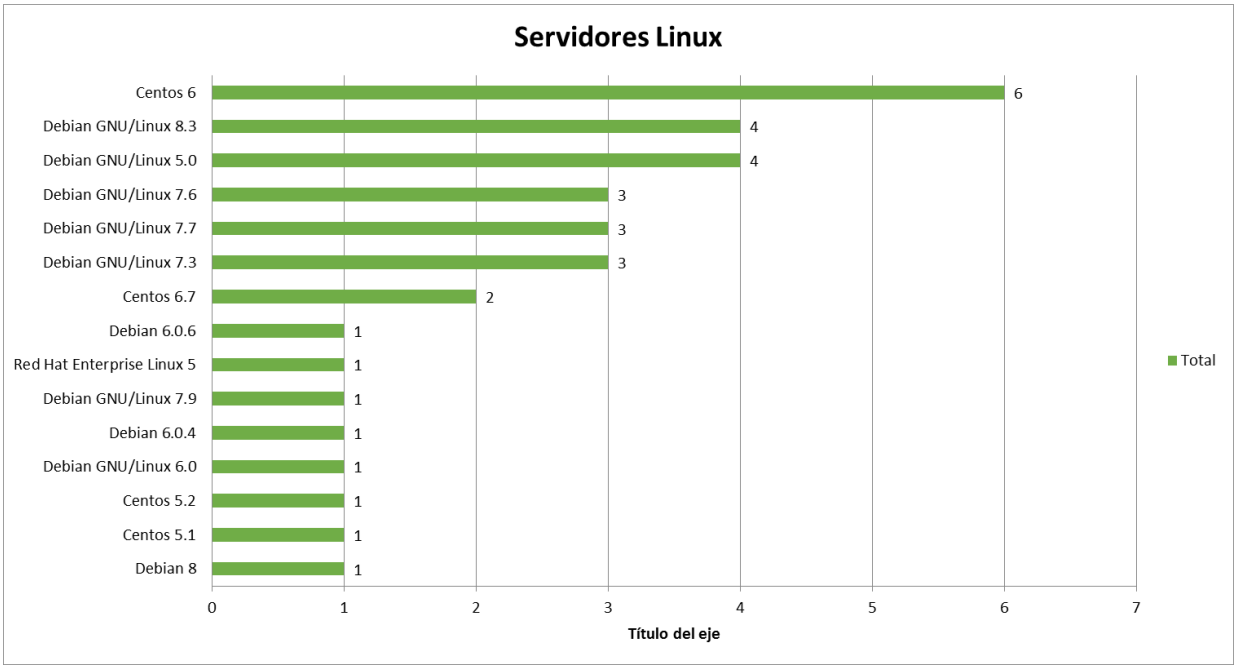


Tabla 6. Servidores Linux

Conclusiones

a. Manejan diferentes versiones y de extensiones del sistema operativo Linux para la administración de servidores.

c. Manejan diferentes versiones en los servidores y por esta razón pueden presentar incompatibilidad en algunas funcionalidades.

e. El costo de manteamiento en cada uno de este tipo software es bajo a comparación del otro software (Windows).

Servidores IBM

A continuación, se detallan la cantidad de servidores que poseen este software:

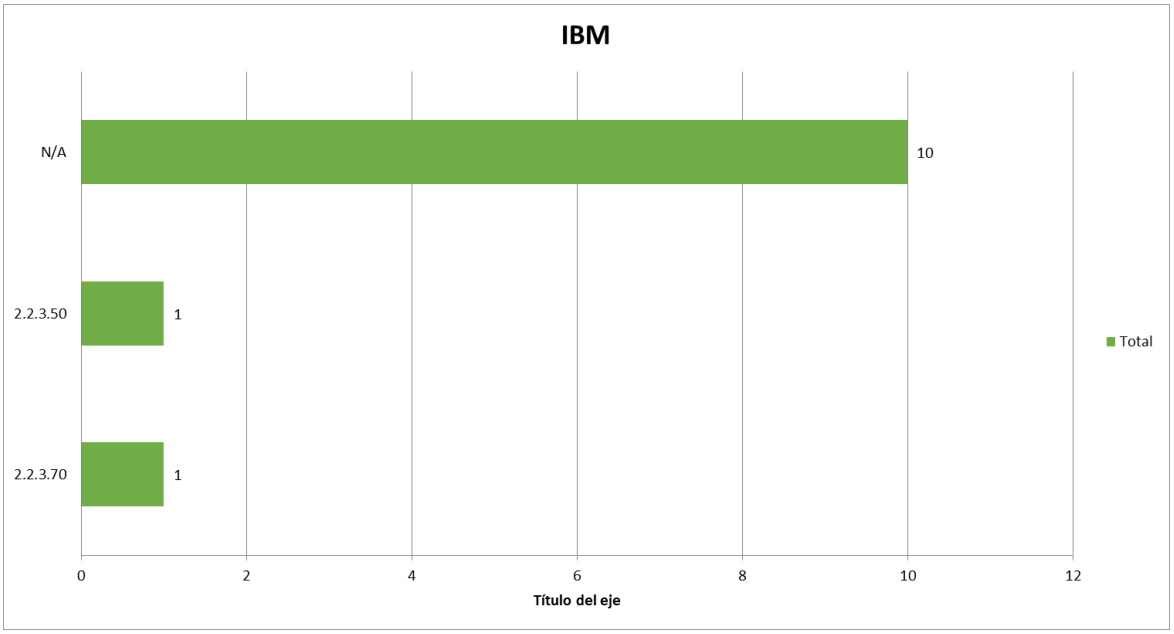


Tabla 7: Servidores IBM

Conclusiones

a. Manejan diferentes versiones del software administrable que ofrece IBM.

b. Manejan diferentes versiones en los servidores y por esta razón pueden presentar incompatibilidad en algunas funcionalidades.

c. El costo de manteamiento en cada uno de este tipo software es alto a comparación del otro software (Windows - Linux).

4.5 SISTEMA DE INFORMACIÓN

Actualmente La institución cuenta con sistemas de información eficaces, que proveen a estudiantes, docentes y administrativo, datos para el registro, consulta administración de información.

Estos sistemas de información facilitan la interacción administrativa entre los estudiantes, los profesores y los diferentes actores administrativos de la institución. Para el registro de información de manera interna y externa se encuentran:

SISTEMA DE INFORMACION ACADEMICA	INTERACCIÓN
ULISES- sistema de información para estudiantes	Los estudiantes pueden hacer uso del módulo para su proceso de matrícula, registro de materias, consulta de horarios y notas parciales y finales, impresión del historial académico entre otros trámites, sin necesidad de desplazarse hasta la institución. El acceso a Ulises se realiza con el usuario y clave asignada en el correo electrónico.
SIRENA- Modulo de acceso de profesores para el cargue de notas	Los profesores tienen acceso al registro de calificaciones de los estudiantes. Los profesores pueden consultar la lista de estudiantes por grupos, ubicación de los salones, registrar ausencias, entre otras.
AYRE- Sistema de admisiones, control y registro	Este es un sistema de gestión e información académica de estudiantes. La coordinación académica puede realizar matriculas, homologaciones, reporte de notas, proceso de verificación de grados, revisión de historias académicas del estudiante, procesos de admisión de estudiantes nuevos y transferencias.
SIPA- Sistema de programación académica	En este sistema se programan los grupos del semestre por parte de la coordinación académica, se asigna carga académica de los docentes, y se pueden consultar asignaciones de aulas.
DISCOVERER- Sistema administrativo y financiero académico	La coordinación académica tiene acceso a la información de los procesos administrativos de los estudiantes, como número de matrículas por programa en semestre académico, cancelación de materias, aplazamientos de semestre entre otros.
SAT- Plan de acompañamiento a estudiantes	Sistemas de permanencia y graduación oportuna.
ADVISOR	Alertas tempranas (programa PYGO)

Grafico 3. Sistemas de información Académicos

A continuación, se describen los sistemas de información del área administrativa:

SISTEMA DE INFORMACION ADMINISTRATIVA	INTERACCIÓN
KAIROS-	Es un sistema que permite la gestión documental.
ICEBERG-	Es un sistema que permite la gestión financiera.
SIRIA- Sistema de información para reserva academica	Es un sistema de información para reserva informática académica.
SEVENET- Sistema de información documental institucional	Es un sistema que permite la gestión documental y de captura de encuestas.
DOTPROJECT	Este es un software categoría OPEN RP basado en web, multiusuario, multiidioma. Esta construido por aplicaciones de código abierto y es mantenida por un pequeño pero dedicado grupo de personas, se utiliza en la institución para registrar y monitorear los planes de mejora.
SIA- Sistema integrado académico	Este sistema establece los mecanismos de control y verificación académica de los estudiantes y docentes
ISOLUCION	En este sistema se registra y administra la información conducente al cumplimiento de los procesos de calidad ISO9001:2008.

Grafico 4. Sistemas Información Administrativos

4.6 ANÁLISIS POLÍTICA DE SEGURIDAD

Procedimiento de Gestión de Incidencia

A continuación, se detalla cómo se realiza la gestión una incidencia en la FULL.

A. Un estudiante o colaborador administrativo reporta una incidencia realizando un ticket por la herramienta de help desk.

B. El coordinador comunica al oficial de seguridad y al personal pertinente, la persona encargada realiza el apoyo a quien reporto la incidencia y documenta minuciosamente lo ocurrido en la solución de esta.

C. Basado en la documentación de la incidencia el personal pertinente evalúa el impacto que puede tener en la operación de las áreas afectadas y el número de personas involucradas.

D. Si en el trascurso de la evaluación se indica que no es incidencia con un impacto real se notifica el resultado en la mesa de ayuda, de lo contrario se asocia la incidencia dependiendo su impacto (Bajo, Medio, Alto).

E. Si la incidencia tiene un impacto real se determina si es necesario contactar con un proveedor o un especialista dentro de la Fundación, en caso de que se considere la incidencia de alto impacto, el Gerente de tecnología involucrara el personal que el caso requiera para su solución.

F. Para dar solución a la incidencia se ejecutan dos tareas:

- Contención: busca que el incidente no se propague y genere más daños a la información a la arquitectura de TI de la Fundación.

- Recuperación: eliminación de cualquier rastro dejado por el incidente.

G. El oficial de seguridad documenta las causas, vulnerabilidades y violaciones encontradas, las contingencias de contención y recuperación implementadas, y los resultados del seguimiento de la incidencia.

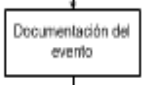
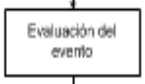
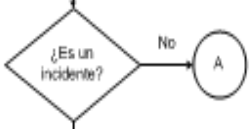
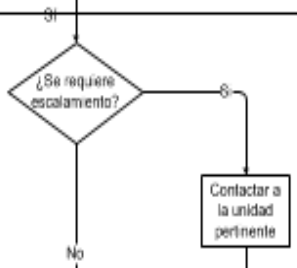
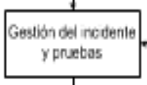
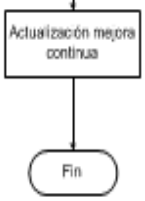
H. El oficial de seguridad actualiza la bitácora de buenas prácticas de seguridad de la información con base en los hallazgos, controles y resultados obtenidos durante el tratamiento de la incidencia.

Conclusiones

- Se detallan los roles de responsabilidad en las distintas etapas de la gestión de la incidencia.
- Se registran (nombres del documento y formatos).
- Se detallan herramientas utilizadas para el desarrollo de la incidencia.

Gráfico 5. Procedimiento de Gestión de Incidencia

5. DESCRIPCIÓN DEL PROCEDIMIENTO

	ACTIVIDAD (Nombre de Actividad en Flujograma)	RESPONSABLE (Cargo del Responsable de la Actividad)	DESCRIPCIÓN DE ACTIVIDAD	REGISTRO (Nombre del Documento, formato o registro)
1		Colaborador o estudiante de La Fundación	Un estudiante o un Colaborador de La Fundación reporta el incidente abriendo un ticket en la herramienta de Gestión de Help Desk	Herramienta de gestión de Help Desk
2		Colaborador o estudiante de La Fundación Coordinador de Servicios Departamento de Tecnología Oficial Seguridad de la información	El Coordinador de servicios comunica al Oficial de Seguridad de la información (y al personal pertinente) la situación que se presentó. El Oficial de Seguridad y el personal pertinente realizan la investigación del incidente ocurrido apoyado en quien reportó el evento. Todas las novedades se documentan minuciosamente	Herramienta de gestión de Help Desk
3		Oficial de Seguridad de la información	Basado en la documentación obtenida en la tarea anterior, el Oficial de Seguridad y el personal pertinente evalúan el incidente en términos del impacto que puede tener en la operación de las áreas afectadas y el número de personas involucradas.	Herramienta de gestión de Help Desk Formato de atención de incidentes de seguridad
4		Oficial de Seguridad de la información	Si la evaluación indica que no es un incidente real, se notifica el resultado en la herramienta de gestión de Help Desk. Si se comprueba que el evento ocurrido sí es un incidente, se evalúa el impacto asociado (Bajo, Medio, Alto)	Herramienta de gestión de Help Desk
5		Oficial de Seguridad de la información	Si es el evento ocurrido es un incidente, el Oficial evalúa el impacto asociado. Según su resultado, el Oficial determina si es necesario contactar a un equipo especializado dentro de La Fundación, a un proveedor o una entidad especializada en delitos informáticos para su solución o incluso para la investigación previa. En caso de no ser así, él lo resolverá con el personal de la Fundación que crea conveniente En caso que el incidente sea considerado de alto impacto, se debe comunicar al Gerente de Tecnología quien involucrará a otras personas si el caso lo requiere.	Herramienta de gestión de Help Desk
6			Para dar solución al incidente, se ejecutan dos tareas: - Contención: Busca que el incidente no se propague y pueda generar más daños a la información o a la arquitectura de TI de La Fundación. - Recuperación: Eliminación de cualquier rastro dejado por el incidente (Ej.: código malicioso) y posteriormente se procede a la recuperación a través de la restauración de los sistemas	
7		Usuario Oficial de Seguridad de la información	El Oficial de Seguridad de la Información documenta las causas, vulnerabilidades, violaciones encontradas, las estrategias de contención y recuperación implementadas y sus resultados en la Herramienta de gestión de Help Desk. Se cierra el ticket.	Herramienta de gestión de Help Desk
8		Oficial de Seguridad de la información	El Oficial de Seguridad actualiza la bitácora de buenas prácticas de seguridad de la información con base en los hallazgos, controles y resultados obtenidos durante todo el tratamiento del incidente.	Bitácora de buenas prácticas de seguridad de la información

Gestión de Acceso de Usuarios

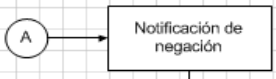
A continuación, se detalla cómo se realiza la Gestión de acceso de usuarios en la FULL.

Conclusiones

a. Se detallan los tipos de acceso
    - Estudiante: Asigna acceso al correo electrónico, a Ulises (modulo portal estudiantil), a la biblioteca, a las bases de datos electrónicas de consulta y a Blackboard (aulas virtuales)
    - Empleado administrativo o docente: asigna acceso a aplicaciones para desarrollar su cargo
b. Se detallan los roles de responsabilidad en las distintas etapas de la gestión de acceso de usuarios
c. Se registran (nombres del documento y formatos)
d. Se detallan herramientas utilizadas para el desarrollo del acceso de usuarios

Gráfico 6. Gestión de Acceso

	ACTIVIDAD (Nombre de Actividad en Flujograma)	RESPONSABLE (Cargo del Responsable de la Actividad)	DESCRIPCIÓN DE ACTIVIDAD
1	Inicio		
2	Generar estado de matriculado o empleado activo	Analista de Tesorería Profesional Talento Humano	• Estudiante: El analista de Tesorería le asigna estado matriculado al estudiante en el Sistema de Información Académico (SAI) cuando éste haya realizado el pago de su matrícula. Se remite la novedad a la Dirección de Admisiones y Registro. • Docente o empleado: el profesional de Talento Humano realiza la vinculación, creando ticket en la herramienta de gestión de Help Desk para la creación de la cuenta del usuario indicando en el Formato la asignación de usuarios y acceso a Sistemas de Información los recursos y permisos respectivos.
3	Abrir ticket para crear solicitud	Profesional Admisiones y Registro Profesional Talento Humano	En el caso de estudiantes, el profesional de Admisiones y Registro abre un ticket en la herramienta de gestión de Help Desk adjuntando el Formato de asignación de usuarios y acceso a Sistemas de Información. Si es un empleado, el profesional de Talento Humano abre el ticket con el formato anteriormente mencionado
4	Si ¿Es contratista? No		Si se requiere asignar correo electrónico o acceso a una aplicación para un contratista, el supervisor del contrato debe notificar dicha novedad al profesional de Talento Humano quien lo informará en el ticket generado en el paso anterior.
5	Validar ticket para aprobación para asignar usuario	Coordinador técnico y de servicios	El ticket le llega al Coordinador técnico y de servicios quien consultará al Gerente del área al que ingresaría al contratista los permisos que necesitaría.
6	Sí ¿Aprobado? No A	Coordinador técnico y de servicios	Basado en la consulta del paso anterior, el Coordinador técnico y de servicios consultará al Gerente del área al que pertenecería el contratista si la solicitud es aprobada o rechazada.
7	Asignación del ticket a Ingeniero encargado	Coordinador técnico y de servicios	El coordinador técnico y de servicios escala el ticket al ingeniero responsable del recurso involucrado.
8	Sí ¿La cuenta del usuario ya existía? No	Ingeniero de sistema de información Ingeniero Plataforma	Validación por parte del Ingeniero responsable del recurso (Directorio Activo, Blackboard, acceso a Ulises para estudiantes, acceso a Sirena para profesores, acceso a Iceberg para funcionarios del área financiera, etc.) para comprobar si la cuenta del usuario ya existía.
9	Se reactiva el usuario con el rol solicitado B	Ingeniero de sistema de información Ingeniero Plataforma	Si la cuenta de usuario ya existía en algún recurso, el ingeniero responsable del sistema de información o de la respectiva plataforma, reactivará la cuenta del usuario con los roles especificados en el ticket.
10	Crear usuario en el Directorio Activo y aplicaciones	Ingeniero de plataforma Ingeniero Sistema de información Ingeniero de plataforma	Se crea la cuenta del usuario basado en las indicaciones dadas en el ticket registrado cumpliendo con los respectivos SLAs. La creación del usuario según su rol viene dado de la siguiente forma: • Estudiante: Asigna acceso al correo electrónico, a Ulises (módulo portal estudiantil), a la biblioteca, a las bases de datos electrónicas de consulta y a Blackboard (aulas virtuales). • Empleado administrativo o Docente: Asigna acceso a aplicaciones para desempeñar su cargo
11	B Validaciones en la plataforma	Ingeniero de sistema de información Ingeniero Plataforma	Los ingenieros responsables de la plataforma y de los sistema de información validan que las cuentas creadas tengan los accesos y permisos correspondientes. Se copia pantallazo en el ticket de servicio.

12		Coordinador técnico y de servicios	En el caso de un empleado o un contratista, las contraseñas de los sistemas de información se enviarán al correo electrónico de la persona mencionada anteriormente. Para su acceso, se manejará una contraseña estándar y el ingeniero responsable de la capacitación de Tecnología solicitará a cada empleado el cambio inmediato de la contraseña. En el caso de los estudiantes, las contraseñas de los sistemas de información que utilizarán se enviarán al correo personal de cada uno de ellos solicitándoles que el cambio es obligatorio he inmediato. Finalmente, con el envío de las contraseñas al correo personal, se cerrará el ticket.
13		Ingeniero de sistema de información Ingeniero Plataforma	En caso que la solicitud de acceso a algún recurso tecnológico sea denegado a un contratista, el ingeniero responsable de dicho recurso, le notificará al Gerente del área la negación de la solicitud y su justificación.
14		Ingeniero de sistema de información Ingeniero Plataforma Coordinador técnico y de servicios	En el caso de los empleados, después de la capacitación y de hacer la validación de que todos los aplicativos funcionan apropiadamente, se cerrará el ticket. En el caso de los estudiantes, el ticket se cierra con el envío de la contraseña a la cuenta de correo personal del estudiante.
15			

4.6.1 Análisis de la Topología de red

Tal como se comunicó durante el levantamiento de la información que se presentó, durante la aplicación de la entrevista, se encontró que muchos de los elementos tales como Firewall y Switch son de alta calidad y están a la vanguardia a nivel de las comunicaciones por ende no es necesario implementar un cambio drástico con dichos elementos.

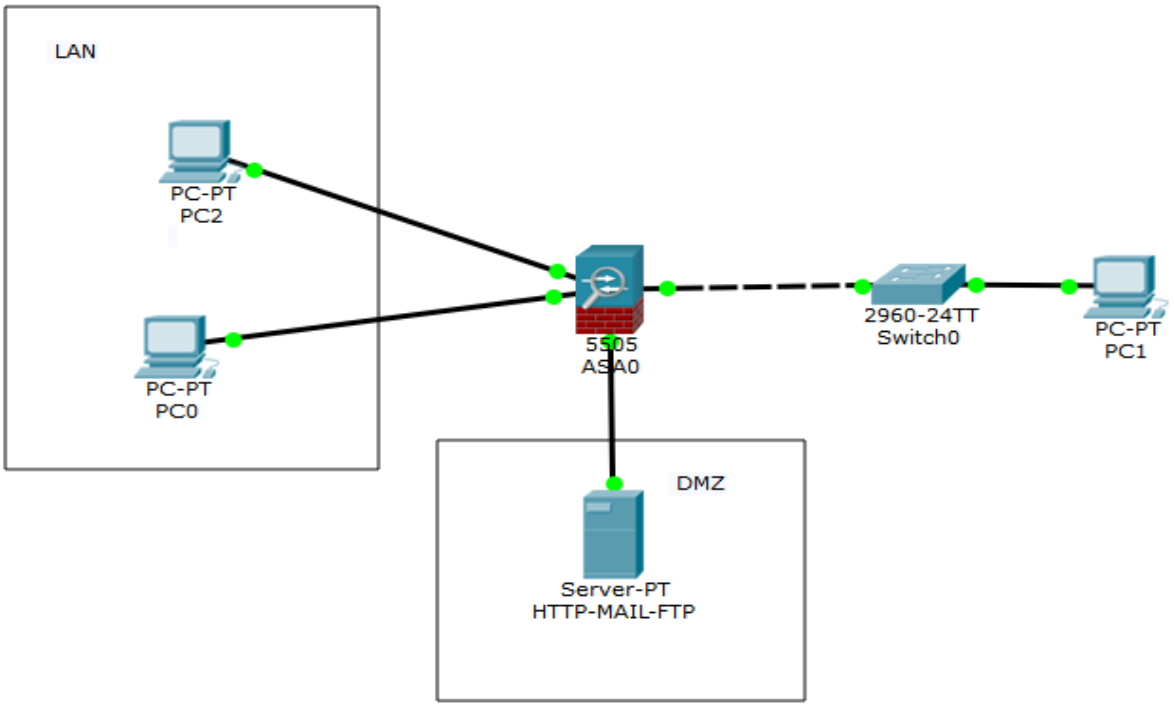
Pero si se evalúa la topología encontramos las siguientes falencias:

- Una falencia que se encontró fue las comunicaciones entre algunas de las sedes, ya que la distancia es muy larga y debe tener conectividad por medio de fibra óptica.
- La siguiente falencia que se encontró es que en algunos canales de comunicación no existía la presencia de un Firewall que permitirá la filtración de tráfico entrante a las diferentes sedes.
- Los elementos que constituían la DMZ no tenían ningún filtrado de paquetes antes de conectarse a los diferentes canales de comunicación.

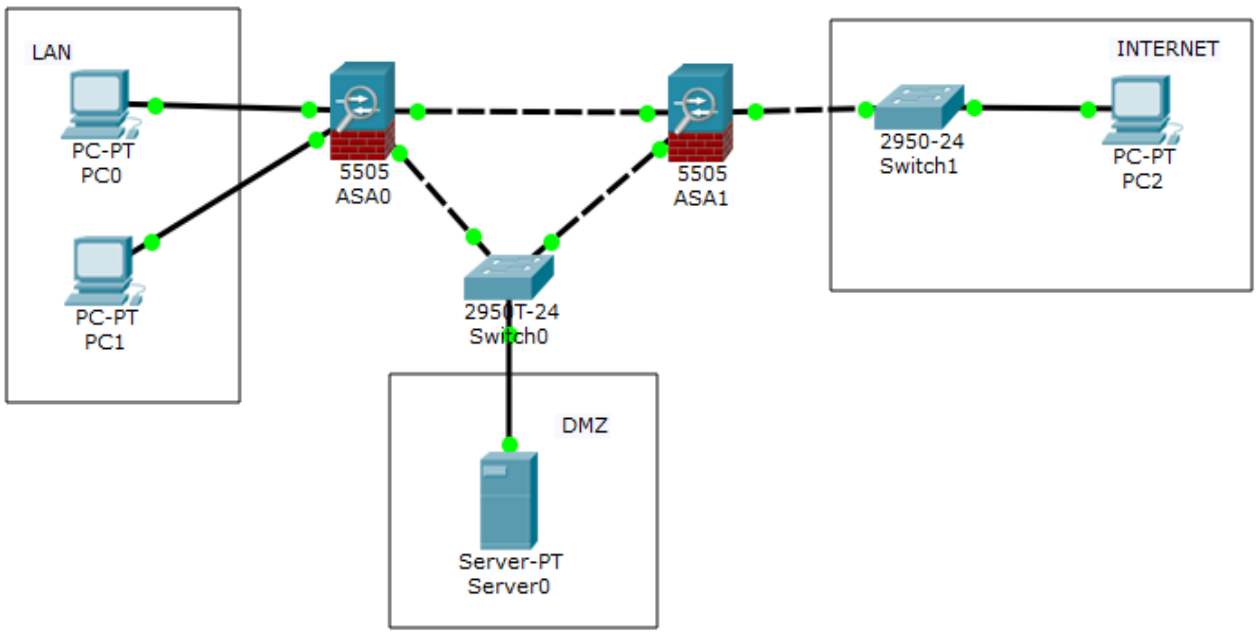
Las descripciones de cada uno de los elementos las pueden validar en el diagrama que se encuentra en el Anexo 3 y que describe la topología actual que posee la fundación universitaria los libertadores.

4.7 SIMULACIÓN

Durante el siguiente punto se demostrará la simulación de cada uno de los esquemas de red que contiene la una DMZ.

<table>
<tr><td colspan="2">Simulación 1</td></tr>
<tr><td colspan="2">Procedimiento realizado</td></tr>
<tr><td colspan="2">En la siguiente simulación se quiere comprobar el intercambio de paquetes en una topología de red, la cual se compone por elementos que estarán intercambiando información con una zona desmilitarizada. El principal objetico de esta simulación es corroborar que los elementos sean compatibles y tenga la correcta configuración dentro del esquema de red.</td></tr>
<tr><td colspan="2">Elementos a utilizar</td></tr>
<tr><td>Software</td><td>Packet Tracer 7.0</td></tr>
<tr><td>Cables</td><td>UPT: Cruzado - Directo</td></tr>
<tr><td>PC</td><td>Tarjeta de red Basica</td></tr>
<tr><td>Hardware</td><td>Switch capa 3 - Firewall ASA 5505 - Servidor</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Diseño Final</td></tr>
<tr><td colspan="2"> 
</td></tr>
</table>

Simulación 2	
Procedimiento realizado	
En la siguiente simulación se quiere comprobar el intercambio de paquetes en una topología de red, la cual se compone por los elementos fundamentales como los Firewall ASA 5505 los cuales permite realizar una configuración de la red en puente la cuan hace que la re posea una configuración de alta disponibilidad y así permita un buen funcionamiento dela misma.	
Elementos a utilizar	
Software	Packet Tracer 7.0
Cables	UPT: Cruzado - Directo
PC	Tarjeta de red Basica
Hardware	(2) Switch capa 3 - (2)Firewall ASA 5505 - Servidor
Diseño Final	



4.7.1 Resultados Obtenidos

Simulación 1

Al realizar esta configuración se pudo evidenciar que cuando el firewall falla la red LAN queda sin acceso a Internet o expuesta a la Internet y ocasionando que los servicios de la DMZ queden también sin conexión alguna. En este tipo de DMZ el firewall supervisa todos los puertos por separado, lo que lo convierte en el punto único de fallo.

Simulación 2

Realizando esta topografía de red de datos con 2 firewall, y simulando una indisponibilidad de un firewall el otro seguirá en funcionamiento, brindando continuidad en la red datos, a si se proporcionara continuidad en los servicios ofrecidos. Esta arquitectura de seguridad en dos etapas hace posible la configuración de rutas estáticas que regulan el tráfico entre las redes, brindando una alta disponibilidad en los servicios ofrecidos.

5. PROPUESTA DE LA DMZ

5.1 DIAGRAMA DE RED

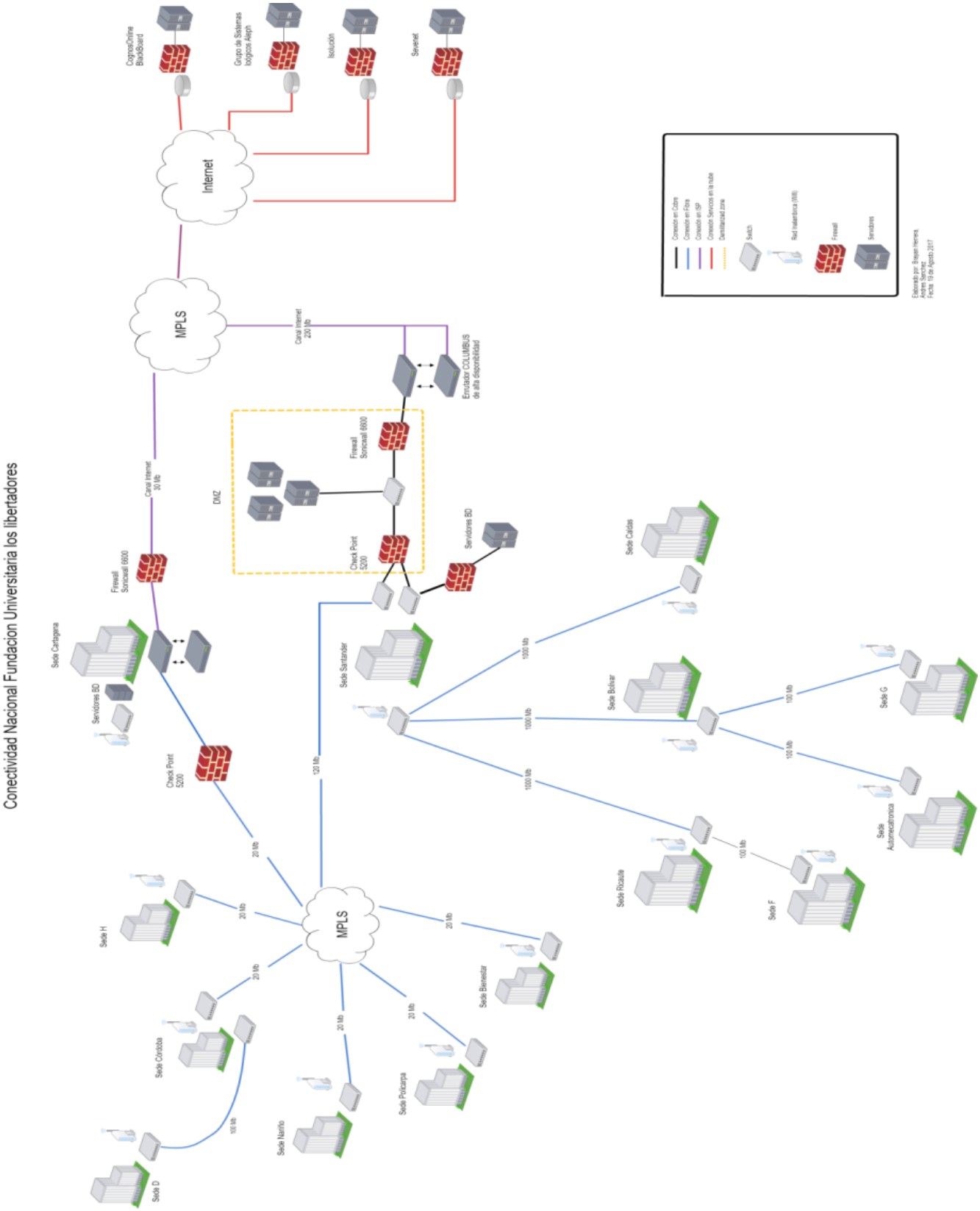
Durante el desarrollo del punto 4.4 Análisis de la información, se logró identificar el inventario de elementos tecnológicos que posee la FULL y con base en la topología de red actual (ver Anexo 3), se propone el siguiente diseño de red, el cual detalla cambios en el diseño original que se encuentran en la gráfica número 5. Diagrama de red. Por otra parte, permite detallar la ubicación del diseño de la DMZ propuesto en el punto 4.5.4 Diseño DMZ Propuesto.

5.1.1 Elementos utilizados en el cambio

El proceso de análisis aplicado al funcionamiento de la red de datos, se encontraron varios elementos los cuales se cambiaron. Estos elementos se describen a continuación:

a. Se debe mejorar las comunicaciones entre la sede D y la sede Córdoba, para esto se recomienda cambiar el cableado de cobre a fibra y así garantizar la continuidad en la comunicación.
b. De igual manera se propone implementar cambios en las comunicaciones entre la sede Bolívar y sus dos dependencias; sede auto mecatrónica y sede G, ya que por la distancia que las separa es posible que existan fallas en las comunicaciones, por esta razón se reemplazó el cableado de cobre por fibra.
c. En la conectividad que existe entre los canales de comunicación y las sedes se decidió implementar un Firewall Sonicwall 6600 para controlar el tráfico entrante de estos canales y poder acoplar el diseño de DMZ con doble Firewall.

Gráfico 7. Diagrama de red



5.1.2 Diseño de DMZ

En toda institución de educación superior, debe presentar un buen manejo de la información que se recoleta de la comunidad de estudiantes, educadores, académica y administrativa, por lo anterior es necesario que existan sistemas de información enfocados en cada uno de las ramas. Cada uno de estos sistemas de información manejan un nivel de seguridad en los datos que recolecta y para ello es necesario que cuenten con el mismo nivel de seguridad en su red de datos por esta razón el diseño de la DMZ propuesta se enfoca en utilizar 2 firewall, los cuales deben estar configurados pertinentemente para que brinden una mayor seguridad, para permitir el tráfico destinado a la DMZ solamente, en el segundo firewall solo permite el tráfico de la DMZ a la red interna.

A continuación, se observa un modelo estándar donde se detalla la configuración de una DMZ con doble Firewall.

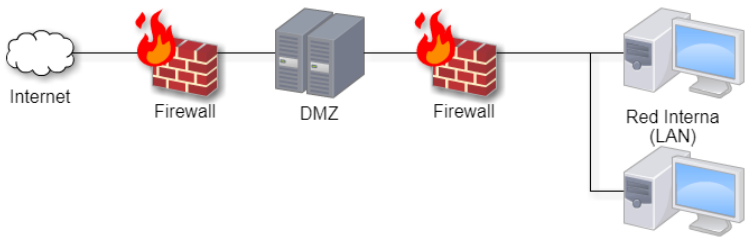


Gráfico 8. Modelo DMZ Doble Firewall

Para implementar esta solución se recomienda instalar un firewall corporativo, el cual sea un dispositivo físico y no agregarle funciones de seguridad a un router estándar, por temas de seguridad, ya que se puede tener un sobre cargar en uno de los dispositivos configurados y pueden causar lentitud en los canales de comunicación.

Las políticas básicas del firewall externo, desde y hacia la DMZ se configuran con las siguientes políticas básicas.

Origen	Destino	Política
Outside	DMZ	Permitido
Outside	Inside	Denegado
DMZ	Outside	Permitido
DMZ	Inside	Denegado
Inside	Outside	Permitido
Inside	DMZ	Permitido

Tabla 8. Políticas Firewall

Trafico desde y hacia la DMZ

En el siguiente grafico se podrá observar cómo funciona el tráfico permitido y no permitió desde y hacia la DMZ.

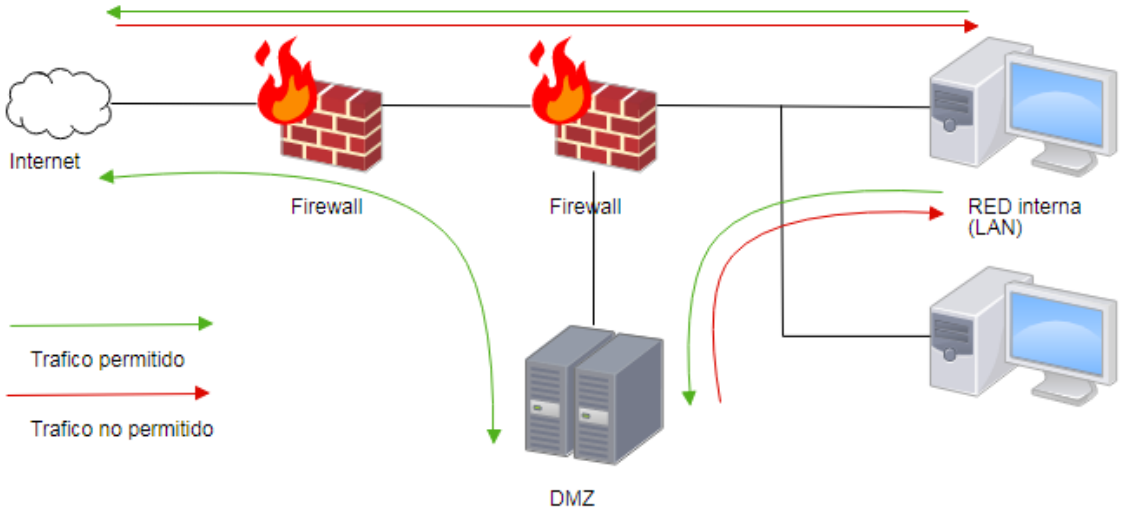


Gráfico 9. Trafico DMZ

Mecanismo de implementación

A continuación, se presentará soluciones comerciales que se han elegido para realizar esta arquitectura de seguridad para una DMZ. Se detallará en orden hacia adentro y por cada una de ellas, se expondrá otra alternativa.

Elementos Físicos (Hardware)

A continuación, se detallan los elementos que se recomiendan actualizar en la red de la Fundación Universitaria Los Libertadores.

Firewall Externo

Propuesta	**Alternativa**
FortiGate 7000E	Firewall FW-6600
La solución FortiGate 7000E trae consigo una configuración robusta, en cuanto a protección, seguridad y rendimiento. Ofreciendo mayor velocidad de procesamiento y mayor fluidez en sus segmentaciones internas.	La solución Firewall FW-6600 trae consigo una configuración de seguridad diseñada para pequeña y mediana empresa, la cual ofrece una protección de seguridad y de procesamiento de datos.
Características técnicas Rendimiento del Firewall 155GBps Rendimiento IPS 60GBps	Características técnicas Rendimiento del Firewall 12GBps Rendimiento IPS 4,5GBps

Firewall Interno

La propuesta para el segundo firewall que está ubicado entre la DMZ y la red local se propone usar una de las siguientes alternativas.

Propuesta	**Alternativa**
Check point 5200	Check Point SandBlast Zero-Day Protection
La solución Check point 5200 trae consigo una configuración de protección estándar para medianas empresas, su velocidad de procesamiento no se ve interrumpida aun cuando este está cifrando o recibiendo paquetes.	La solución Check Point SandBlast Zero-Day Protection trae consigo una configuración de seguridad diseñada para pequeña y mediana empresa, la cual ofrece distintas configuraciones gracias a su software libre y soporte gratuito.
Características técnicas Rendimiento del Firewall 16GBps Rendimiento IPS 3GBps	Características técnicas Rendimiento del Firewall 12GBps Rendimiento IPS 2GBps

Firewall externo

Políticas de seguridad controles de seguridad y preventivos

En la siguiente tabla se encuentra los controles de seguridad que deben ser aplicados hacia la DMZ.

Periodicidad	Descripción de tareas
Diaria	• Revisión de logs en busca de algún funcionamiento Anómalo. • Verificación de la correcta rotación de logs • Resolución de incidencias, mantenimiento y soporte de la política de reglas. • Búsqueda de vulnerabilidades y fallos conocidos del sistema del sistema en listas de distribución y páginas web. • Instalación de parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
Semanal	• Búsqueda de nuevas versiones y mejoras de StoneGate. • Instalación de parches de funcionalidad y nuevas versiones publicadas para StoneGate. • Revisión del correcto funcionamiento del Log Server y consola de gestión del sistema cortafuegos StoneGate. • Verificación de la capacidad de disco para almacenar logs.
Mensual	Revisión general de la política de seguridad de los sistemas cortafuegos internos.

Tabla 9. Firewall externo

Firewall Interno

Políticas de seguridad controles de seguridad y preventivos

En la siguiente tabla se encuentra los controles de seguridad que deben ser aplicados hacia la DMZ.

Periodicidad	Descripción de tareas
Diaria	• Revisión de logs en busca de algún funcionamiento anómalo. • Verificación de la correcta rotación de logs • Resolución de incidencias, mantenimiento y soporte de la política de reglas. • Búsqueda de vulnerabilidades y fallos conocidos del sistema del sistema en listas de distribución y páginas web. • Instalación de parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
Semanal	• Búsqueda de nuevas versiones y mejoras de CheckPoint. • Instalación de parches de funcionalidad y nuevas versiones publicadas por CheckPoint. • Verificación de la capacidad de disco para almacenar logs
mensual	• revision general de la política de seguridad de los sistemas Firewall

Tabla 10. Firewall Interno

Procedimiento de actuación ante un fallo de un elemento de red

Se realizará una descripción del procedimiento frente al fallo de un elemento de red de la infraestructura de seguridad.

Los pasos a seguir son los siguientes:

- Detección del fallo en la red, mediante el uso de los sistemas de gestión de las plataformas.

- Se clasificaría la incidencia según nivel de criticidad (alta, media, baja)
- En caso de criticidad alta (indisponibilidad de algún servicio esencial) se procedería a informar de forma inmediata al responsable de la organización.
- Se procederá a intentar resolver el problema.
- Si en un plazo razonable el problema persistiera se escalaría el problema al equipo de soporte del fabricante del elemento de red.
- Una vez resuelta la incidencia se documentaría su desarrollo y resolución.

Procedimiento de actuación frente a la detección de una vulnerabilidad en la red.

Los pasos a seguir son los siguientes:

- Detección de la vulnerabilidad, en el transcurso de una revisión periódica o mediante la notificación de una incidencia.
- Estudio y análisis de la vulnerabilidad (cuantificación de la amenaza y riesgo asociado a esa vulnerabilidad).
- En caso de vulnerabilidad grave con un alto índice de riesgo se procedería a informar de forma inmediata al responsable de la organización.
- Se procederá a buscar una solución a dicha vulnerabilidad.
- Una vez encontrada la forma de solucionar dicha vulnerabilidad se procederá a mitigarla (instalando parches, cerrando servicios, etc.,). Si el sistema afectado no pertenece a la infraestructura de seguridad perimetral, se procedería a informar al administrador correspondiente de cómo mitigar la vulnerabilidad.
- Una vez resuelta la vulnerabilidad se documentaría su desarrollo y resolución en un informe de vulnerabilidad.

Procedimiento de actuación frente a la realización de un cambio en la red

Los pasos a seguir son los siguientes:

- Determinación del alcance del cambio, elementos afectados, implicaciones del cambio y duración del procedimiento de cambio (migración).
- Elaboración de un plan de cambio de red (o plan de migración).

- Autorización del cambio por parte de la organización.
- Programación del cambio en horario de mínimo impacto.
- Comunicación, con la suficiente antelación, a los usuarios afectados del momento de realización del cambio.
- Realización del cambio en horario de mínimo impacto.
- Documentación del cambio realizado y actualización de los documentos afectados por el cambio.

Procedimiento de actuación frente a un cambio de políticas de seguridad

Los pasos a seguir son los siguientes:

- Determinación del alcance del cambio, elementos afectados, implicaciones del cambio y duración del procedimiento de cambio (migración).
- Elaboración de un plan de cambio de red (o plan de migración).
- Autorización del cambio por parte de la organización.
- Programación del cambio en un horario acordado.
- Comunicación, con la suficiente antelación, a los usuarios afectados del momento de realización del cambio.
- Realización del cambio en el momento acordado.
- Documentación del cambio realizado y actualización de los documentos afectados por el cambio.

Reglas para el firewall

El primer paso en la definición de una regla de firewall es determinar qué se debe hacer con una conexión que cumple con los criterios que define la regla. Dos acciones son posibles:

Permitir	Permite que ocurra la comunicación de este tipo
Bloquear	Impide que ocurra la comunicación de este tipo

Tabla 11. Definición de Regla

Especifique los equipos a los cuales se debe aplicar la regla:

Cualquier equipo	La regla se aplica a todos los equipos
Cualquier equipo de la subred local	La regla se aplica solamente a los equipos en la subred local
Elegir equipos	La regla se aplica solamente a los equipos, los sitios o los dominios que se detallan en la lista. Las opciones incluyen lo siguiente: • Individualmente: mediante la especificación de un nombre de equipo o URL • Uso de rango: mediante la especificación de un rango de direcciones IP • Uso de dirección de red: mediante la especificación de una dirección IP y su máscara de subred Las opciones de identificación de equipos se pueden combinar en direcciones definidas.

Tabla 12. Especificación de Equipos

El paso final en la creación de una nueva regla de firewall es definir los protocolos de comunicaciones usados para la conexión. Puede especificar estos protocolos:

TCP, UDP, TCP y UDP, ICMP, ICMPv6 o todos.

Cuando selecciona un protocolo a excepción de Todos, se permiten las comunicaciones de todos los tipos de protocolos seleccionados. Cuando necesite ser más restrictivo, genere una Lista personalizada.

Una Lista personalizada permite generar la lista en función de lo siguiente:

Puertos conocidos de lista	Los puertos conocidos ofrecen servicios reconocidos. Las aplicaciones menos comunes o propietarias necesitan que identifique los puertos que usa la aplicación.
Puertos individuales específicos	La regla se aplica a los puertos que especifica. Delimite varios puertos varios con espacios.
Rango de puertos	La regla se aplica a todos los puertos entre el número de puerto más bajo y el más alto. Especifique el rango de puertos del número de puerto más bajo al más alto.

Tabla 13. Lista personalizada

5.1.3 Elementos De la red de datos de la FULL

Para determinar que camino se debe tomar, la correcta distribución de los elementos tecnológicos que se van a utilizar, se recomienda como buena práctica, realizar un inventario de los sistemas de información principales de la red de datos y de los elementos físicos con los cuales cuenta la FULL.

De esta manera se detalla la información que es privada, de la información que debe ser publica y así se toma la decisión de que elementos físicos interactúan dentro de esta red de datos que pueden intercambiar información la cual debe estar protegida.

Realizando el análisis de los puntos 4.4 y 4.5, se deduce que los elementos a participar dentro de esta propuesta son los siguientes:

Tabla 14. Servidores DMZ

Sistema Operativo	Servicio	Concepto
WINDOWS	Citrix Web Interface	Publicos
WINDOWS	Citrix XenApp A	Publicos
WINDOWS	Citrix XenApp B	Publicos
WINDOWS	Citrix XenApp C	Publicos
WINDOWS	Citrix XenApp D	Publicos
WINDOWS	Citrix XenApp E	Publicos
WINDOWS	Citrix XenApp F	Publicos
WINDOWS	Servidor de administración de VMWare	Publicos
LINUX	Servidor de Autenticación Google Apps	Publicos
WINDOWS	FTP BlackBoard	Publicos
LINUX	HelpDesk Gerencia de Tecnología	Publicos
LINUX	Administrador de Oracle VM para nodo intel	Publicos
WINDOWS	http://helpdeskvirtual.libertadores.edu.co:8088/helpdeskvirtual/index.php http://helpdeskvirtual.libertadores.edu.co:8088/distancia http://helpdeskvirtual.libertadores.edu.co:8088/dotproject/	Publicos
LINUX	Portal Joomla para las pantallas	Publicos
LINUX	Apache, MySql, PhP, JOOMLA	Publicos
LINUX	Apache, MySql, Portal Tesis Psicológica	Publicos
LINUX	Apache, MySql, Portal Revista Perfiles	Publicos
LINUX	Software de Votaciones, apache, Mysql, PHP	Publicos
LINUX	Digiturno Tesoreria	Publicos
LINUX	Notificaciones de correo electronico	Publicos
WINDOWS	Servidor de VmWare VsPhere, Blade 5	Publicos
FIREWALL	https://172.16.0.55:7070/WebManagement/WebManagement.html	Publicos

5.1.4 Diseño DMZ propuesto

En el grafico 8. Propuesta DMZ, se evidencia la estructura final de la DMZ para la Fundación Universitaria los Libertadores, realizando la propuesta de los servidores que se consideran deben estar dentro de ella.

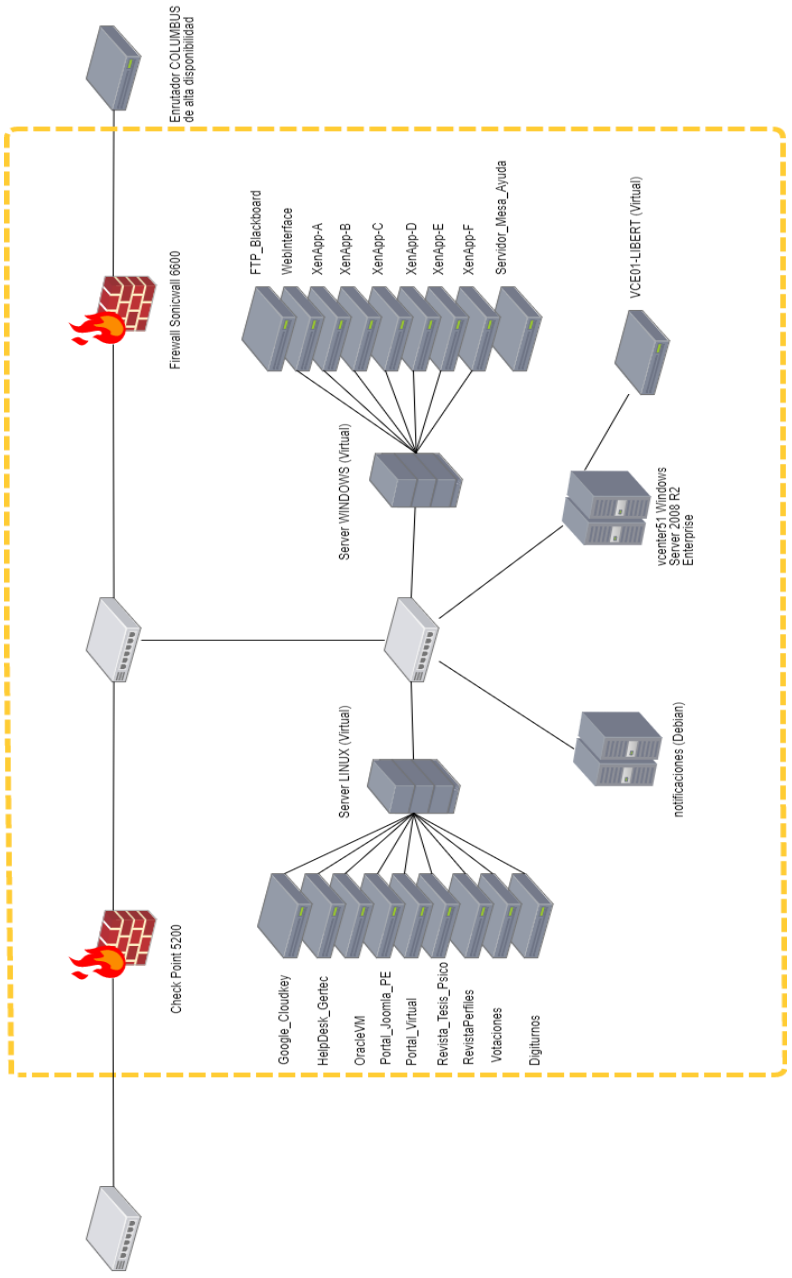


Gráfico 10. Propuesta DMZ

5.2 IMPLEMENTACION DE LA DMZ

La siguiente propuesta fue desarrollada y planteada bajo la red actual con la que cuenta la Fundación Universitaria Los Libertadores. Teniendo en cuenta que por directrices de seguridad, cierta parte del levantamiento de información no se pudo llevar acabo, se establecen criterios limitados para realizar esta propuesta.

En esta propuesta a tratado de dar a conocer lo que es una DMZ, sentando bases teóricas, y a si posteriormente exponer la implementación de una DMZ. Para ello partimos con la red actual de la institución, luego de establecer los requerimientos se ha ofrecido una solución que cumpla en todo momento con un nivel de seguridad y un rendimiento óptimo. Además, se han incluido métodos de gestión y controles.

La elaboración de esta propuesta consta de 2 firewall los cuales ayudarán a proteger el tráfico desde la DMZ a internet como el tráfico desde DMZ hacia la red local, se detallarán las características específicas de los cambios a realizar los cuales contribuyen al mejoramiento de la red actual. Otro de los cambios que se sugieren es un nuevo diseño en la elaboración de una DMZ la cual consta de mejoras en la comunicación, reconfigurar un firewall el cual restringirá la navegación que entra desde el enrutador Columbus.

Dando un propósito a los diseños realizados, se hacen con el único fin de contribuir con el mejoramiento continuo de la universidad y poder aportar algo del conocimiento adquirido a la institución.

5.3 CONFIGURACIÓN DMZ

A continuación, se detalla los parámetros de configuración que deben tener en cuenta durante el proceso de implementación, para ello se detallaron los siguientes puntos como recomendaciones, los cuales se consideran los más importantes.

5.3.1 Balanceo de carga

Equilibrio de carga de soniwall 6600

El equilibrio de carga, los miembros de varias WAN son compatibles (N-1), donde N es el número total de interfaces en una plataforma de hardware. Por ejemplo:

• Interfaz Ethernet de WAN primaria

• WAN alternativa 1

• WAN alternativo 2

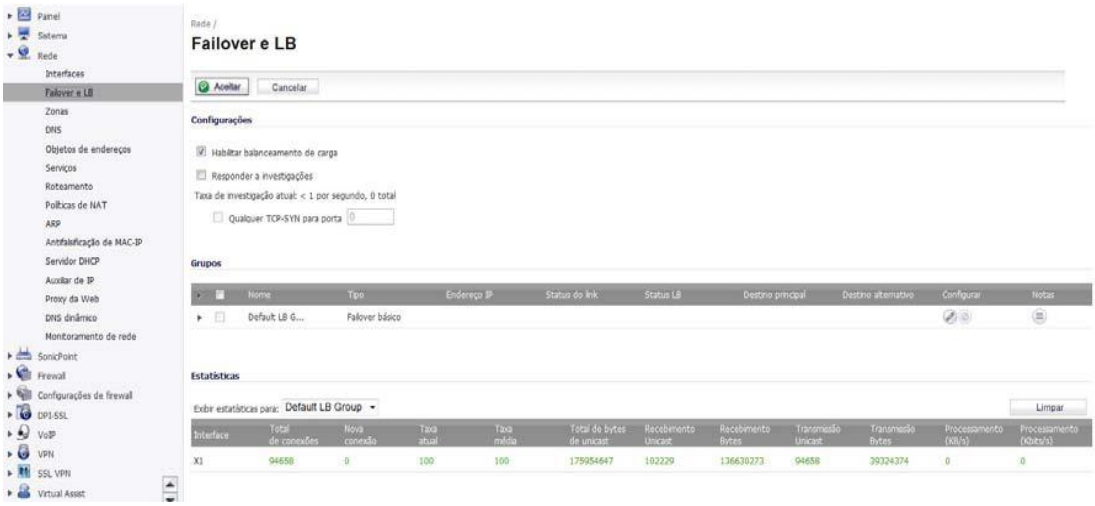
• WAN alternativa <n-1>. . .

La interfaz Ethernet de WAN primaria. Es la interfaz de WAN de clasificación más alta en el grupo. La WAN alternativa 1 corresponde a la "WAN secundaria", tiene una clasificación más baja que la WAN primaria, pero tiene una clasificación más alta que las próximas dos alternativas. La otras, WAN alternativa 2 y WAN alternativa <n-1>, son nuevas, siendo WAN alternativa <n- 1> la más baja en términos de clasificación entre los cuatro miembros de la WAN del grupo. Las configuraciones de conmutación por error y de equilibrio de carga se describen a continuación:

• Habilitar equilibrio de carga: esta opción debe estar habilitada para que el usuario acceda a la sección Grupos y estadísticas de la configuración de Failover y equilibrio de carga.

• Responder a las investigaciones - cuando la opción está habilitada, el dispositivo puede responder a los paquetes de solicitud de investigación que lleguen a cualquiera de las interfaces del dispositivo. Cualquier TCP-SYN para puerto - esta opción está disponible cuando la opción Responder las investigaciones están habilitadas. Cuando

se selecciona, el dispositivo responder sólo a paquetes de solicitud de investigación TCP con el mismo número de puerto TCP dirección de destino de paquete que el valor configurado.



Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

Realizar el equilibrio de carga de miembros y grupos

Los miembros agregados a un grupo de failover y equilibrio de carga asumen ciertas "funciones". Una miembro sólo puede trabajar en una de las siguientes funciones:

• Primario: sólo un miembro puede ser el Primario por Grupo. Este miembro siempre aparece primero o en la parte superior de la lista de miembros.

• Alternativo - más de un miembro puede ser Alternativo, sin embargo, no es posible tener un Grupo de miembros sólo alternativos.

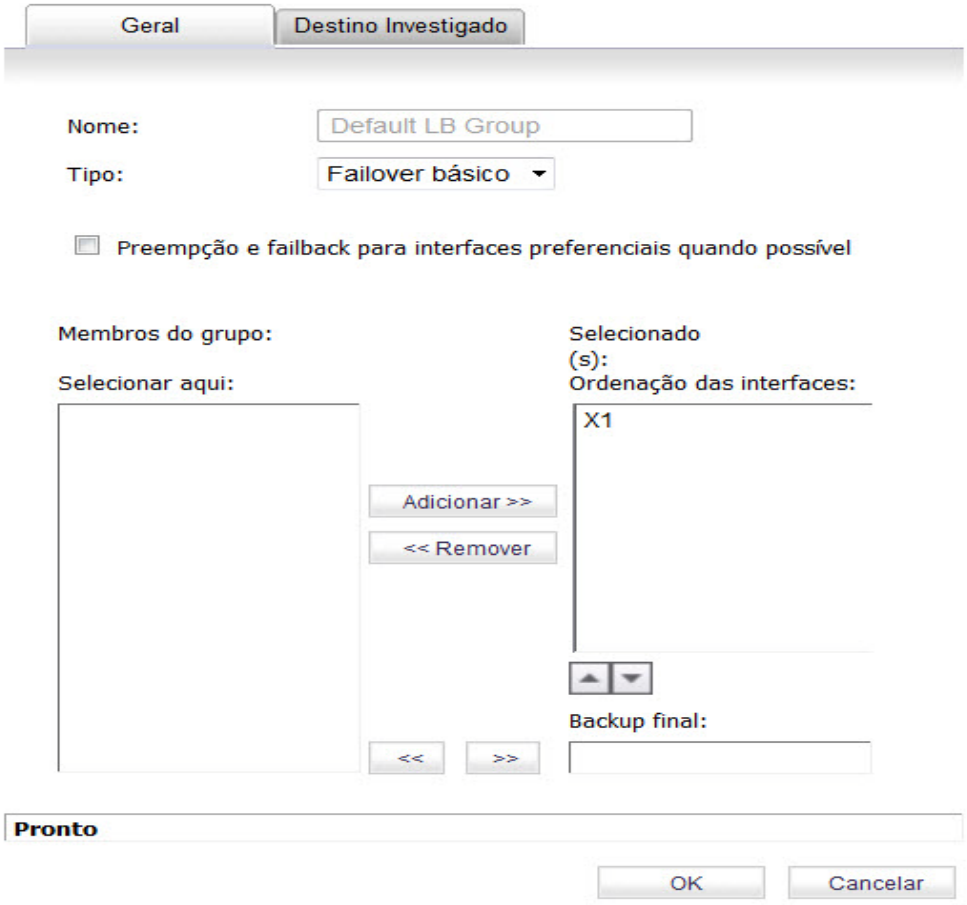
• Último recurso: sólo un miembro se puede proyectar como último recurso. El último el recurso sólo se puede configurar con otros miembros del grupo.

Cada miembro de un grupo tiene una clasificación. Los miembros se visualizan en orden decreciente de clasificación. La clasificación está determinada por el orden de las interfaces como aparecen en la lista de miembros del grupo. La orden es

importante para determinar las preferencias de uso de las interfaces, así como el nivel de precedencia dentro del grupo. Por lo tanto, las dos interfaces dentro de un grupo no tendrán la misma clasificación; cada interfaz tendrá una clasificación distinta.

5.3.2 Configuración de clasificación de miembros de grupo

Para establecer la configuración de clasificación de miembros del grupo se accede a la pantalla en ficha general como se muestra a continuación.



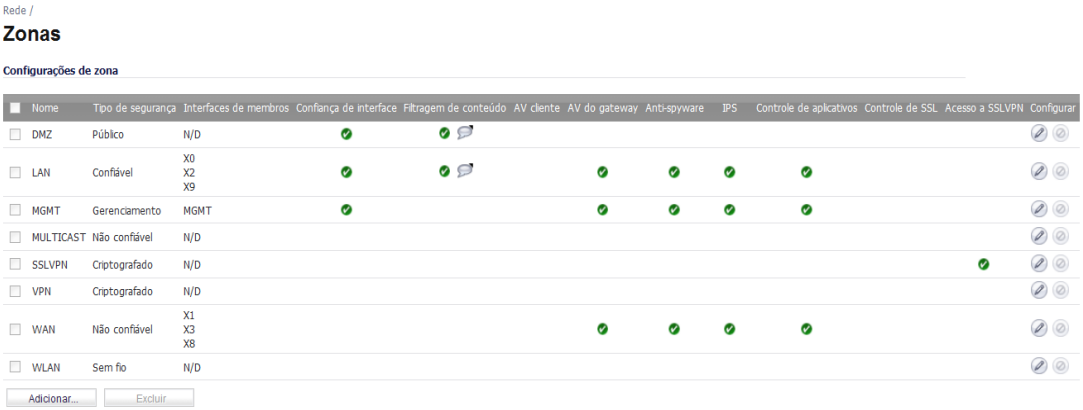
Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

La ficha General permite al usuario modificar las siguientes configuraciones:

- Nombre de visualización: modifique el nombre para mostrar del grupo
- Tipo (o método): seleccione el tipo de balanceo de carga en la lista desplegable (Failover activo / pasivo básico, Round Robin, Basado en spillover o Con base en el porcentaje).
- Transbordo - el límite de ancho de banda se aplica a la WAN primaria. Después de que el límite se supere, los nuevos flujos de tráfico se asignan a las Alternativas de una Ronda Robin. Después de que el ancho de banda de WAN principal esté por debajo del límite configurado, el Round Robin para y comenzarán siendo enviados nuevos flujos de salida sólo a través de la WAN primaria. Observe que los flujos existentes se quedarán asociados a las Alternativas (ya que están en caché) hasta que el tiempo el límite se alcanza normalmente.
- Agregar / eliminar interfaces de miembros - se pueden agregar miembros seleccionando una interfaz que aparece en la columna "Miembros del grupo".

5.3.3 Redes y zonas

Una zona es un agrupamiento lógico de una o más interfaces diseñadas para hacer gestión, como la definición y la aplicación de reglas de acceso, un proceso más simple e intuitivo que seguir el esquema estricto de interfaz física. La seguridad basada en zona es un método poderoso y flexible de gestión de segmentos de redes internas y externa, permitiendo que el administrador separe y proteja recursos esenciales de la red interna contra el acceso no aprobado o el ataque.



Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

Dentro de la configuración del firewall soniwall 6600 vienen como predefinidas ciertas zonas como lo son

• DMZ: Esta zona se utiliza normalmente para los servidores públicos accesibles. Esta zona puede ser compuesta por una a cuatro interfaces, dependiendo del diseño de su red.

• LAN: Esta zona puede estar compuesta por varias interfaces, dependiendo del diseño de su interfaz red. Aunque cada interfaz tiene una subred de red diferente conectada a ella, cuando se agrupan se pueden administrar como una sola entidad.

• MGMT: Esta zona se utiliza para la administración de dispositivos e incluye sólo la interfaz de MGMT. Las interfaces en otras zonas también se pueden habilitar para gestión de SonicOS.

• DIFUSIÓN SELECTIVA: Esta zona admite la difusión selectiva de IP, que es método de envío de paquetes de entrada de un único origen simultáneamente para varios anfitriones.

• SSLVPN: Esta zona se utiliza para proteger el acceso remoto mediante el cliente NetExtender de Dell SonicWALL.

• VPN: Esta zona virtual se utiliza para simplificar la conectividad remota y segura.

• WLAN: Esta zona admite los SonicPoints de SonicWALL. Cuando se asigna a la el puerto Opt, realiza la imposición de SonicPoint, descartando automáticamente todos los paquetes recibidos de dispositivos no SonicPoint. La zona de WLAN admite el protocolo de descubrimiento de SonicPoint (SDP) para buscar e identificar SonicPoints conectados de forma automática. También apoya el protocolo de aprovisionamiento simple de SonicWALL para configurar los SonicPoints usando perfiles.

• WAN: Esta zona puede consistir en varias interfaces. Si está utilizando la característica de la conmutación por error de WAN del dispositivo de seguridad, tendrá que agregar la segunda interfaz de Internet a la zona de WAN.

Tipos de seguridad

Cada zona tiene un tipo de seguridad que define el nivel de confianza asignado a esa zona. Existen seis tipos de seguridad:

• Confiable: Confiable es un tipo de seguridad que ofrece el más alto nivel de confianza, que significa que el mínimo de control se aplica al tráfico procedente de zonas fiable. La seguridad confiable se puede considerar como en el lado de la LAN (protegido) del dispositivo de seguridad. La zona de LAN siempre es confiable.

• Gestión: El tipo de seguridad de administración es exclusivo para la zona de MGMT y la interfaz de MGMT y también proporciona el más alto nivel de confianza.

• Cifrado: Cifrado es un tipo de seguridad utilizado exclusivamente por zonas de seguridad VPN y SSLVPN. Todo el tráfico hacia y desde una zona cifrada está cifrado.

• Inalámbrico: Inalámbrico es un tipo de seguridad aplicado a la zona de WLAN o a cualquier zona donde la única interfaz para la red consiste en dispositivos SonicPoint de SonicWALL. El tipo de seguridad inalámbrica está diseñada específicamente para su uso con dispositivos SonicPoints.

• Público: Un tipo de seguridad pública ofrece un nivel más alto de confianza que una zona no confiable, pero un nivel más bajo de confianza que una zona Fiable. Las zonas públicas pueden considerarse como un área segura entre el lado de la LAN (protegido) del dispositivo de seguridad y el lado de la WAN (desprotegido). La DMZ, por ejemplo, es una zona pública porque el tráfico fluye de él a la LAN y la WAN. Por de forma predeterminada, se deniega el tráfico de DMZ a LAN. Pero el tráfico de LAN para CUALQUIER es permitido. Esto significa que sólo las conexiones iniciadas por LAN tendrán el tráfico entre DMZ y LAN. La DMZ sólo tendrá acceso estándar a la WAN, no a la LAN.

• No confiable: El tipo de seguridad no confiable representa el nivel más bajo de la confianza. Se utiliza por la WAN y la zona de difusión selectiva virtual. Una zona no confiable puede considerarse que está en el lado de la WAN (desprotegido) dispositivo de seguridad. De forma predeterminada, no se permite la entrada de tráfico de zonas No fiables en cualquier otro tipo de zona sin reglas explícitas, pero el tráfico de tipos de se permiten zonas alternas en zonas no confiables.

5.3.4 Configuración NAT

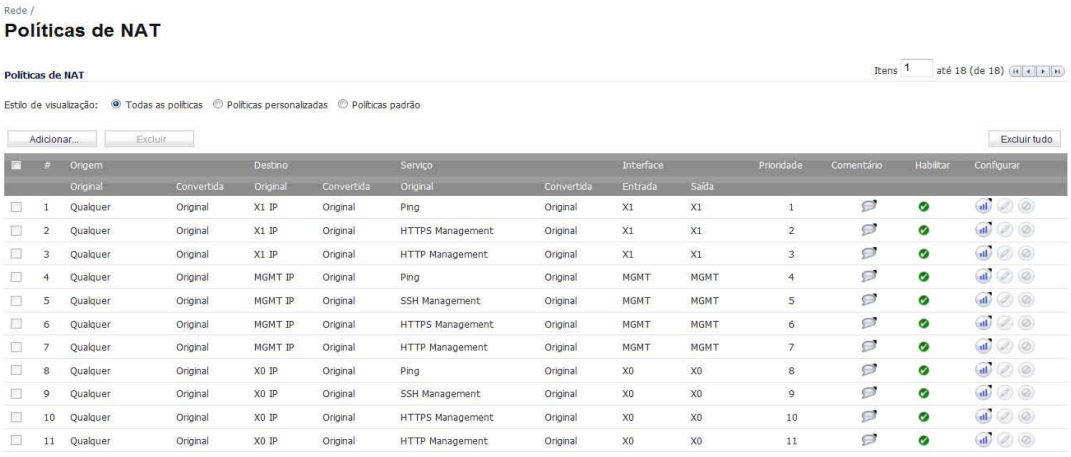
Las nociones básicas sobre cómo utilizar las políticas de NAT comienzan con la construcción de un paquete IP. Cada paquete contiene información de direccionamiento el cual permite que llegue a su destino y que el destino, responda al solicitante original. El paquete contiene (entre otras cosas) la dirección IP del solicitante, la información de protocolo del solicitante y la dirección IP del destino. El mecanismo de políticas de NAT en SonicOS puede inspeccionar las partes relevantes del paquete y, de forma dinámica, reescribir la información en los campos especificados para el tráfico entrante y saliente. Puede agregar hasta 512 políticas NAT en un dispositivo de seguridad Dell SonicWALL ejecutando SonicOS y pueden ser tan granulares como sea necesario. También es posible crear varias directivas NAT para el mismo objeto, por ejemplo, puede especificar que un servidor interno utiliza una dirección IP al acceder a servidores Telnet y utiliza una dirección IP totalmente diferente en todos los demás protocolos. Como el mecanismo NAT en SonicOS admite el enrutamiento de puerto de entrada, puede ocultar varios servidores internos de la dirección IP de WAN del firewall. Cuanto más granular es la política de NAT, mayor será la precedencia.

La siguiente tabla muestra un número máximo de rutas y políticas de NAT permitidas para cada uno modelo de dispositivos de seguridad de red SonicOS 6.2.

Modelo	Rotas	Políticas de NAT
NSA 2600	—	1024
NSA 3600	—	1024
NSA 4600	—	1024
NSA 5600	—	2048
NSA 6600	1024	2048
SM 9200	1024	2048
SM 9400	1024	2048
SM 9600	1024	2048

Tabla 15. Política del NAT

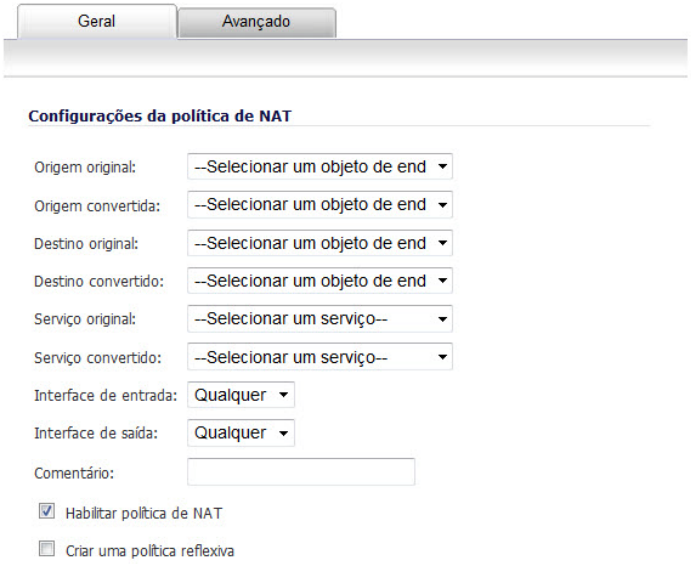
La tabla de directivas de NAT le permite ver sus políticas NAT a través de todas las políticas, las políticas personalizadas o las directivas predeterminadas.



Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

5.3.5 Configuración de política NAT

A continuación, se explican las configuraciones utilizadas para crear una entrada de directiva NAT en las ventanas Agregar directiva NAT o Editar política NAT.



Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

Origen original: Esta configuración de menú desplegable se utiliza para identificar las direcciones IP de origen en el paquete que cruza el firewall, ya sea a través de interfaces o en / fuera de los túneles de VPN. Puede utilizar los objetos de direcciones predeterminados en SonicOS o puede crear sus propios objetos de direcciones. Estas entradas pueden ser entradas de host único, rangos de direcciones o subredes de IP.

• Origen convertida: Esta configuración de menú desplegable es aquella en la que el origen original se convierte a medida que sale del firewall, ya sea para otra interfaz o en / fuera de los túneles de VPN. Puede utilizar los objetos de direcciones predeterminados en SonicOS o puede crear sus propias entradas de objetos de dirección. Estas entradas pueden entradas de host único, rangos de direcciones o subredes de IP.

• Destino original: Esta configuración de menú desplegable se utiliza para identificar las direcciones IP de destino en el paquete que cruza el firewall, ya sea a través de interfaces o en / fuera de los túneles de VPN. Al crear directivas NAT de salida, esta entrada normalmente se establece en Cualquiera, ya que el destino del paquete no se cambia, pero sí su origen. Sin embargo, estas entradas de objeto de dirección pueden ser entradas de host único, rangos de direcciones o subredes de IP.

• Destino convertido: Esta configuración de menú desplegable es aquella en la que el servidor de seguridad convierte el destino original a medida que sale del firewall, ya sea para otra interfaz o en / fuera de los túneles de VPN. Al crear directivas NAT de salida, esta entrada normalmente se define como Original, ya que el destino del paquete no se cambia, sino su origen. Sin embargo, estas entradas de objetos de dirección pueden ser entradas de host único, rangos de direcciones o subredes de IP.

• Servicio original: Esta configuración de menú desplegable se utiliza para identificar el servicio de IP en el paquete que cruza el firewall, ya sea a través de interfaces o en / fuera de túneles de VPN. Puede utilizar los servicios predeterminados en el servidor de seguridad o puede crear sus propias entradas. Para muchas políticas de NAT, este

campo se establece en Cualquiera, ya que la directiva está cambiando sólo las direcciones IP de origen o de destino.

• Servicio convertido: Esta configuración de menú desplegable es aquella en la que el servidor de seguridad convierte el servicio original a medida que sale del servidor de seguridad, ya sea a otra interfaz o en / fuera de los túneles de VPN. Puede utilizar los servicios predeterminados en el servidor de seguridad o puede crear sus propias entradas. Para muchas políticas NAT, este campo se define como Original, ya que la directiva está cambiando sólo las direcciones IP de origen o de destino.

• Interfaz de entrada: Esta configuración de menú desplegable se utiliza para especificar la interfaz de entrada del paquete. Al tratar con las VPN, esto generalmente se define como Cualquiera, ya que los túneles VPN no son realmente interfaces.

• Interfaz de salida: Este menú desplegable se utiliza para especificar la interfaz de salida paquete una vez aplicada la directiva NAT. Este campo se utiliza principalmente para especificar qué interfaz de WAN se aplicará a la conversión. De todos los campos en la política NAT, este es el que tiene más potencial para la confusión. Al tratar con VPN, esto generalmente se establece en Cualquiera, ya que los túneles de VPN no son realmente interfaces. Además, como se indica en la sección "Preguntas y respuestas rápidas" de este capítulo, al crear políticas de NAT uno a uno de entrada, en el que el destino está siendo reasignado de una dirección IP pública a una dirección IP particular, este campo se debe establecer en Cualquiera.

• Comentario: Este campo se puede utilizar para describir su entrada de directiva NAT. El campo tiene un límite de 32 caracteres y, una vez guardado, se puede ver en la página principal Red Políticas de NAT pasando el ratón sobre el globo de texto al lado de la entrada de directiva NAT. Su comentario aparece en una ventana emergente si el ratón está sobre el globo de texto.

• Habilitar política NAT: De forma predeterminada, esta casilla está marcada, lo que significa que la nueva se activa la directiva NAT en el momento en que se guarda.

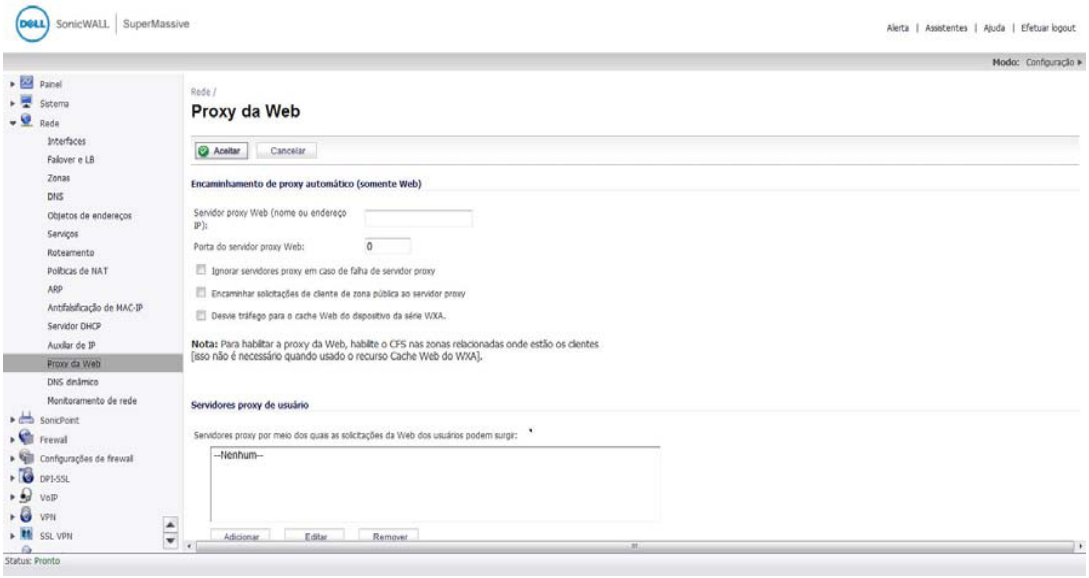
Para crear una entrada de directiva de NAT, pero no activarla inmediatamente, desmarque esta casilla.

• Crear una política reflexiva: Cuando marca esta casilla, se crea automáticamente una política NAT de entrada o salida reflejada de la política NAT que ha definido en la ventana Agregar directiva NAT.

5.3.6 Proxy web cache

Un servidor proxy Web intercepta solicitudes HTTP y determina si se almacenó copias de las páginas Web solicitadas. Si no se ha almacenado, el proxy finaliza la solicitud al servidor en Internet, devolviendo la información solicitada al usuario y también salvándolas localmente para futuras solicitudes. La configuración de un servidor proxy Web en una red puede ser complicada, ya que cada equipo de la red debe estar configurado para direccionar solicitudes Web al servidor.

Si tiene un servidor proxy en su red, en lugar de configurar el explorador Web cada equipo para apuntar al servidor proxy, puede mover el servidor a la WAN o DMZ y habilitar el reenvío de proxy Web mediante la configuración de la página Red.



Obtenida desde https://es.scribd.com/document/363655939/sonicos-6-2-admin-guide-28brazil-29-pdf, SoniWall(2014), guía de administración de SonicOS 6.2,octubre 2014.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Durante el desarrollo se llegaron a las siguientes conclusiones.

- Considerando la estructuración de la universidad los libertadores, a nivel interno, se resaltó los niveles en los que se debe distribuir la segmentación interna de la red, siendo así un argumento para proponer las variables que debe ser monitorear dentro de la red interna.
- Detallando los elementos utilizados para el levantamiento de información y los mecanismos utilizados para este fin, se demostró el conocimiento adquirido, durante el desarrollo de este proyecto y así poder aportar un cambio estructural en la red interna de la fundación universitaria los libertadores.
- Observando cuantos servidores están expuestos a ataques provenientes de internet, e incluso desde la red local, los controles de seguridad tienen que cumplirse de forma muy estricta y ser vigilados constantemente.

6.2 RECOMENDACIONES

Teniendo en cuenta los cambios sugeridos en los puntos anteriores y según el análisis realizar durante el desarrollo de la investigación, se han encontrado ciertos patrones en la red y según lo implementado se recomienda lo siguiente:

- Requiere implementar un sistema de monitoreo periódico en los servicios que están dentro del diseño DMZ.
- Aplicar estrategias para aprovechar el tiempo de vida de cada uno de los elementos inalámbricos que poseen la universidad.
- Monitorizar el tráfico de la red desde y hacia la DMZ para verificar la cantidad de servicios que esta presta y así tener una medición real del consumo de canal.
- Establecer planes estratégicos para la ejecución periódica de auditorías internas en cada proceso que compone la DMZ.

- Generar un control de mantenimientos preventivos como mínimo 1 vez a año para así garantizar la vida útil de los elementos que componen la red.
- Establecer planes de actualización de cada uno de los servidores o dispositivos que requieran dicho proceso y tener un control periódico para que mensualmente se realice esta actividad.
- Establecer controles de hardening en el sistema para reducir las vulnerabilidades que afectan al sistema

7. VOCABULARIO

IPsec: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que, para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código (Carlos Diaz, SEPTIEMBRE 2013).

Ssl: Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo SSL saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos (laurel, 2012).

NAT: La conversión de direcciones de red o NAT se desarrolló para resolver la falta de direcciones IP con el protocolo IPv4 (dentro de poco tiempo el protocolo IPv6 resolverá este problema) (laurel, 2012).

web-cache: Se llama caché web a la caché que almacena documentos web (es decir, páginas, imágenes, etcétera) para reducir el ancho de banda consumido, la carga de los servidores y el retardo en la descarga. Un caché web almacena copias de los documentos que pasan por él, de forma que subsiguientes peticiones pueden ser respondidas por el propio caché (Hector Rodolfo, MAYO 2009).

DMZ: La DMZ es una subred situada en el perímetro de la red. El límite explícito de DMZ hace su fácil para proporcionar servicios de alta velocidad en muchos aspectos. Un administrador del sistema puede obligar a las políticas de seguridad específicas en la zona de distensión e instalar herramientas de seguridad para la protección y detección. Por otro lado, estrictas protecciones de seguridad pueden estar relajadas en la DMZ. Para lograr un alto rendimiento, hardware especializado, en sintonía para la transferencia de datos, se puede colocar y compartida entre los usuarios (Carlos Diaz, SEPTIEMBRE 2013).

Firewall: Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad (Carlos Diaz, SEPTIEMBRE 2013).

Router: un router es un dispositivo hardware que permite la interconexión de ordenadores en red (laurel, 2012).

Switch: Un switch es un dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un PC, una impresora, la misma televisión, tu consola preferida o cualquier aparato que posea una tarjeta Ethernet o Wifi (laurel, 2012).

Servidor: Un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos (laurel, 2012).

RADIUS: (Remote Authentication Dial-In User Service). Sistema de autenticación empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. El usuario realiza una conexión a su ISP introduciendo su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y si es así autorizará el acceso al sistema del ISP.

8. LISTA DE REFERENCIAS

Soler,J.(2010). Seguridad informática capitulo dos: (Diseñando redes seguras) retrieved from https://sites.google.com/a/iesterrassa.cat/feines-del-segon-trimestre/noticias-de-intes/seguridadinformaticacapitulodosdisenandoredesseguras

Moreno,J. (2009). Bastionar una DMZ. Retrived from https://www.securityartwork.es/2009/11/10/bastionar-una-dmz/

Protocolo_ipsec. Retrieved from http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

Zwiky,E.D., Cooper, S., & Chapman, D. B. (2000) Building internet Firewalls (2.ed.ed.). Bejing u.a: O´Reilly.

G. Nakamoto, J. Schwefler and K. Palmer, "Desktop Demilitarized Zone," 2011 - MILCOM 2011 Military Communications Conference, Baltimore, MD, 2011, pp. 1487-1492. doi: 10.1109/MILCOM.2011.6127516

E. Dart, L. Rotman, B. Tierney, M. Hester and J. Zurawski, "The Science DMZ: A network design pattern for data-intensive science," 2013 SC - International Conference for High Performance Computing, Networking, Storage and Analysis (SC), Denver, CO, 2013, pp. 1-10.
doi: 10.1145/2503210.2503245

K. Jutawongcharoen, V. Varavithya, K. Lekdee, A. Chaichit and T. Sribuddee, "The implementation of the UniNet's research DMZ," 2016 International Computer Science and Engineering Conference (ICSEC), Chiang Mai, 2016, pp. 1-5. doi: 10.1109/ICSEC.2016.7859906

ISO. (2008). Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®). Retrieved from ISO: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716

Microsoft. (2016). Security Development Lifecycle. Retrieved from Microsoft: https://www.microsoft.com/en-us/sdl/

Cabrera, Luis F. (2015). WEB Services Atomic Transactions. V1. http://specs.xmlsoap.org/ws/2004/10/wsat/wsat.pdf

Gary McGraw, (2009), Software Security Building Security in http://www.swsec.com/resources/

Normas APA, (2016), Normas APA actualizadas 2016, http://normasapa.com/

ISO/IEC 15408-1:2009. Information technology – Security techniques - Evaluation criteria for IT security -- Part 1: Introduction and general model. https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en

El Tiempo.Ataques cibernéticos en Latinoamerica. (2016). http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataques-ciberneticos-en-latinoamerica/16383752.

Fondo Nacional de Garantías (FNG). (2008). Ley de Hábeas Data Ley 1266 de 2008. https://www.fng.gov.co/ES/Documentos%20%20Proteccin%20de%20Datos%20Personales/Manual%20Habeas%20Data.pdf

Régimen Legal de Bogota DC (1999). Decreto 1360 de 1999 Nivel Nacional. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10575

Colciencias.gov. (2009). GRINDTIC. Retrieved from http://scienti.colciencias.gov.co:8080/gruplac/jsp/visualiza/visualizagr.jsp?nro=000000000 09603

MINTIC Colombia (2016). Conpes de Seguridad Digital está acorde con estándares de la industria TI. http://www.mintic.gov.co/portal/604/w3-article-15463.html

A. C. Johnston & R. Hale. "Improved Security through Information Security Governance". Communications of the ACM, Vol. 52, No. 1, pp. 126-129, 2009.

J. M. Kizza. “Computer Network Security”. Springer, 2010.

C. A. Parra & H. Porras D. "Las amenazas informáticas: Peligro latente para las organizaciones actuales". Gerencia tecnológica Informatica, Vol. 6, No. 16, pp. 85-97, 2007.

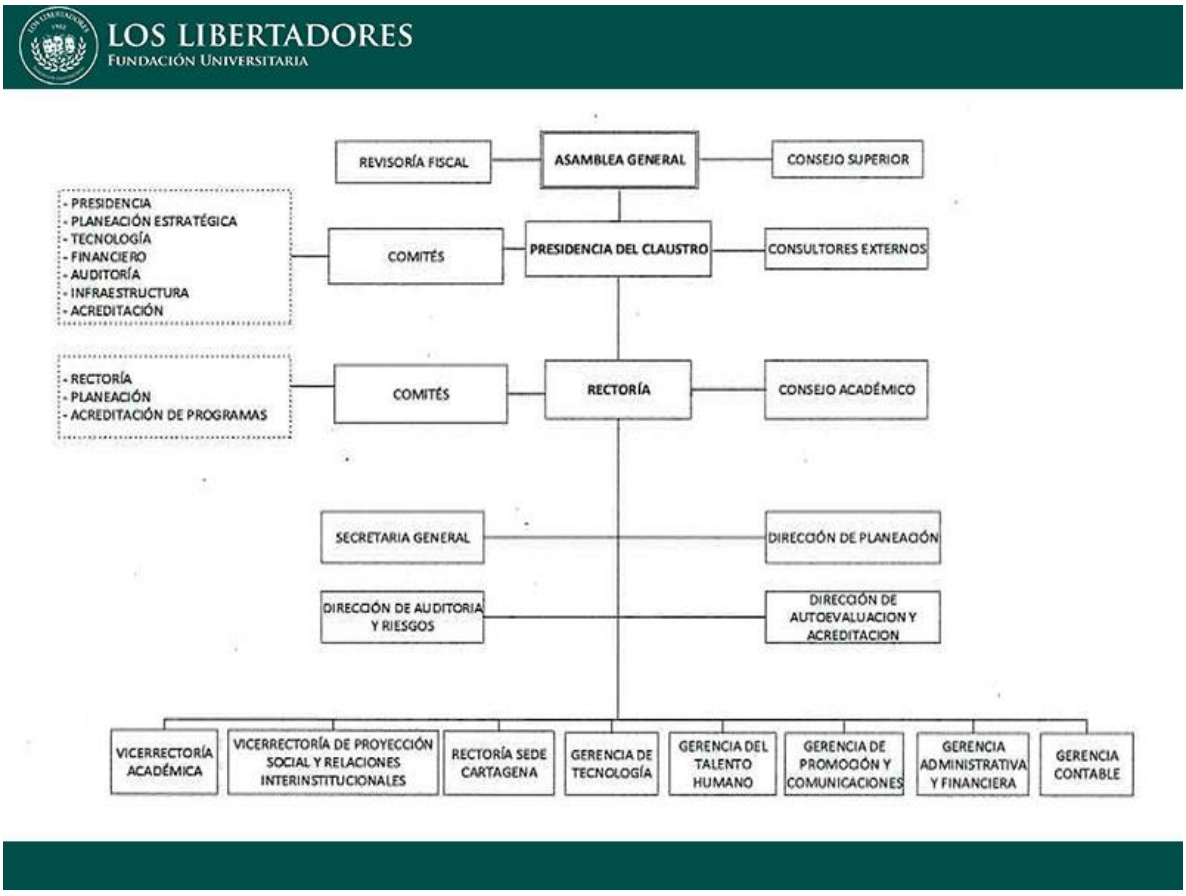
Robert J. Shimoski. Building DMZs for Enterprise Networks. Estados Unidos: Syngress, 2003.

Gary A. Donahue. Network Warrior. Estados Unidos: O´Reilly Media, 2007.

Cherie Amon. The Best Damn Firewall Book Period. Estados Unidos: O´Reilly Media, 2004.

Syngress. Building DMZs. Inglaterra: Syngless, 2003.

Anexos 1. Organigrama Fundación Universitaria Los Libertadores



Anexos 2. Cuestionario

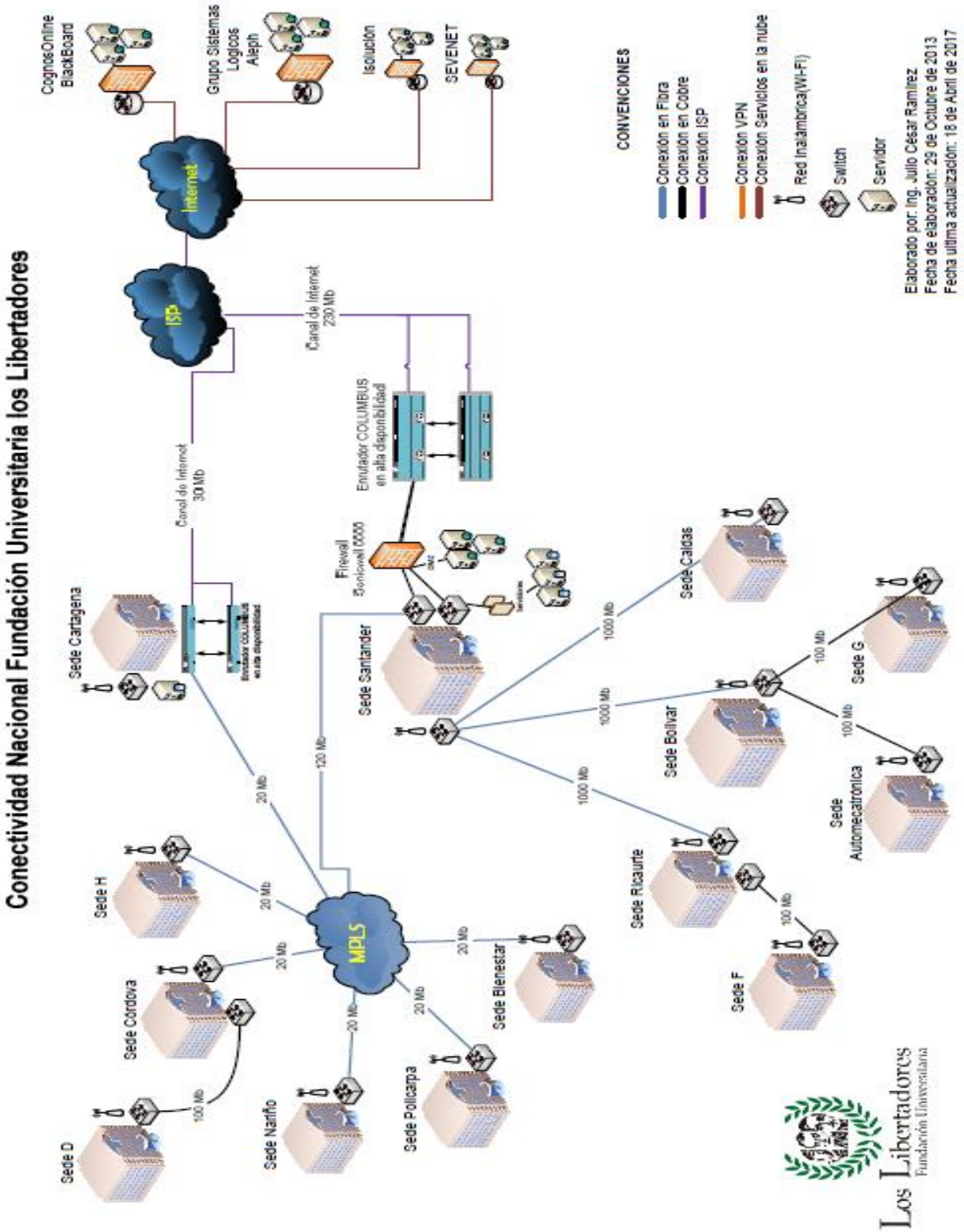
Entrevista para el levantamiento de información acerca de la seguridad implementada en la Fundación Universitaria Los Libertadores.

Estructura

1. ¿Cuantos canales de comunicación posee y que capacidad tiene cada uno?
2. ¿Cuántas sedes tiene la universidad y donde están ubicadas?
3. ¿Están interconectadas las sedes? ¿Y cómo se conectan?
4. ¿Qué tipo de arquitectura y topologías de red usa la Fundación Universitaria los Libertadores en sus distintas redes?
5. ¿Cómo esta segmentada la red?
6. ¿Cómo es la segmentación en las sedes?
7. ¿Cuantos Host, en promedio por cada red?
8. ¿cuántas redes Wifi existen?
9. pedir diagrama de red
10. ¿Qué tipos y cuantos firewalls, Swicht router, cuenta la universidad?
11. ¿Cuantos servidores tiene la universidad y en donde se encuentran alojados?
12. ¿Qué tipos de servidores y que servicios ofrece la Fundación Universitaria Los Libertadores?
13. ¿Manejan máquinas virtuales que tipo de sistema operativo usan?
14. ¿Qué Sistemas Operativos manejan a nivel de servidores en la Fundación Universitaria Los libertadores?
15. ¿Cuantos servidores están expuestos a internet?
16. existe una segmentación en los servicios o servidores que tiene la universidad (DMZ)
17. ¿Tienen implementas políticas de control de acceso?
18. ¿Hay registros de ataques a la red de la institución?
19. ¿Hay Logs (Registros) que los respalde hay seguimiento de los casos?
20. ¿Qué tipo de tráfico entrante de internet se puede considerar válida y cual no es válido?

21. ¿Se han realizado ataques fuera o dentro de la red hay Logs sobre esto?
22. ¿Cuáles son las medidas preventivas o reglas de seguridad, con las que cuenta la Fundación Universitaria Los Libertadores?
23. ¿Cómo se protege la Fundación Universitaria Los Libertadores de ataques dentro y fuera de su red?
24. ¿Qué controles de riesgos de seguridad de la información maneja la Fundación Universitaria los Libertadores?
25. ¿Cuáles son los permisos básicos en los distintos usuarios del sistema desde usuario a administrador?
26. ¿Qué tipo de información es la de mayor importancia o es la más sensible, y en qué tipo de servidor está alojada esta información?
27. ¿Qué Sistemas Operativos manejan a nivel de servidores en la Fundación Universitaria Los libertadores?
28. ¿Cuenta la Fundación Universitaria Los Libertadores con personal capacitado para procedimientos apropiados si ocurre un incidente de violaciones en la seguridad de la información que causen daños financieros o interrupción de los servicios?

Anexos 3. Topología de Red Fundación Universitaria Los Libertadores



Anexos 4. Listado redes inalámbricas Fundación Universitaria Los Libertadores

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN	FULL-ESTUDIANTES	FULL-ESTUDIANTES	Enabled
2	WLAN	FULL-DOCENTES	FULL-DOCENTES	Enabled
3	WLAN	FULL-ADMIN	FULL-ADMIN	Enabled
4	WLAN	FULL-INVITADOS	FULL-INVITADOS	Enabled
5	WLAN	Tablets Autoevaluacion	FULL-EVAL	Enabled
6	WLAN	FULL-ADMINISTRATIVOS	FULL-ADMINISTRATIVOS	Enabled
7	WLAN	---	---	Disabled
8	WLAN	FULL-CSENA	FULL-CSENA	Disabled
9	WLAN	LIBERTADORES	LIBERTADORES	Enabled

Anexos 5. Política de reglas del firewall aplicadas por defecto

	Servidor Web		Servidor de correo		Servidor SSH	Servidor FTP		Servidor DNS	Regla po defecto
General	Acceso web DMZ	Acceso web externo	Acceso mail DMZ	Acceso mail externo	Acceso ssh DMZ	Acceso ftp DMZ	Acceso ftp externo	Acceso dns	Denegació
Acción	Permitido	Permitido	Permitido	Permitido	Permitido	Permitido	Permitido	Permitido	Denegado
Desde	Interna DMZ Externa	Interna	Interna DMZ Externa	Interna	Interna Local Host	Interna Local Host DMZExterna	Interna DMZ	Interna Local Host DMZ	Todas la redes (incluida Local Host
Hacia	DMZ	Externa	DMZ	Externa	DMZ Externa	DMZ	Externa	Externa DMZ	Todas la redes (incluida Local Host
Horas	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre	Siempre
Protocolos	HTTP HTTPS	HTTP HTTPS	POP3 SMTP	POP3 SMTP	SSH	FTP	FTP	DNS	Todo el tráfico
Usuarios	Todos	Todos	Usuarios autenticados	Todos	Usuarios autenticados	Todos	Todos	Todos	Todos
Tipos de contenido	Todos	Todos	Todos	Todos	Todos	Todos	Todos	Todos	Todos