UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

ADMINISTRACIÓN DE SISTEMAS PARA EL INSTITUTO DE FISIOLOGÍA CELULAR

REPORTE DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A :

MICHAEL CRUZ ROJAS

DIRECTOR DE REPORTE:
DR. JOSÉ DAVID FLORES PEÑALOZA
2012

Datos del alumno

Apellido paterno	Cruz
Apellido materno	Rojas
Nombre	Michael
Teléfono	5441 3697
Universidad	Universidad Nacional Autónoma de México
Escuela	Facultad de Ciencias
Carrera	Ciencias de la computación
Numero de cuenta	303196547

Tutor

Grado	Doctor
Nombre	José David
Apellido paterno	Flores
Apellido materno	Peñaloza

Sinodales

Grado	Matematico
Nombre	José Luis
Apellido paterno	Torres
Apellido materno	Rodríguez

Grado	Matematico
Nombre	Salvador
Apellido paterno	López
Apellido materno	Mendoza

Grado	M. en C.
Nombre	Manuel Cristobal
Apellido paterno	López
Apellido materno	Michelone

Grado	M. en C.
Nombre	Jesús Alejandro
Apellido paterno	Juárez
Apellido materno	Robles

Datos del trabajo escrito

Titulo	Administración de sistemas para el Instituto de Fisiología Celular de la UNAM
Apellido paterno	88
Apellido materno	2012

A José Sánchez y Jorge Sánchez,
los grandes inventores de mi familia. Seguiré inspirándome con sus logros.

Índice general

Índice de figuras

Índice de algoritmos

Índice de cuadros

Lista de abreviaturas y definiciones[1]

IFC	Instituto de Fisiología Celular
dmesg	Comando de UNIX para listar los mensajes del núcleo
Servidor	Computadora que ofrece uno o más servicios
Servicio	Programa que se ejecuta dentro de un servidor
Appliance	Servidor y servicio dedicado específicamente para un solo propósito
VPN	Red privada virtual
HTTP	Protocolo usado para transferencias en la WWW
WWW	Sistema de hipertextos enlazados accesibles por Internet.
IMAP	Protocolo para dar acceso a mensajes de correo electrónico
SMTP	Protocolo para transferir correo electrónico
POP	Protocolo para obtener los mensajes de correo electrónico
LDAP	Protocolo para acceder a directorios de personas
DNS	Servicio para la resolución de nombres de dominios
NAS	Servidor dedicado a compartir su capacidad de almacenamiento por red
ARP	Protocolo de resolución de direcciones MAC
Dirección MAC	Dirección única de dispositivo de red
Ruteo	Función de buscar un camino en una red que posee gran conectividad
Fibra monomodo	Fibra óptica en la cual se propaga una sola frecuencia de luz
Fibra multimodo	Fibra óptica en la cual se propaga varias frecuencias de luz
Nodo	Dispositivo dentro de una red
Red tipo A	Red con 2^{24} nodos y con mascara de red 255.0.0.0
Red tipo B	Red con 2^{16} nodos y con mascara de red 255.255.0.0
Red tipo C	Red con 2^{8} nodos y con mascara de red 255.255.255.0
DMZ	Zona dentro de una red donde no existe seguridad alguna
MDF	Centro de conexión principal en toda la red
IDF	Centro de conexión intermedio entre el MDF y los nodos
Cable UTP	Cable utilizado para conectar dispositivos de red entre si
RAID 5	Arreglo de discos usado para evitar la perdida de datos
DoS	Ataque para denegar algún servicio informático
IEEE	Asociación encargada de la estandarización de protocolos
Widget	Programa para desplegar información de manera simple
KVM	Appliance que ofrece vía remota el teclado, video y ratón de un servidor
Appliance	Hardware dedicado específicamente a un objetivo
FPGA	Placa electrónica con un algoritmo programado en ella

Introducción

Prefacio

El Instituto de Fisiología Celular es un sitio de investigación científica en Ciudad Universitaria. Como su nombre lo dice este instituto se dedica a estudiar todo el mundo microscópico. Al ser muy recurrido en todo el mundo por sus aportaciones farmacéuticas e investigaciones que en lo general ayudan a la medicina, se debe de tener en cuenta que los servicios de cómputo que se ofrecen deban funcionar siempre en su totalidad.

En este instituto laboré dos años como administrador de sistemas. Aunque mi puesto fue solamente como administrador se deben de hacer otros trabajos como programar, diseñar e incluso en ocasiones apoyar en una investigación. En este reporte se dará a conocer como trabajé y que logros obtuve durante mi estancia en el instituto.

Se le llama administrador de sistemas a la persona que opera, corrige, mantiene, renueva y asegura el correcto funcionamiento de un sistema de cómputo y red[8]. A continuación se dará una breve introducción a cada uno de estos deberes y como los desarrollé en el instituto.

Operar — Se debe de tener conocimiento pleno de los sistemas operativos Windows, Linux y Mac OS X para poder corregir en cualquier contingencia y dar soporte a los usuarios.

Corregir — La corrección del mal funcionamiento esporádico en los sistemas es de vital importancia para garantizar una correcta operación de los servicios. Para corregir los sistemas se debe de tener control para el trabajo bajo presión, manejo fluido del sistema que se corregirá y confianza para ejecutar las acciones necesarias. Estos requisitos son los indispensables para poder garantizar el completo funcionamiento de los sistemas.

Mantener Es necesario observar los sistemas de forma casi ininterrumpida para estar al tanto de lo que se necesita corregir. En este ramo yo tengo tres formas diferentes de clasificar la observación de los sistemas las cuales son: alta prioridad, baja prioridad y red. Es necesario poner diferentes tipos de prioridad cuando una sola persona administra varios servicios.

Alta Se deben de estar observando continuamente. Si al resultar un problema en este tipo de sistemas se corrige inmediatamente, no es necesario invertir tanto tiempo en ellos. Para vigilar el buen funcionamiento de estos sistemas es necesario revisar las bitácoras el mayor tiempo posible, los reportes de sistema (dmesg) y su conectividad con dispositivos de apoyo. En el caso de errores físicos existen métodos para impedir la perdida de datos. Por ejemplo: mensajes de advertencia al correo electrónico, alarmas sonoras en los arreglos de discos duros y respaldos de los archivos más importantes del sistema.

La red también entra en los sistemas de alta prioridad. Para garantizar el optimo funcionamiento de la red, una de las cosas más importantes que se deben de verificar es el firewall para descartar ataques. En caso de que lo haya, se procede a su inmediata corrección que generalmente es el bloqueo y el reporte de la persona o programa que atacó. Muchas veces existen personas que no se dan cuenta del tipo de trafico que están generando su computadora y sin saberlo saturan la red entera. En este caso se notifica a la persona involucrada y se revisa su maquina para liberar carga en la red. En caso de un desperfecto en la infraestructura física se notifica a los ingenieros para repararlo.

Baja Estos servicios son los que se utilizan en ocasiones, por ejemplo un servidor de pruebas de programación. Este tipo de servidores se revisan periódicamente, más no constantemente. Al ser estos servidores de pruebas, el usuario se comunica directamente con el departamento de cómputo y notifica del error en el sistema para proceder a la inmediata reparación del servicio.

Renovar Este es el caso donde se toman decisiones para cambiar sistemas viejos y adquirir nueva tecnología. Esto se logra con un análisis exhaustivo de los precios y los beneficios que se pudieran obtener con cada una de las opciones a adquirir. Siempre se debe pensar en lo mejor para la institución y los usuarios.

Asegurar Para asegurar el correcto funcionamiento de todos los sistemas se tienen que ejecutar satisfactoriamente todas las tareas anteriormente mencionadas. Estas tareas son las básicas para lograr el objetivo para el cual fui contratado, que es tener un conjunto de sistemas estables trabajando en óptimas condiciones para los usuarios.

Desarrollar El trabajo de administración en un instituto de investigación deja muchos conocimientos enriquecedores. Apoyar una investigación de cualquier tipo da mucha satisfacción personal. La diferencia entre un administrador de sistemas que labora en un instituto de investigación y uno que labora por ejemplo en un centro bancario, no es solamente mantener a los servidores convencionales como correo, web o firewall; además se mantiene a los servidores de investigación los cuales tienen software muy particular que se debe de aprender a utilizar al menos al mínimo.
Este tipo de software regularmente requiere aplicar aprendizajes de algoritmos, programación, sistemas operativos y otras ramas de la carrera, muy especialmente algoritmos ya que en ocasiones se debe de apoyar al investigador en su proyecto informándole que la complejidad de su algoritmo es muy alta y se puede optimizar. Este tan solo es una experiencia de las muchas que he tenido en el instituto.

Estructura del reporte

El documento está estructurado en cinco partes que están organizadas en las siguientes categorías:

Administración de sistemas: todo lo referente a mi trabajo base y a la infraestructura de red del IFC. Por ejemplo: que tipo de software, hardware y redes manejé.

Mantenimiento y mejora de servicios: explico los problemas más comunes con sus respectivas soluciones y las labores extras de mejoramiento que realicé.

Desarrollo: las aportaciones que he brindado mejorar software ya existente o implementar nuevo para beneficio de los usuarios del instituto.

Conclusión: en la ultima sección hace una conclusión final del trabajo, así como también una justificación de por que este trabajo es suficiente para obtener el titulo de licenciado en ciencias de la computación.

Apéndices: En esta sección se incluye información adicional de la infraestructura del instituto.[1].

[1] Este trabajo servirá para complementar la documentación existente del instituto

Capítulo 1

Administración de Sistemas

En el Instituto de Fisiología Celular he desempeñado el trabajo de administrador de sistemas por dos años. Como se mencionó en la introducción en este trabajo se encarga de asegurar el correcto funcionamiento de un conjunto de sistemas para el servicio de la comunidad del IFC.

A continuación se mencionarán detalladamente las actividades más destacadas que realicé durante mi estancia en el Instituto de Fisiología Celular. Dividiré estas acciones en dos categorías:

- Sistemas y plataformas
- Administración de red, servicios y usuarios

1.1. Plataformas y sistemas

1.1.1. Plataformas

En un instituto de investigación científica, como lo es el de Fisiología Celular, siempre se encontrarán sistemas y arquitecturas de diferentes tipos. Las arquitecturas con las que he trabajado han sido desde computadoras comunes hasta especializadas en el análisis de cadenas de genes (FPGA).

¿Por qué toda esta amplia gama de plataformas?, la respuesta es muy simple. Generalmente las herramientas de investigación son unicamente funcionales para desempeñar las tareas para las que fueron construidas. Además, en muchas

ocasiones son también antiguas y ya no es fácil encontrar repuestos para esa máquina. Por ejemplo, computadoras con las que se controlan los microscopios digitales utilizados en los laboratorios es antigua porque el microscopio electrónico fue adquirido hace varios años, sin embargo el microscopio funciona bien aunque se le tiene que dar mantenimiento constante. Es por esa razón que esta tecnología sigue siendo útil.

Empezaré haciendo el reporte de las arquitecturas que utilicé dividiéndolas por tipo de sistema operativo, ya que resulta más fácil de comprender. Los sistemas operativos que abarcaré en esta sección serán Linux y Mac OS X.[3]

La mayoría de las arquitecturas con las que he trabajado han sido x86. La arquitectura x86 en sus diferentes versiones es la que predomina en el mundo de la computación. Sobre está arquitectura en la mayoría de los casos siempre esta implementada alguna distribución de linux, es por esta razón que dedicaré una sección de este reporte para dicha arquitectura y algunos sistemas operativos con los cuales trabaja. Para mayor información de las características completas de las plataformas puede consultar el apéndice B.

1.1.1.1. Linux

1.1.1.1.1. Servicios

Una de las máquinas más antiguas que he manejado con esta arquitectura ha sido una AMD Athlon. Ésta es una PC que tiene una servicio web para dar acceso a los datos de los usuarios del laboratorio de microarreglos[18]; almacena respaldos de los servidores y tiene el servidor DNS local del instituto[1].

He utilizado también servidores con los primeros procesadores Intel Xeon. Un ejemplo es el servidor que mantiene la base de datos de los estudiantes de posgrado[2], paginas web y ciertas aplicaciones programadas en Perl por el departamento de cómputo.

Además de usar servidores antiguos también he utilizado servidores con procesadores de ultima generación como, Intel Xeon de más de 8 núcleos. Por ejemplo el que sirve para virtualizar servicios[3]. En éste se encuentran varias máquinas importantes para el instituto como el servicio dedicado para compartir archivos en Windows (Samba) y varios servidores de prueba que utilizan los programadores del departamento de cómputo.

[1] Apéndice B.10
[2] Apéndice B.9
[3] Apéndice B.19

En los servicios esenciales tenemos generalmente procesadores Intel Xeon. Algunos de esos servicios esenciales son: correo, firewall, DHCP y web[4]. La velocidad y la memoria de estos servidores son muy variables, pero el procesador, la marca y el tipo de servidor son los mismos: Intel Xeon, memoria DDR2, servidores marca Dell. Todos funcionan con alguna distribución de Linux.

Se utilizan solamente dos distribuciones de Linux en el instituto, las cuales son Fedora y CentOS. Ambas distribuciones están basadas en RedHat por lo que la configuración es la misma. No hay necesidad de cambiar las distribuciones ya que todo esta automatizado y tenemos un repositorio de estás distribuciones para no bajar de la red varias veces las mismas actualizaciones.

1.1.1.1.2. Investigación

Para la investigación de alineamiento de cadenas de genes utilizamos tres tipos de arquitecturas diferentes. Estas arquitecturas son FPGA's, procesadores gráficos o GPU's y servidores de alto rendimiento.

Estas herramientas son bastante concurridas en las investigaciones del instituto, ya que el alineamiento de cadenas genéticas es una labor cotidiana en el IFC. El servidor FPGA tiene implementado el algoritmo Smith-Waterman y el algoritmo BLAST. Para hacer funcionar el FPGA se necesita un servidor esclavo y un maestro. En el servidor maestro esta físicamente el FPGA y el servidor esclavo procesa los datos arrojados por el FPGA y los almacena[5].

Estos servidores de alto rendimiento tal vez son de diferentes arquitecturas, sin embargo todos funcionan sobre una distribución del sistema operativo Linux y es por eso que se mencionan dentro de esta sección.

1.1.1.2. Mac OS X

1.1.1.2.1. Servicios

El servicio de VPN es indispensable para poder dar acceso a las terminales de los investigadores desde cualquier lugar del mundo. La VPN se ejecuta sobre una Mac Mini con Mac OS server X 10.4[6]. Esta Mac Mini tiene arquitectura Power PC. Se escogió una Mac Mini ya que se contaba con una de sobra en el departamento y se decidió montar el servicio ahí por ser muy fácil de hacerlo. Al no tener conectados más de 20 usuarios simultáneamente, este pequeño dispositivo a funcionado perfectamente para el objetivo señalado.

[4] Apéndices, B.2, B.11, B.8, B.1 respectivamente.
[5] Apéndice B.16
[6] Apéndice B.17

Debí de aprender completamente la configuración de Mac OS X Server para dar mantenimiento constante a esta maquina de vital importancia dentro de la comunidad del instituto. Por lo tanto es una más de las plataformas que aprendí a utilizar.

1.1.1.2.2. Investigación

El instituto cuenta con un servidor Mac para ejecutar un software de alineamiento de genes que utiliza el jefe del departamento de cómputo. La arquitectura es Power PC G4 y el sistema operativo es el mismo que utilizan las Mac Mini, es decir Mac OS server X 10.4[7].

La importancia de mencionar este servidor es que hay que estar al tanto de todos los movimientos que hacen los usuarios que tienen acceso a el para hacer sus pruebas. Debí de ayudar a los usuarios con información acerca de permisos y rutas de archivos para que sus experimentos funcionaran correctamente.

1.1.1.3. Otras plataformas

También debemos de hablar sobre la forma en la que se garantiza el servicio constantemente. Para esto utilizamos 4 UPS APC, dos de ellos son de 2.2 KVA y los otros dos son de 2.7 KVA. Ambos son rack tipo U2. Tenemos otro UPS rack 4U Dell de 2.7KVA. Con todo esto garantizamos el servicio constante en el instituto por aproximadamente media hora sin energía eléctrica; esto es suficiente ya que el instituto cuenta con generadores a gasolina, los cuales entran a los 10 segundos después de la falta de suministro energético.

Estos servicios no requieren configuración remota ya que en sus paneles está la información completa de la carga del sistema y de su estado, es decir sí están funcionando con baterías o a corriente.

1.1.2. Sistemas

En la actualidad existe una gran variedad de sistemas operativos. Para la administración en el IFC generalmente se utilizó solo un tipo de sistema operativo. En lo particular siempre opte por instalar sistemas basados en RedHat. Básicamente porque mi experiencia con los sistemas basados en Debian no fue nada buena, estos terminaban por ceder ante todo el tráfico que pasaba por los servicios. ¿Por qué opté por esos sistemas?. Definitivamente no es favoritismo. Opté

[7] Apéndice B.12

por esos sistemas porque RedHat fue diseñado para dar servicios de red por lo que las configuraciones y ubicaciones de archivos me parecen más cómodas, además las herramientas nativas nos parecen más estables y aptas para este trabajo.

Es cierto que cualquier distribución de Linux puede echar a andar algún servicio de cualquier tipo, sin embargo a mi parecer y experiencia, la diferencia está completamente en la cantidad de usuarios que estén utilizando el servicio al mismo tiempo.

Utilizando estos sistemas basados en RedHat no se ha colapsado algún servicio por causa de exceso de trafico. [8] Por lo que en general el 90 % de los servidores en el instituto utilizan una distribución basada en RedHat.

1.1.2.1. Sistemas de cómputo principales

Los sistemas principales son los que utilizamos para hacer funcionar la mayoría de los servicios, ya que mantienen cierta homogeneidad entre todos, es decir todos son parecidos en la mayoría de los aspectos.

En el instituto los servicios críticos están montados sobre el sistema operativo CentOS. No se instala el servicio X en estos servidores porque no requieren de interfaz gráfica. Para los servicios que requieren que se despliegue una interfaz gráfica utilizamos Fedora. [9]

Otro tipo de sistemas con los que el instituto cuenta es Mac OS X. El IFC cuenta con 3 Mac Server que tienen el sistema operativo Mac OS X Server 10.4 instalado. El sistema Mac es similar a Linux, pero como se sabe, la interfaz gráfica y la forma de configurarlo es muy diferente. Mac OS X Server es similar a la Desktop de Mac OS, con la diferencia de que existe un panel adicional con todos los servicios que están en funcionamiento. Este panel ofrece toda la información de los servicios de serie integrados al sistema, desde configuración hasta bitácoras.

1.1.2.2. Sistemas de cómputo especializados

Los sistemas especializados son los que no tienen características, instrucciones, ambiente de trabajo, etc., que se parezca a los típicos o entre ellos mismos, es decir cada fabricante hace su sistema a su manera.

[8] Se hablará más de esto en la sección de mantenimiento.

[9] Las computadoras del personal de cómputo siempre trabajan con la versión de Fedora más actual.

El sistema especializado más importante que he manejado ha sido Barracuda[10], el cual es un servicio utilizado como filtro de correo electrónico y es muy útil por filtrar los correos ayudándose de una base de datos almacenada en los servidores de Barracuda Networks. Este sistema es muy preciso al separar el correo electrónico deseado del no deseado.

También he manejado los sistemas de Aberdeen[11] que están instalados en los NAS de la misma marca. Este sistema es práctico porque se puede crear un nuevo volumen de almacenamiento en pocos segundos y compartirlo por alguno de los protocolos de transferencia de archivos que tiene implementado el sistema de serie.

El sistema de los switches Dell se especializa en la configuración de la capa de red[2]. Las opciones que manejan son relacionadas al tema de tablas ARP, control de flujos, redes virtuales, administración remota de la red; entre otras cosas que son muy técnicas de redes. Es en este sistema donde aplico toda la teoría aprendida en la materia de redes de computadoras.

Muchos de los dispositivos con los que trabaje en el instituto fueron nuevos para mi, por lo que enriquecieron mis conocimientos de sistemas aprendidos en la carrera. Esto me dio un panorama más amplio sobre qué tipo de software y hardware debería utilizar si me pidieran implementar una red de este tipo o más grande, porque en el tiempo que he estado administrando esta red, se debe de pensar continuamente en implementar nuevas ideas. Por esa razón antes de hacer algún pedido realizo un análisis del hardware o software que más convenga a la institución.

1.2. Administración de red, servicios y usuarios

En esta sección se hablará de cómo está conformada la infraestructura de telecomunicaciones en el IFC, desde la red hasta los servidores y los servicios que prestan dichos servidores. Es importante mencionar esta parte por el hecho de que se debe de tener al menos una idea global de qué tipo de red administraba para demostrar que necesité de bastantes conocimientos en redes, programación, sistemas operativos, seguridad y otros aspectos que cubren el perfil de licenciado en ciencias de la computación, para mantenerla funcionando.

Esta parte además da una breve idea de cómo está constituida la infraestructura del instituto para continuar con los temas de mantenimiento, mejora de servicios y desarrollo.

[10] Apéndice B.14
[11] Apéndice B.3, B.4 y B.5

Dividiré este sección en tres partes para facilitar el procesamiento de información, ya que son varios segmentos los que se tocarán para adquirir el panorama general de la infraestructura del instituto.

1.2.1. Red

La red del Instituto de Fisiología Celular es bastante compleja y amplia. Se extiende por los 4 edificios del complejo, llegando a cada uno de los laboratorios y pasillos que existen, esto con el fin de garantizar siempre alguna forma de conectarse a Internet. Por la alta demanda se debe de tener una buena distribución para evitar las sobrecargas en los diferentes segmentos de la red.

Para evitar la sobrecarga tenemos una buena conexión hacia el exterior, la cual principalmente está constituida por un cable de fibra óptica monomodo hacia el IIMAS. Éste nos provee de una conexión a Internet únicamente limitada por la velocidad del proveedor de Internet de la UNAM que en nuestro caso tenemos un tope máximo de 400mbps y la que en horas de alto tráfico nos da aproximadamente 1500kbps por usuario[12]. La variación depende de la época. Por ejemplo, en finales de semestre la velocidad llega a disminuir drásticamente por la alta demanda de toda la comunidad del instituto. El caso contrario es que en todo el semestre y obviamente las vacaciones el IFC cuenta con un muy buen ancho de banda. Por lo general las variaciones en la red dependen de los usuarios, no existen servidores que cronológicamente consuman ancho de banda excesivo.

A continuación se describirá la topología de la red del instituto. Será descrita por las siguientes partes: no homologada y homologada.[13].

1.2.1.1. Segmento homologado

Existen dos segmentos homologados en el instituto. Uno de ellos pertenece al edificio principal y el otro pertenece al edificio de neurociencias. Cada uno tiene asignado el rango de IP's 132.248.16.0/24 y 132.248.212.0/24 respectivamente.

1.2.1.1.1. Edificio principal

En este segmento se encuentra la mayor parte de servicios en el IFC y la principal conexión a Internet del instituto. Esta conexión está vinculada directamente al IIMAS por fibra óptica.

[12] Mediciones tomadas en días de exámenes finales y primeros días de semestre.
[13] Estos segmentos con sus aplicaciones se presentan en el Apéndice A.

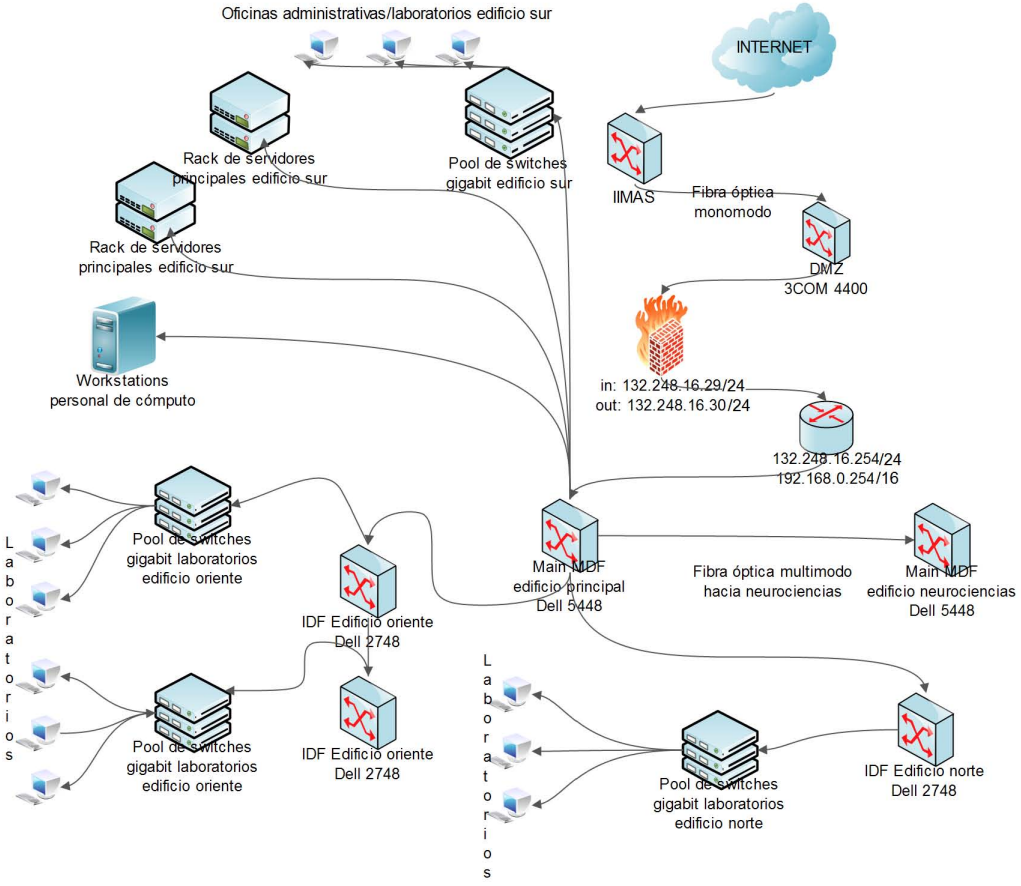
La fibra óptica está conectada a un switch gigabit de 48 puertos 3COM 4400 el cual funciona como zona DMZ. Este switch se conecta hacia el MDF Dell 5448 que será llamado de ahora en adelante MDF principal. En el se encuentra conectado el firewall y los servicios principales del instituto como DHCP, Web, Correo, etc. En el diagrama se muestra primero la fibra conectada al firewall y luego al ruteador, se menciona así ya que el orden mostrado en el diagrama es el físico no el lógico. Es buen ejercicio conectar los diferentes dispositivos así ya que se reserva un switch solamente para los servicios más importantes [8].

Al MDF principal se conectan varios switches Dell 5448 de 48 puertos los cuales proveen de conexión a todos los laboratorios del edificio sur y a las oficinas administrativas del instituto. Además, a este MDF principal están conectados los IDF del edificio oriente, norte y el edificio de neurociencias. Este ultimo está conectado también por fibra óptica, de esta manera se crea un enlace directo y se garantiza una conexión fluida entre los dos edificios principales que están alejados entre si por aproximadamente 100 metros.

Los IDF oriente y norte trabajan con switches Dell gigabit 2748 de 48 puertos. El edificio oriente cuenta con dos de estos switches, mientras que el edificio norte cuenta tan solo con uno.

De todos los IDF se desprenden otros switches de 24 puertos o menos para cada uno de los laboratorios, los cuales son aproximadamente 30 por edificio. El modelo de estos switches puede variar, ya que entre los IDF y MDF en general se mantiene una velocidad de 1000mb, sin embargo los que están en los laboratorios pueden ser switches de velocidad 1000mb o 100mb; así como también puntos de acceso inalámbricos b/g/n. En la Figura 1.2.1 se encuentra un diagrama detallado de la topología del edificio principal.

Figura 1.2.1: Diagrama de la distribución de la red en el edificio principal[1].



1.2.1.1.2. Neurociencias

El edificio de neurociencias es un edificio de 3 pisos y es más pequeño que el principal, sin embargo puede ser totalmente independiente de este. Es por eso que tiene su propia salida a Internet y su propio segmento asignado, pero para facilitar la administración, todos los usuarios del edificio de neurociencias salen por el edificio principal a Internet y el hilo dedicado de neurociencias se reserva unicamente para la VPN y las videoconferencias. Se configuró así ya que la salida a Internet de neurociencias tiene un ancho de banda de 100mbps y se satura demasiado para mantener a todo un edificio.

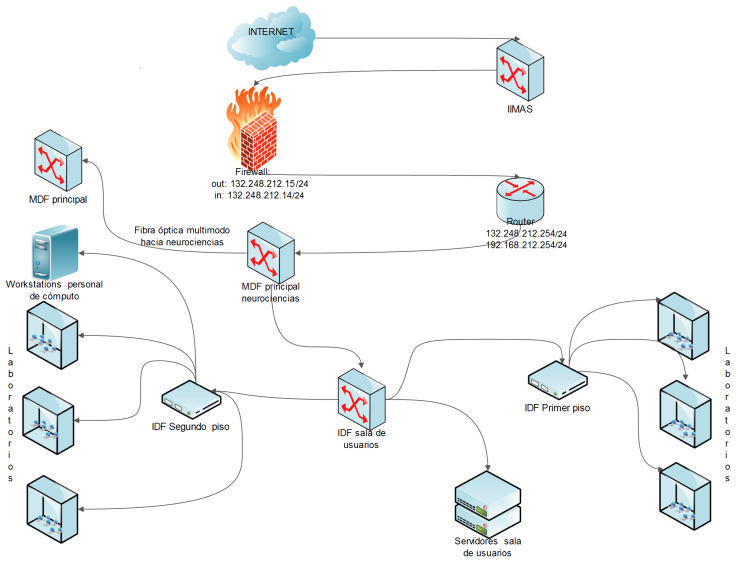
En el edificio de neurociencias se desarrollan conferencias durante todo el semestre, por lo que existen varias direcciones reservadas para el hardware dedicado a la transmisión de video en vivo. A este hardware no he tenido acceso directamente ya que lo maneja la encargada de ese edificio, sin embargo es buen ejercicio mencionarlo para crear un mapa completo de los servicios albergados en este edificio y justificar la configuración.

La conexión de neurociencias a Internet llega por cable UTP desde el IIMAS hacia un switch de 100mbps en el cual están conectados servidores como el firewall del edificio y la VPN. A este switch se conectan dos switches Dell 5448. Uno de ellos tiene la conexión por fibra óptica hacia el edificio principal y el otro distribuye la red a los IDF de cada piso del instituto. De cada IDF se distribuye un hilo a los switches de cada laboratorio y punto de acceso inalámbrico en distintas zonas.

En general la red del edificio de neurociencias es más simple ya que los únicos servicios que alberga son la VPN y el firewall de ese edificio.

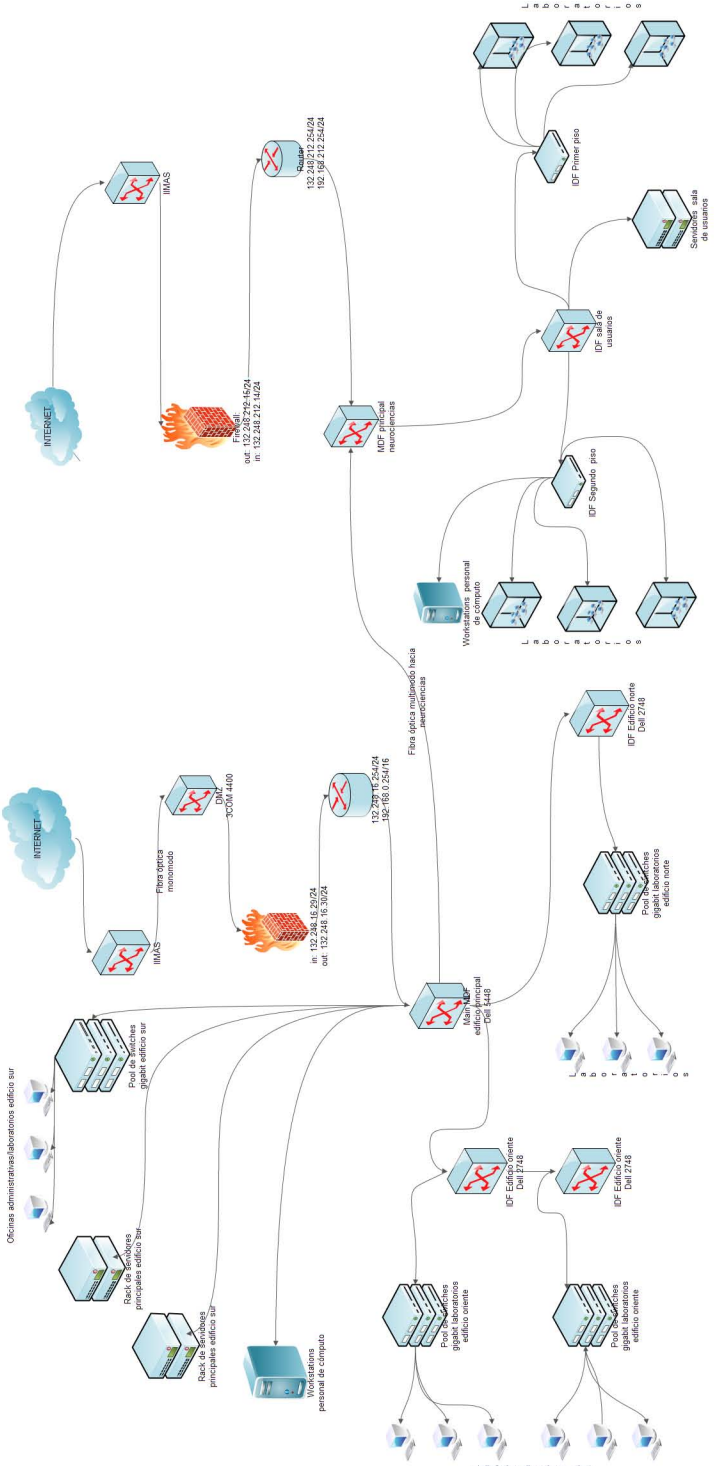
En la Figura 1.2.2 se muestra la topología del edificio de neurociencias.

Figura 1.2.2: Diagrama de la distribución de la red en el edificio de neurociencias[1].



Después de haber presentado la topología de red del instituto edificio por edificio, a continuación presento el diagrama completo de la red del Instituto de Fisiología Celular en la Figura 1.2.3.

Figura 1.2.3: Diagrama de la infraestructura de red del IFC[1].



1.2.1.2. Segmento no homologado

Está conformado por una red del tipo B[2]. En esta red es donde le damos a los usuarios una IP para poderse conectar a los servicios del instituto y para salir a Internet. Además, tenemos ciertos dispositivos listados ordenadamente en alguno de los 254 subsegmentos del tipo C, esto es un segmento para cada tipo de dispositivo. Algunos ejemplos de dichos dispositivos son impresoras, switches, puntos de acceso, etc. El segmento no homologado está dado por la red 192.168.0.0/16.

Este segmento particularmente es simple ya que no existe una división entre edificios como en el segmento homologado. El único motivo por el cual este segmento existe, es para proporcionar direcciones dinámicas al personal del instituto en general. Existen 4 segmentos tipo C cada uno de ellos está destinado a dispositivos del mismo propósito, como impresoras, switches, servicios para compartir archivos de Windows y otros más que no son trascendentales pero es necesario mencionarlos, ya que una red del tipo C no es suficiente para todo el personal.

En esta red tenemos 3 segmentos del tipo C[14], para ofrecer mediante el servicio DHCP una IP para conectarse a Internet, lo cual da la idea de lo grande de la red y lo difícil que es mantenerla funcionando, en el aspecto lógico, con una sola persona.

1.2.2. Servicios

En el instituto se ofrecen los servicios de correo electrónico, almacenamiento web, almacenamiento de archivos personales, acceso a Internet inalámbricamente y alámbricamente en cualquier parte del instituto, computadoras dedicadas a la investigación, VPN, entre otras. Sin embargo detrás de todos estos servicios que se ofrecen a la comunidad existen maquinas a las que los usuarios no pueden acceder pero que son vitales para el funcionamiento de todos los servicios.

A continuación haré un desglose de todos estos servicios para explicar desde el fondo como están formados cada uno de ellos. También se hablará de los servicios personalizados para algunos investigadores.

1.2.2.1. Correo electrónico

El correo electrónico en el instituto es la herramienta más importante para la comunidad. Si esta herramienta falla los usuarios empiezan a llamar inmediatamente a cómputo reportando la interrupción del servicio.

[14] Más de 750 nodos.

El correo electrónico está distribuido en varios servidores: almacenamiento, correo de salida, correo de entrada, firewall de correo electrónico, webmail, Zimbra y Gmail.

La distribución de las cuentas de los usuarios está dada de la siguiente forma.

- Correo principal (inmail, outmail, antispam, webmail): en este conjunto de servidores se encuentran los investigadores, administrativos y técnicos académicos. El dominio de este servicio es ifc.unam.mx
- Zimbra: en este servidor se encuentra la nueva versión de correo electrónico. El dominio de este servicio será ifc.unam.mx al dar de baja el servidor principal.
- Gmail: Solo estudiantes. El dominio de este servidor es email.ifc.unam.mx

1.2.2.1.1. Correo de entrada

Mail, como se llama el servidor principal, aloja el correo de entrada, en el están habilitados los puertos POP e IMAP, siendo este último el principal protocolo para que los usuarios lean su correo electrónico. Este servidor tiene la dirección IP 132.248.16.2, está registrado en el DNS de la UNAM con el nombre de mail.ifc.unam.mx y tiene el alias de inmail.ifc.unam.mx para hacer más fácil la configuración del correo electrónico a los usuarios.

Sendmail es el encargado de manejar el correo electrónico y lo almacena con la siguiente organización: en la carpeta /var/spool/mail están los correos nuevos, es decir la bandeja de entrada. En la carpeta `/home/usuario` se almacenan todas las carpetas de los usuarios[9].

En ocasiones, para aminorar la carga de trabajo para las lecturas del disco duro, transfiero los correos más antiguos de las carpetas bandeja de entrada, basura y enviados hacia una carpeta "`prefijo-ifc-año-semestre`", donde prefijo es el nombre de la carpeta de donde provienen los correos (inbox, trash, sent), año es el año en curso a cuatro dígitos y semestre a un dígito.

La autenticación en muchos servicios se hace en mail.ifc.unam.mx, ya que en este servidor se guardan todos los usuarios del instituto y sus respectivas contraseñas. Para autentificar a los usuarios que acceden a la VPN del edificio de neurociencias se utiliza RADIUS.

El servidor mail.ifc.unam.mx está conectado hacia un NAS de 4TB de almacenamiento en RAID 5 por medio de un switch independiente, para garantizar un buen ancho de banda para este servicio. En este NAS se guardan absolutamente todos los correos de los usuarios, así como información de configuración para el servidor de webmail.

1.2.2.1.2. Correo de salida

Para enviar correos electrónicos existe otro servidor independiente, con el fin de aminorar la carga entre tarea y tarea. El servidor está registrado en el DNS de la UNAM como outmail.ifc.unam.mx, con la IP 132.248.16.18. Este servidor no tiene autenticación de ningún tipo y utiliza MailScanner para enviar y revisar los correos salientes. Además de manejar el correo de salida también nos sirve como DHCP, del cual hablaré en la sección de Internet.

1.2.2.1.3. Firewall de correo electrónico

El firewall que tenemos es uno de los pocos servicios que administré que no son software libre. Este servidor es de la marca Barracuda modelo 300 y es indispensable para el servicio de correo.

Más del 50 % del correo electrónico que recibimos en el instituto es spam, por lo que para no saturar nuestros servidores y el ancho de banda necesitamos algo como Barracuda, que sea realmente robusto para recibir aproximadamente 10 mil correos al día y separar el correo no deseado. En la Figura 1.2.4 y la Figura 1.2.5 se muestran gráficas con las estadísticas del correo de entrada por hora y por día, respectivamente.

Figura 1.2.4: Estadística de correo electrónico por hora.

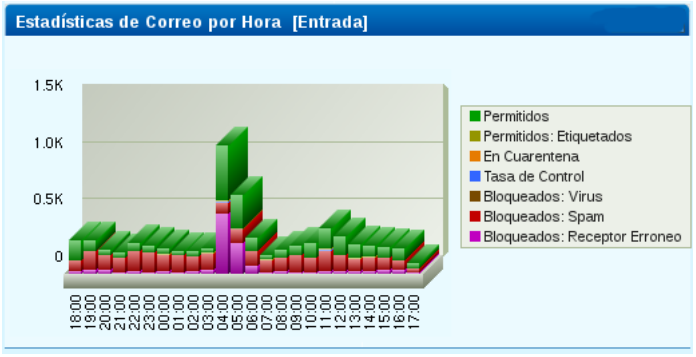
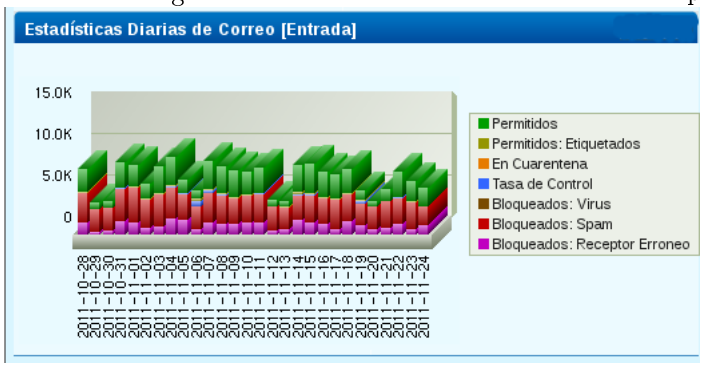


Figura 1.2.5: Estadística de correo electrónico por día.



El nombre con el que está registrado el barracuda en el DNS es gw-smtp y tiene la IP 132.248.16.45, teniendo éste prioridad 10 en el DNS, es decir, es el principal receptor de correo electrónico en el instituto[10]. Al comprar el Barracuda también compramos una suscripción a las bases de datos de spam de Barracuda Networks, las cuales son indispensables para separar adecuadamente el correo no deseado.

1.2.2.1.4. Webmail

Es el servidor que sirve de interfaz gráfica entre todos los servicios anteriores y el usuario. Tiene instalado Horde, que es muy útil para saber quienes son las personas que envían spam dentro del instituto o para conocer quien pudo haber entrado a cierta cuenta de correo electrónico sin autorización, ya que en este servidor se guardan todas las bitácoras con toda la información de las IP's, nombres de usuarios, hora y qué correos enviaron los usuarios afectados. De esto se hablará más adelante en el capítulo de mantenimiento.

1.2.2.1.5. Zimbra

Al darme cuenta de que el manejo del actual servicio de correo electrónico no era ágil, comencé a instalar Zimbra en un servidor robusto como nueva alternativa de correo electrónico. Este servidor ya está terminado y configurado para recibir todo el correo, solo se necesitan cambiar las IP's entre el servidor de correo actual y el de zimbra para ponerlo en producción.

La razón por la cual no lo he llevado a producción es que algunos investigadores no aceptan el cambio al nuevo servidor, ya que están familiarizados con el correo actual.

Este servidor cuenta con servicios que antes no contábamos como IMAPS, POPS, LDAP y una interfaz web basada en Ajax. Todo está en un mismo servidor, de esta manera habrá un ahorro energético considerable y eficiencia en la administración de este sistema.

Para que este servidor estuviera listo se tuvo que realizar una serie de transformaciones del servidor anterior a este nuevo. Esto se debe a que la forma de almacenar información en Zimbra es por medio de bases de datos y en el actual servidor de correo electrónico la mayoría de los correos se guardan en archivos[10].

Utilicé imapsync para realizar las transformaciones del correo electrónico y de las libretas de direcciones. Para migrar a los usuarios utilicé una serie de scripts aprovechando el CLI de Zimbra. De esto se hablará más a fondo en el capítulo de mejoramiento de sistemas.

Al finalizar pude notar que toda la información almacenada en Zimbra ocupó menos espacio que en el servidor de correo actual, por lo que hubo una importante optimización de espacio. Se libero aproximadamente un tercio del espacio original. Esto debido a que Zimbra almacena la información en una base de datos comprimida.

1.2.2.1.6. Gmail

Anteriormente, cuando empecé a trabajar en el instituto, todas las cuentas de los usuarios, incluyendo a los estudiantes, se alojaban en el servidor principal. Sin embargo, al darme cuenta de que los estudiantes son los que más reciben y envían spam, inmediatamente noté que ellos saturaban la red drásticamente. Otra cosa sobresaliente es que sus cuentas son atacadas muy frecuentemente para robar su identidad, supongo que por suscribirse en foros y bajar archivos de manera ilegal. Por estas razones decidí migrar a los estudiantes a una plataforma diferente para no perjudicar a los investigadores por el exceso de trafico.

Decidimos migrarlos a Gmail porque la mayoría de la gente está familiarizada con este servicio de correo, además de ser un sistema robusto, de fácil administración y con un gran espacio de almacenamiento.

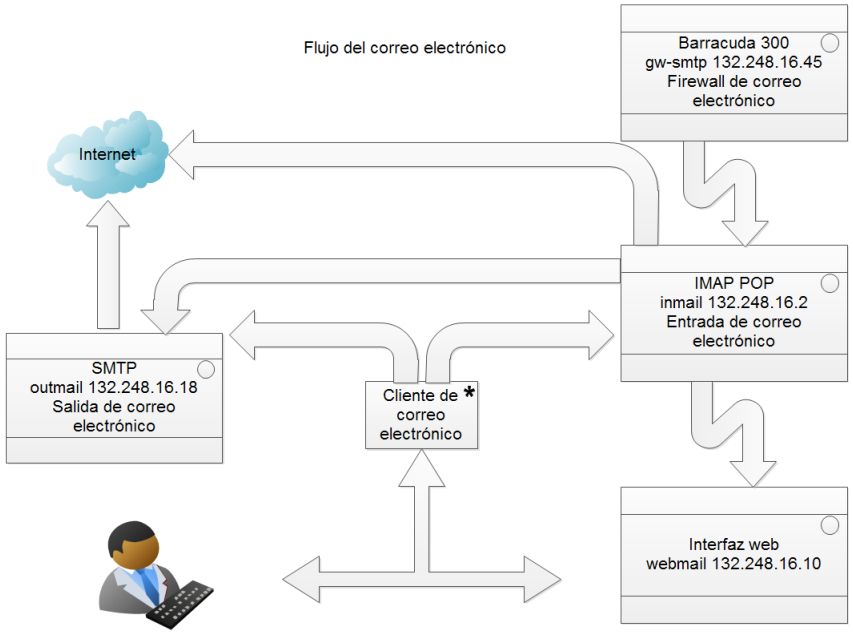
Lo interesante de migrar a Gmail fue transferir todos los correos electrónicos a los servidores de Google. Para realizar esta tarea utilicé la herramienta imapsync, que está programada en Perl y tiene bastantes opciones para la migración de servidores.

Migré a los estudiantes creando un archivo CSV con el nombre de usuario que tenían en mail.ifc.unam.mx y una contraseña aleatoria que los estudiantes deberían cambiar eventualmente, al iniciar sesión por primera vez en su nueva

cuenta de Gmail. El dominio de este nuevo correo electrónico cambió, ya que no se podía tener el mismo dominio del servidor principal con los servidores de Gmail.

Una pregunta muy importante la cual se debe responder es ¿por qué solo migré a los estudiantes?. La decisión de migrar solo a los estudiantes a Gmail fue que los investigadores manejan información muy importante dentro de sus correos, en muchas ocasiones patentes suyas. El ofrecer esta información a Gmail implicaría enriquecer a Google con información que tiene derechos de autor e innovaciones tecnológicas. La decisión tiene que ver con privacidad y un poco de nacionalismo. La figura 1.2.6 muestra el flujo de correo electrónico en el IFC.

Figura 1.2.6: Diagrama del flujo del correo electrónico.



1.2.2.2. Almacenamiento web

El servicio Web del Instituto de Fisiología de Celular es muy concurrido por tener paginas con los perfiles personales de los investigadores y por alojar varios servidores web virtuales. Para el servicio web solo se utiliza un servidor con PHP, MySQL y Apache.

En este servidor están almacenadas algunas páginas extras, además de la página oficial del instituto. Algunos ejemplos son: la Sociedad Mexicana de Bioquímica;

la unidad de microarreglos del instituto; experimenta, que es una página de divulgación científica dirigida por el Dr. Francisco Fernández; paginas sobre las investigaciones del Dr. Alfredo Torres, Dr. Roberto Coria, la Dra. Xochitl Pérez y varias páginas de congresos nacionales e internacionales, como el tercer Congreso Mundial de Cronobiología.

Además de servicios web de almacenamiento, también se ofrecen transmisiones de las conferencias realizadas en los auditorios del instituto y un servicio de podcast de las mismas conferencias; acceso al software desarrollado en el institutom como NeuronGrowth, que cuantifica de manera semiautomática patrones de crecimiento neuronal a partir de videos; HERMES que sirve para buscar, recuperar y almacenar artículos que están en varias bases de datos; GenArise para el análisis de datos de microarreglos de ADN; JAMMING que es una interfaz gráfica de redes de mínima interacción programada en Java, y por último, acceso a la herramienta EMBOSS que, es una suite de herramientas bioinformáticas.

La pagina web principal del instituto muestra las noticias más recientes sobre el trabajo de los investigadores. Estas noticias se agregan a la cuenta de Twitter del instituto, al mismo tiempo de publicarlas en la página web. Para desplegar las noticias utilicé el widget oficial y el servicio de ligas cortas de Twitter. Tomé la decisión de utilizar Twitter ya que Google indexa los estados de los usuarios, por lo que de esta forma la difusión de la ciencia es más eficiente por el creciente auge e impacto de las redes sociales en la vida cotidiana. Se hablará más de este tema en el capítulo de desarrollo.

También se cuenta con una Intranet la cual ofrece servicios solamente para las personas de la comunidad. En Intranet podemos encontrar: guías de configuración para los diversos servicios, formatos para realizar tramites, las listas de correo del instituto y la base de datos de los estudiantes.

Cualquier persona en el instituto que lo requiera puede pedir algún tipo de servicio web. En general se solicita almacenamiento y publicación de alguna pagina web.

Muchas veces, además de administrar las paginas web también les debo de dar mantenimiento y actualizarlas constantemente, por lo que debo de tener conocimientos en programación web, en especifico en PHP ya que es con lo que las páginas del instituto están construidas.

Debo también de conocer muy bien el funcionamiento del servicio Apache porque muy frecuentemente agrego nuevos alias y host virtuales al archivo de configuración, además de estar monitoreando el trafico en ese servidor por los constantes intentos de ataques DoS.

La prioridad de esté servidor es muy alta, por lo que hago respaldos cada semana de los archivos importantes, como la base de datos y todas las páginas web. A este servidor no se puede acceder vía SSH desde otra parte que no sea dentro del instituto. Tengo bloqueados todos los puertos al exterior para evitar intrusiones.

1.2.2.3. Acceso a Internet

Como se ha mencionado antes, el acceso a Internet en el instituto está garantizado desde cualquier zona en los múltiples edificios. Alámbrica o inalámbricamente, la comunidad siempre se podrá conectar a Internet para poder acceder a los servicios del instituto en linea.

Para el funcionamiento de la red se necesita más que un cable UTP conectado a un switch. Son varios dispositivos los cuales están interconectados para dar una IP al cliente (DHCP), dar una ruta de salida a Internet (Gateway y firewall) y resolver nombres de dominios (DNS)[1].

Para explicar el funcionamiento global de las conexiones en el instituto pasaré desde el nivel más bajo que son los switches hacia el IIMAS, hasta el usuario mismo.

El usuario primero se debe conectar a cualquiera de los puntos de acceso del instituto. Los puntos de acceso alámbricos e inalámbricos están conectados a un switch en los laboratorios. Lo primero que la computadora del usuario hace al conectarse a la red del instituto es tratar de obtener una dirección IP.

1.2.2.3.1. DHCP

El servidor DHCP otorga direcciones en los rangos 192.168.16.0/24, 192.168.17.0/24 y 192.168.212.0/24. Estos rangos son los que se utilizan para las personas que no necesitan una dirección estática, como estudiantes o invitados. Además de ofrecer direcciones a invitados o estudiantes, el DHCP también se encarga de asignar las direcciones estáticas para hacer más sencilla la configuración de los dispositivos.

Observar este servicio constantemente es de vital importancia. Para observar que todo esté funcionando correctamente se deben revisar las bitácoras del servicio de manera regular. Los errores más comunes en este servicio son que los puntos de acceso inalámbrico ofrezcan direcciones diferentes a las permitidas causando que los usuarios no puedan conectarse a Internet por choques de direcciones o configuraciones erróneas.

Otro tipo de error de DHCP sucede cuando algunos puntos de acceso empiezan a transmitir paquetes SNMP que en broadcast. Este problema ocasiona que consuman todo el ancho de banda y sea imposible salir a Internet en el segmento[15] que esté conectado el punto de acceso problemático.

[15] Los segmentos son el edificio principal o el edificio de neurociencias.

Este servidor de DHCP comparte su espacio físico con el servicio de correo saliente, ya que DHCP no requiere tanto poder de cómputo en sus tareas habituales. Por lo que la dirección del servicio DHCP es la misma que la del correo saliente, que es 132.248.16.18.

1.2.2.3.2. Gateway y Firewall

Después de que el cliente haya obtenido una IP por medio del servicio DHCP, lo siguiente es obtener las rutas de salida a Internet. En este caso, el firewall y el gateway comparten el mismo espacio físico. La dirección del gateway es 132.248.16.254, en su modalidad homologada, y 192.168.0.254 en su modalidad no homologada.

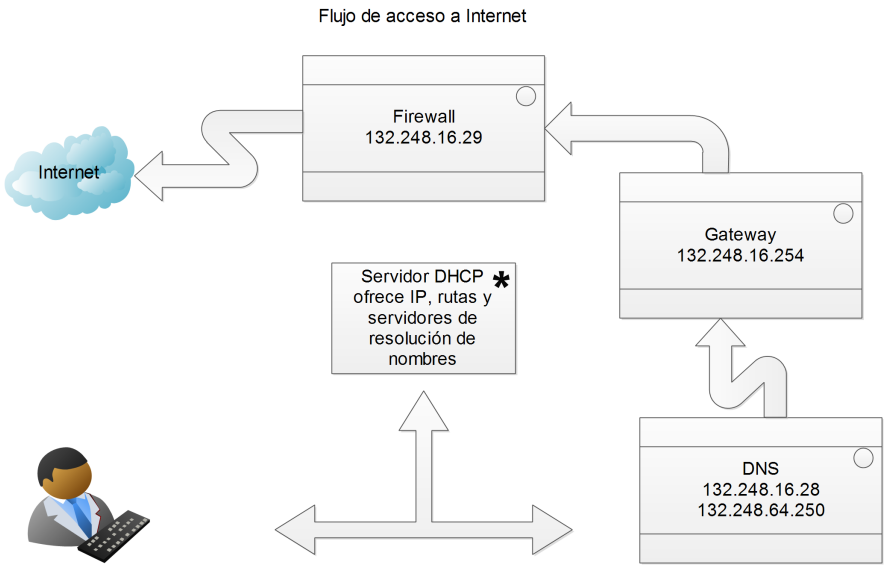
El firewall está implementado con IPtables. Es un firewall muy básico ya que lo único que se necesita es un script que contiene todas las reglas.

Lo primordial es bloquear todos los puertos e IPs entrantes, aunque tenemos desbloqueados los servicios básicos, éstas se van desbloqueando conforme se solicite. A continuación una breve lista de los servicios a los cuales se tiene permitido el acceso.

- Salida
  - Puertos de uso común como DHCP, SSH, HTTP, IMAP, SMTP y POP, todos estos también en su modalidad segura.
  - Puertos de redes sociales y comunicación como, Facebook y MSN messenger.
  - Skype, aunque por ser P2P es difícil abrirlo para todos los usuarios, es por eso que este servicio lo abrimos solamente bajo pedido.
  - Entretenimiento. Por ejemplo, estaciones de radio.
  - Transferencia de archivos por medio de varios protocolos de transferencia de archivo como: RSYNC, NFS, ISCSI, AFS, SMB.
  - Otros puertos para tramites administrativos con varias dependencias de gobierno y de la UNAM.
- Entrada
  - La mayoría de los puertos de entrada están cerrados por defecto, sin embargo si se solicita se abren los puertos que se necesiten.

En la Figura 1.2.7 se muestra el flujo de Internet en el IFC.

Figura 1.2.7: Diagrama del flujo de Internet.



En el tiempo que laboré en el instituto no existieron errores en el firewall o el gateway. Sin embargo, por ser el servidor donde pasa todo el tráfico del instituto, es una herramienta importante para analizar los problemas de otros servidores. Para el análisis de los problemas con los servidores muy comúnmente utilizo tcpdump y las bitácoras del sistema, además de las bitácoras de correo electrónico para cotejar las IPs obtenidas con los nombres de usuario y detectar el problema en el lugar exacto.

La forma de detectar si alguna computadora dentro del instituto está causando conflictos está descrita por el Algoritmo 1.1.

Algoritmo 1.1 Algoritmo para detectar un dispositivo conflictivo dentro del instituto por medio de la IP.

1. Obtener información de las IP's sospechosas en el gateway utilizando tcpdump.
2. Obtener la dirección MAC de la IP asociada al dispositivo problemático.
3. Bloquear temporalmente la dirección MAC del dispositivo.
4. Buscar en las bitácoras del servicio de correo electrónico si esa dirección MAC tiene asociado algún inicio de sesión reciente.
5. Si se encuentra alguna persona involucrada en el incidente.
    a) Reportar a soporte técnico para solucionar el problema en el dispositivo involucrado.
6. Si no se encuentra alguna persona involucrada en el incidente.
    a) Dejar bloqueada la dirección MAC involucrada hasta que el responsable se reporte en cómputo.

En la Figura 1.2.8 se muestra el script de inicialización y establecimiento de rutas y reglas del IFC[6, 8].

Figura 1.2.8: Código de inicialización de las funciones del gateway y firewall del instituto.

```
#!/bin/bash
## ********************************
## /etc/rc.d/init.d/firewall-ifc
## Sergio J Rojas H V 1.0
## 11/10/2002
## ********************************
## ********************************
## Michael Cruz Rojas V 1.1
## 19/04/2011
## ********************************
## ********************************
## Activa enrutamiento y parámetros de kernel para el reenvió de
## paquetes por ARP Cache, controlado por iptables por medio
## de dos interfaces de red.

## eth0 ------> RED PROTEGIDA
## eth1 ------> INTERNET

## Nota:
## "Se supone que el script /etc/rc.d/init.d/network no fue inicializado"
## Activa reenvio de paquetes

sysctl -w net.ipv4.ip_forward=1

## Configuración de las interfaces de red

ifconfig lo    127.0.0.1      netmask 255.0.0.0      up
ifconfig eth0 132.248.16.29 netmask 255.255.255.0 broadcast 132.248.16.255 up
ifconfig eth1 132.248.16.30 netmask 255.255.255.0 broadcast 132.248.16.255 up
ifconfig eth0:0 192.168.0.254 netmask 255.255.0.0 up

# Permite conexiones directas al edificio principal
# desde direcciones 132.248.212.0/24

ifconfig eth0:1 132.248.212.100 netmask 255.255.255.0 up

## Configuración de enrutamiento

route del -net        132.248.16.0    netmask 255.255.255.0 dev eth1
route add -net        127.0.0.0       netmask 255.0.0.0     dev lo
route add -host       132.248.16.254                        dev eth1
route add default gw 132.248.16.254                         dev eth1

## Rutas estáticas

for IP in 11 31; do
        route add -host 132.248.16.$IP dev eth1
done

## Modifica tabla ARP

arp -f /etc/ethers

## Establece las políticas de acceso de iptables

/root/scripts/politicas/politicas
```

1.2.2.3.3. DNS y salida a Internet

Para resolver algunos nombres locales tenemos un servidor DNS que mantiene algunas túplas de nombres y direcciones IP. Este servidor es el que se ubica primero en la configuración DHCP. Si este servidor no contiene la IP del nombre que solicita el cliente, entonces se pregunta a los servidores DNS de la UNAM que son DNS3 y DNS4, es decir 132.248.64.250 y 132.248.237.250.

Una vez que se obtiene el nombre del sitio a donde se quiere ir, el trafico se dirige al IIMAS por la fibra óptica conectada al MDF principal y de ahí a Internet.

1.2.2.4. Almacenamiento de archivos personales

Muchas personas en el instituto necesitan tener archivos de vital importancia compartidos por Internet. Por esa razón contamos con la mayoría de los servicios para compartir archivos.

En el instituto la gente puede encontrar mediante Samba archivos de instaladores de software libre que comparte el departamento de cómputo para toda la comunidad para cuando lo necesiten. También cada usuario, si así lo desea, puede tener su carpeta personal y compartir los archivos que crea conveniente por la red local del instituto.

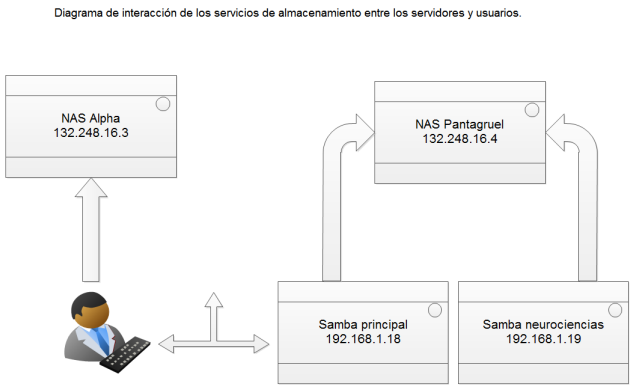
Existen también particiones compartidas por medios diferentes a AFS o Samba. Si un usuario lo requiere podemos crearle una partición en alguno de los NAS, del tamaño que se necesitem para que pueda montarla desde su computadora. De esta forma el usuario puede acceder y escribir más rápidamente que con Samba, además de contar con particiones más grandes.

Nuestros servidores para compartir archivos por Samba son 192.168.1.19 y 192.168.1.20. Para compartir archivos vía NFS puede ser por las siguientes direcciones 132.248.16.3 y 132.248.16.4. En general estos dos últimos servidores pueden soportar cualquiera de los protocolos comunes para compartir archivos.

Estos servidores, al ser muy sencillos, no han presentado problema alguno, más que cambiar discos descompuestos para preservar RAID 5. Sin embargo, son muy utilizados por la comunidad por lo que siempre deben de estar bajo observación. Esta observación suele ser más física que lógica ya que lo más importante es reemplazar los discos duros dañados para preservar el arreglo.

En la Figura 1.2.9 se muestra un diagrama de como interactúan estos servicios con la red y los usuarios.

Figura 1.2.9: Diagrama de interconexión de los servidores de almacenamiento.



1.2.3. Usuarios

Los usuarios de el IFC son en su mayoría estudiantes. Se debe de tener en cuenta este tipo parámetros para planificar servicios. Por ejemplo el correo electrónico está completamente basado en el numero de estudiantes y de investigadores. No se puede dar el mismo tipo de servicio siendo que las necesidades de ambos son diferentes, por lo que para garantizar el servicio es mejor dividirlos.

En este caso los dividiré como usuarios locales y externos.

1.2.3.1. Usuarios locales

Los usuarios locales son los que se albergan en el servidor de correo electrónico y son usuarios del sistema. Estos usuarios tienen un poco más de prioridad por ser el personal académico y administrativo. Se monitorean más principalmente por que los usuarios locales tienen acceso a más servicios en el instituto.

Estos son los tipos de usuarios locales: investigadores de tiempo completo; investigadores asociados; personal administrativo y estudiantes que necesitan tener su cuenta de correo electrónico en el servidor principal por el CONACYT, ya que no se puede cambiar la dirección de correo que se le dio al inscribirse a la lista de correo del mismo.

Los estudiantes no tienen acceso a los servicios locales del instituto por defecto, con el fin de no saturar los servicios que más ocupan los investigadores. Esto no

quiere decir que esté prohibido para ellos, sin embargo no tiene caso darlos de alta si no utilizan el servicio. Se puede hacer una solicitud al departamento de cómputo para darlos de alta en estos servicios sin mayor problema.

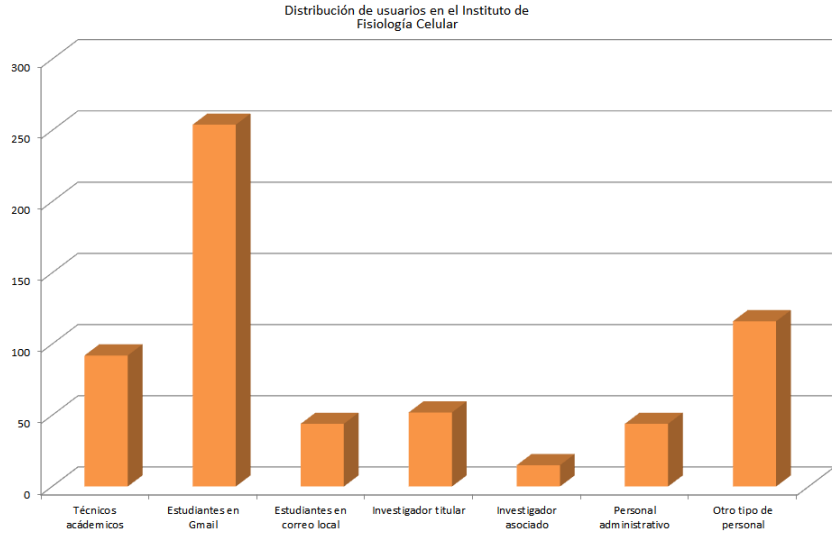
1.2.3.2. Usuarios externos

Los usuarios externos son los que están en la plataforma Gmail y en su gran mayoría son estudiantes. Estos usuarios no tienen acceso a los servicios del instituto, como la VPN o el almacenamiento en nube. Separamos a los estudiantes ya que en general no necesitan más de lo que ofrece Gmail, además de que de esta manera no saturan el servidor principal ni la red del instituto con ataques de spam.

Existen algunos usuarios externos que no son estudiantes. Estos usuarios están dados de alta en ambos servidores, sin embargo el servidor interno es el que recibe el correo electrónico y envía una copia del mismo a Gmail. Esta configuración también es bajo petición al departamento de cómputo. Los usuarios piden este tipo de mezcla de servicios ya que están más familiarizados con la interfaz gráfica de Gmail. No son muchos los usuarios con esta configuración.

En la Figura 1.2.10 podemos ver la distribución de los tipos de usuarios en el IFC:

Figura 1.2.10: Distribución de usuarios en el Instituto de Fisiología Celular.



1.3. Conclusión

Lo escrito en esta parte del reporte trata de crear una perspectiva concisa sobre como está estructurada la red del instituto. Se debió de empezar desde este punto para que en las próximas dos partes sea más simple procesar la información teniendo ya en mente como está conformado el instituto.

Como se pudo observar, la infraestructura del instituto es bastante compleja por lo que su administración en muchas ocasiones no es trivial. Desde este punto se puede apreciar el por qué la decisión de utilizar mi trabajo como forma de titulación. Como se había mencionado en la introducción, no se trata solamente de administrar un par de servicios, sino también de tomar decisiones críticas para optimizar la carga de trabajo en los distintos edificios que conforman el instituto.

Con la afirmación anterior, descrita en este capitulo del reporte, se tienen las suficientes bases para empezar a describir las tareas cotidianas, el mantenimiento de los servicios y las decisiones que he tomado para mejorarlos.

Capítulo 2

Mantenimiento y mejora de servicios

El propósito de este capitulo es hablar de la tarea que toma garantizar que los servicios funcionen correctamente en al menos 3 edificios, ya que es bien sabido que toda la carga de trabajo no es mi responsabilidad pero si la mayor parte. Este capitulo tratará sobre cuáles son las tareas que debo de realizar para garantizar el funcionamiento de los servicios del instituto en cuestiones de hardware y mayormente de software. Se describirán ciertas contingencias comunes en los diferentes servicios.

Los errores generalmente radican en el software y tienen una solución fácil. Para encontrarlos se deben observar constantemente las bitácoras de los servicios. En el instituto los errores más conflictivos y mas comunes provienen del correo electrónico o de las salidas a Internet, se le dedicará una sección completa de este trabajo al mantenimiento de esos servicios.

Como se acaba de mencionar, los errores generalmente surgen en el software pero si en algún caso llegará a fallar el hardware, lo que se tiene que hacer es decidir que hardware remplazará al defectuoso, desde un disco duro hasta un servidor entero. Se debe de tomar bien la decisión, siempre teniendo en mente que el instituto seguirá expandiéndose. Es por eso que se deben de comprar cosas de ultima generación. A este tipo de decisiones también le dedicaré una parte entera de este capitulo.

2.1. Mantenimiento de servicios

Las tareas cotidianas básicas de un administrador son pocas. Si estas tareas no se descuidan generalmente, no tiene por que haber problemas, siempre y cuando se reparen rápida y eficazmente los errores detectados.

Una de esas tareas es indiscutiblemente revisar constantemente las bitácoras para conocer el estado de los servicios. En el instituto los servicios que se deben de tener más en observación son el correo electrónico y la salida a Internet.

2.1.1. Correo electrónico

Hay varias cosas que se deben estar observando del correo electrónico de por ser el servicio más importante de todo el instituto y además por que el servicio correo electrónico está repartido en varios dispositivos. Se describirán las formas en las cuales se da mantenimiento para garantizar el servicio en dos casos, las cuales son físico y lógico.

2.1.1.1. Lógico

Lo básico a revisar es el tamaño de las bandejas de entrada en el servidor local. Estas bandejas de entrada no deben de llenar el espacio en los arreglos de discos. Si lo estuviesen haciendo, inmediatamente se tienen que agrandar las particiones para garantizar el servicio.

La partición de las bandejas de entrada tiene 100GB de espacio para los usuarios internos. En el tiempo que laboré en el instituto se llenó casi en su totalidad un par de veces. Esto paso regresando de vacaciones ya que nadie revisa su correo.

El espacio utilizado no debe de ser mayor al 40 %, ya que las lecturas y escrituras en las bandejas de entrada se empiezan a tornar lentas y por consecuencia el sistema completo de correo electrónico se torna ineficiente, al formarse un cuello de botella por intentar leer varios archivos al mismo tiempo. Por esa razón cada cierto tiempo se trasladan los correos electrónicos con más antigüedad hacia una carpeta diferente dentro del sistema de correos, la cual está en una partición diferente, esto con el fin de agilizar la lectura y escritura de lo que es leído con más frecuencia, que en el caso del correo son las bandejas de entrada.

Se debe de tener cuidado también del espacio utilizado con la partición donde se encuentra todo el correo almacenado, a excepción de la bandeja de entrada. Esta partición se debe de observar si está a punto de llenarse, ya que no hay otra

partición a donde enviar todo el correo electrónico almacenado. Esta partición se debe de expandir al tener el 85 % de su capacidad máxima, que son 500GB.

Otro de los problemas más comunes en el instituto es el spam y es de alta importancia vigilarlo, ya que pueden poner el dominio del IFC en listas negras al haber una computadora infectada dentro del instituto con algún tipo de gusano que envía spam a listas de direcciones de correos electrónicos. Para localizar la persona que está enviando spam se hace una averiguación muy rápida para conocer la identidad y el laboratorio en el que se está enviando el spam. Describiré dicha actividad en el algoritmo 2.1.

Este problema fue muy común mientras laboré en el instituto. Detecté y reparé exitosamente varios problemas de este tipo, la razón se debía al robo de identidad principalmente. Las personas maliciosas obtenían la información de la victima por medio de correos electrónicos falsos enviados desde fuera del instituto. Los usuarios al no saber como evitar el robo de su identidad responden generalmente a estos correos. Envíe varios correos mencionando hacer caso omiso a estos mensajes, sin embargo alguien cae en la trampa ocasionalmente.

En caso de que nos estén enviando mucho spam a nuestros servidores no nos afecta en nada ya que en la entrada de correo electrónico posicionamos el firewall Barracuda y separa la mayoría del spam. En ciertas épocas existe un gran afluente de spam del cual Barracuda no se hace cargo por como esta constituido el spam[1]. En este caso ponemos ciertas reglas en el firewall de correo para bloquear esos mensajes de uno por uno conforme se van observando.

La razón de por que Barracuda no está también en la salida del correo electrónico es por que la licencia que se compró se limita a cierto numero de cuentas de correo de entrada y de salida, estos usuarios se completan con tan solo las cuentas de correo de entrada que son los destinatarios. Además el correo de salida generalmente está limpio de spam. Como mencione anteriormente en 2 años solo tuve aproximadamente unos 10 incidentes de spam interno.

2.1.1.2. Físico

Los errores físicos que pudiera presentar el sistema de correo electrónico son varios, al estar distribuido en distintos servidores. Uno de los más difíciles de reparar sería la perdida de datos por falla en los discos duros. Aunque los discos estén en RAID 5, se pueden descomponer tres discos y perderse todo el arreglo. En este caso al tener el arreglo de discos en un servidor de propósito específico, tenemos alarmas audibles que nos alertan inmediatamente de la falta de algún

[1] Al estar en contacto frecuente con las farmacéuticas, se deben permitir los mensajes de este tipo aunque el contenido de la mayoría de spam contenga información sobre medicamentos ilegales.

Algoritmo 2.1 Algoritmo para detectar ataques de spam.

1. Se verifica que realmente haya una persona enviando spam hacia el exterior con las bitácoras de correos enviados en, el servidor de correo de salida.

2. En caso de que en las bitácoras aparezcan varios registros de envíos masivos de correo electrónico, se debe observar por cual servidor se están enviando los correos, para determinar el cliente que usa la máquina afectada. Puede ser por el servidor de webmail.ifc.unam.mx o outmail.ifc.unam.mx.

3. En el caso de webmail.ifc.unam.mx:

   a) Se trata de un ataque vía web, por lo que el atacante es muy probable que no se encuentre dentro del instituto y se trate de un robo de identidad.

   b) Se procede a investigar dentro de las bitácoras del cliente web de correo. Se debe de encontrar una IP, la cual envía correos a la misma lista que se encontró en la bitácora de outmail.ifc.unam.mx.

   c) Cotejamos que la información de la lista de receptores sea la misma en las bitácoras de ambos servidores, de ser así obtenemos el usuario al cual le fue robada su contraseña y la IP del atacante.

   d) Se bloquea la IP del atacante en el firewall.

   e) Se bloquea la cuenta afectada y se notifica vía telefónica a la persona con la identidad usurpada para, que vaya personalmente a cambiar su contraseña.

   f) Una persona de soporte técnico es enviada a verificar que la computadora de la persona afectada no esté infectada con algún virus.

   g) Al verificar todo lo anterior se cierra el caso.

4. En el caso de outmail.ifc.unam.mx:

   a) En este caso la persona seguramente está dentro del instituto por lo que es muy probable que esté infectada con algún gusano.

   b) Se obtiene el nombre de usuario directamente de las bitácoras, ya que no hay ningún cliente intermediario.

   c) Se bloquea momentáneamente la cuenta y se envía a una persona de soporte técnico a verificar si la computadora de la persona afectada está infectada con algún gusano.

   d) El usuario cambia su contraseña.

   e) Se cierra el caso al ser neutralizado el ataque.

disco para reemplazarlo de inmediato. Durante mi estancia he remplazado alrededor de 10 discos duros en los distintos arreglos con los que el instituto cuenta. No se perdió nunca ningún correo ni información.

Por otra parte se deben observar los switches con los que cada uno de los arreglos cuenta para comunicarse con los servidores de correo, ya que éstos están aislados de cualquier otro servidor para garantizar que nadie pueda entrar directamente a la partición de correo electrónico; además, como se mencionó antes, garantiza un buen ancho de banda. Estas medidas de seguridad físicas nos aseguran que para entrar directamente a la información de los correos electrónicos se necesita estar presente en el instituto.

Cuando llegué a laborar al instituto, el servidor de correo de entrada solía perder comunicación con los servidores de almacenamiento ya que, el switch que conectaba ambos no tenia fuente de poder redundante y estaba conectado solamente a un UPS. Por esta razón al haber un corte de energía eléctrica el correo automáticamente dejaba de funcionar. Solucionar el problema era de alta prioridad, así que se tuvo que pedir un nuevo UPS para cubrir este problema en el correo electrónico de salida. Este problema fue muy difícil de diagnosticar ya que el anterior administrador de sistema no me lo mencionó y el generador de corriente a diésel entra en un par de segundos, por lo que fue difícil saber que era exactamente lo que pasaba.

Para el caso de total avería física de los servidores, se guarda un respaldo cada semana de toda la información importante, como archivos de configuración y bitácoras, para restaurar en el menor tiempo posible un servidor sustituto con las mismas características. Durante mi estadía jamas tuve la necesidad de utilizar los respaldos, ya que corregía inmediatamente los errores que surgían.

2.1.2. Internet

Verificar el trafico en la red del instituto es de vital importancia no solo para poder acceder a Internet, también es sumamente necesario porque sobre esta red están todos los servicios del instituto, en caso de que existiera un exceso de flujo en la red inmediatamente se pierde el acceso a los servidores de correo y da como resultado algo parecido a un DoS. Es sumamente importante encontrar la causa del problema lo más rápido posible.

Existen muchas formas por las cuales puede fallar la red o perderse algún tipo de conexión entre servidores o edificios. De igual forma que en la sección de correo, es conveniente separar estos dos casos como físico y lógico.

2.1.2.1. Físico

Este tipo de errores en la infraestructura de Internet son difíciles de reparar, ya que en el caso de un switch trabado es muy difícil encontrar la causa por la cual la red está obstruida, por el exceso de tráfico que el mismo switch provoca. En el caso de que un switch deje de trabajar completamente es muy fácil identificarlo, porque es solamente una área en específico la que tiene el problema. Esto vuelve al problema fácil de reparar.

2.1.2.1.1. Tarjetas de red descompuestas

Este es uno de los problemas más difíciles de solucionar ya que, para encontrar el dispositivo que causa conflicto se necesita hacer una búsqueda similar a la binaria sobre el conjunto de switches, para saber cual es el switch o tarjeta de red que está causando problemas.

En estos casos primeramente debía darme cuenta entre cuál de los dos institutos se encontraba la tarjeta, para esto tenía una gran ventaja ya que en el MDF estaban conectados en el switch principal los dos edificios más grandes, es decir neurociencias y el edificio principal.

Para conocer en qué edificio se encuentra el problema que se debe de desconectar la fibra óptica que une a los dos institutos y en caso de en el edificio principal aun no haya acceso a Internet[2], entonces el problema seguramente está en el edificio de neurociencias por lo que hay que trasladarse a ese edificio para reconocer el IDF conflictivo.

Por esta razón mencioné que es búsqueda binaria, ya que hay que ir bajando de nivel en nivel hasta encontrar el laboratorio donde se encuentra la tarjeta descompuesta y poder apagar el dispositivo conflictivo inmediatamente, para dejar de saturar la red. Después de ubicar el dispositivo podemos trabajar solamente con él para analizar que fue lo que sucedió y reemplazar lo que sea necesario.

Este tipo de errores no se pueden detectar en las bitácoras, ya que el tráfico generado es tan grande que no se puede acceder a ningún servicio de diagnostico y revisar cuál es la causa del problema. Lo más rápido para solucionar el problema es desconectar de uno en uno los laboratorios. Esta solución puede sonar drástica pero definitivamente es más rápida ya que sigue los principios del algoritmo divide y vencerás. Este algoritmo indica dividir un problema en problemas ms pequeños, tanto como sea necesario para obtener una solución[19].

[2] El MDF se encuentra en el edificio principal.

2.1.2.1.2. Ciclos en switches antiguos

Los usuarios del instituto generalmente tienen muy pocos conocimientos en redes por lo que hacen cosas que afectan mucho a la red. Una de las cuales nos ha causado mucho problema durante todo este tiempo es la conexión cíclica de un switch, que los investigadores compran e instalan en su laboratorio sin nuestro consentimiento.

Estos switches que nos han dado dificultades con la conexión cíclica son muy viejos o están mal configurados. El problema no es instalar switches que los investigadores adquieran, el problema es no pedirnos asesoría antes de instalarlos y además que los alumnos jueguen con los switches.

Un error común que el personal comete es conectar dos cables en un mismo switch y hacer en un ciclo, aunado a esto los switches se descomponen y envían paquetes ARP broadcast. Al existir dicho puente los paquetes broadcast se replican de forma exponencial inhabilitando el acceso a los servicios en linea en todo el instituto.

Encontrar esto es una labor complicada. La solución a este problema es la misma que la de la sección anterior, una búsqueda con el algoritmo divide y vencerás sobre la red.

2.1.2.2. Lógico

Los problemas lógicos son los que pueden ser causados por ataques o programas en ciclo infinito, estás dos ultimás son muy comunes en el instituto.

2.1.2.2.1. Ataques

Los ataques son muy comunes en cualquier red grande o pequeña, siempre existirá una persona la cual quiera hacer mal uso de los servicios que se prestan.

Para determinar los ataques existen herramientas muy básicas pero útiles, por ejemplo tcpdump en cualquiera de sus distribuciones, como wireshark, snort, etc. Para detectar ataques solamente suelo utilizar tcpdump, pero en varias ocasiones utilicé wireshark y snort en su versión de linea de comandos[7].

Otra de las herramientas que utilizaba mucho para conocer quién y qué estaba haciendo con la red para alentarla, son las bitácoras del firewall, ya que con ellas puedo darme cuenta de que tipo de ataque están haciendo, en qué puertos, desde qué IP, desde cuándo y con qupe periodicidad[8].

Una vez que se haya detectado el equipo desde donde se está atacando la red, si está dentro del instituto simplemente bloqueo su dirección MAC. En este caso debo de cerciorarme si no existe alguna infección en la máquina que se puso en cuarentena. En caso de que sí exista algún gusano se notifica a soporte técnico para reparar la máquina lo más pronto posible. Además de todas las herramientas anteriores obviamente no puede faltar un firewall, que en el caso del instituto se implementa con IPtables. No hubo necesidad de implementar otro tipo de firewall ya que éste cubría completamente las necesidades del instituto.

Si es una persona ajena a la red del instituto simplemente se bloquéa la IP de la persona que intenta dañar la integridad de la red del instituto. Estos bloqueos los hacemos en el firewall.

2.1.2.2.2. Programas en ciclo infinito

Existen ocasiones en las que la red presenta dificultades cuando algún tipo de programa entra en un estado de ciclo infinito y envía paquetes basura en broadcast.

Estos paquetes son muy difíciles de bloquear con el firewall. ya que son confusos y pueden venir de cualquier parte del edificio. Por ejemplo, si es un paquete del tipo ARP "who has 192.168.255.255", todos los nodos dentro de esa red van a responder. Este error sucede con el software de los switches, puntos de acceso inalámbricos y programas de administración como MRTG. Lo que sucede en estos casos es lo siguiente:

1. Se suplanta la dirección MAC del equipo con la dirección MAC broadcast, es decir FF:FF:FF:FF:FF:FF.
2. Envía paquetes broadcast del tipo ARP en toda la red local.
3. Todos los equipos responden a la MAC de origen, como es la MAC para broadcast se responde a todas los equipos en la red haciendo que las replicas crezcan de manera exponencial, con el resultado de consumir todo el ancho de banda de la red interna.

Al ser falsa la MAC de origen, no se puede bloquear por medio del firewall, ya que si se bloquéa FF:FF:FF:FF:FF:FF ningún equipo podría comunicarse entre si o a Internet. Este tipo de problemas me sucedió solo un par de veces y para resolverlo debí de hacer una búsqueda binaria sobre los switches, al igual que en la sección 2.1.2.1.2, esto debido al exceso de tráfico que no deja utilizar ningún servidor ni programa para diagnosticar el origen del tráfico. Esta contingencia es la que más ocurre cuando se pierde la conexión entre equipos, lo que sucede es que el acceso es tan lento que es como si no hubiera conexión.

Afortunadamente contaba con las suficientes herramientas y experiencia para solucionarlo de una manera rápida y restablecer el servicio en muy pocos minutos. Como es habitual, en el laboratorio donde se estaba gestando el problema se debe trabajar más a fondo, ya que de no estar seguros de la causa, al volver a conectar el laboratorio a la red es muy probable que se vuelva a presentar el mismo problema en toda la red.

2.1.2.2.3. DHCP

El servicio de direcciones también forma parte de la infraestructura lógica de la red del instituto. Darle mantenimiento y solucionar sus problemas es sumamente fácil al ser este servicio muy básico.

El único problema de esté servicio es que switches, acces points entre otros lo traen implementado y empiezan a ofrecer configuraciones de red las cuales no están aceptas. Para solucionar este problema es necesario reconfigurar el dispositivo con los parámetros adecuados para que no ofrezca ninguna dirección fuera de estos rangos.

Es fácil averiguar qué dispositivo está causando conflictos, ya que los paquetes incluyen la dirección IP de origen y podemos buscar en las bitácoras del servicio DHCP qué dirección MAC tiene la IP de origen. De ser el caso que haya cambiado la dirección IP, se captura el tráfico para averiguar la dirección MAC de origen[3]. Con la dirección MAC puedo bloquear el dispositivo en el firewall para detener el tráfico conflictivo y averiguar qué es lo que le sucedió[8].

Está garantizado que este servicio funcionará todo el tiempo y siempre habrá un respaldo para en caso de perdida recuperarlo, ya que comparte el mismo equipo que el servicio de correo de salida.

El servicio DHCP jamás dio problemas extraordinarios más que en alguna ocasión que el servicio se trabó. Sin embargo, es importante mencionarlo, ya que sin este servicio el personal tendría que configurar manualmente su equipo lo que resultaría en un dolor de cabeza para todos.

2.1.3. Otros servicios

Los servicios anteriormente mencionados son los más importantes para que el personal del instituto pueda trabajar sin problemas. Existen otros servicios los cuales también son esenciales para un grupo particular de personas, como por ejemplo el servicio Web y la VPN. Estos servicios no son vitales para el funcionamiento de la red, sin embargo son usados muy frecuentemente por todo el personal.

[3] El instituto cuenta con una base de datos de todas las direcciones MAC de los dispositivos de red con los que se cuenta.

2.1.3.1. Servicio Web

Para mantener siempre el servicio web funcionando se debe de tomar en cuenta que es el servicio que da la cara por el instituto hacia el mundo, es decir, siempre que la gente quiere saber algo sobre el instituto acude al buscador de su preferencia y el resultado será la página web del IFC. Por esta razón todo el tiempo está recibiendo ataques.

Todos los puertos de la máquina donde se encuentra el servicio Web están bloqueados a la red externa, excepto el 80 obviamente. De esta forma garantizo que no existirán desde el exterior ataques para acceder al servidor.

Con lo dicho anteriormente únicamente me resta preocuparme por los ataques del tipo DoS. En el caso de que sucediera en la noche simplemente se revisan las bitácoras un día después y se bloqueá la persona que ataca al servidor. Existen scripts que pueden automatizar el bloqueo de ataques, sin embargo no los tenía implementados localmente, ya que los ataques los notifica directamente el CERT[4].

Jamás recibí un ataque DoS distribuido, pero si tenía planeado que hacer en caso de que sucediera. Primero revisaría cual es el patrón de ataque en todas las peticiones Web. Al encontrar el patrón crearía un script para recabar las IP's de las peticiones con dicho patrón y ejecutar IPtables para que bloquee automáticamente la IP detectada, hasta que termine el ataque. Al ser un momento crítico seguramente entrarían al bloqueo IP que no tienen nada que ver con el ataque, así que al mismo tiempo que se ejecuta el script se deberían de depurar tales IP[7].

En pocas ocasiones hubo algún DoS, pero no fue distribuido, por lo que solucionarlo fue muy fácil. Además, al tener un ancho de banda tan grande es difícil que cualquier persona pueda denegar completamente el servicio.

2.1.3.2. VPN

El personal del instituto, al terminar sus actividades en sus laboratorios u oficinas, llegan a trabajar a sus domicilios y generalmente requieren acceder a sus estaciones de trabajo. Como se mencionó antes, las IP's para la mayoría del personal son no homologadas, no se puede acceder desde el exterior de las instalaciones a las estaciones de trabajo sin una VPN.

Por esta razón está implementada la VPN. Igual que si DHCP, es un servicio muy sencillo pero muy importante. Su mantenimiento es sencillo, los únicos problemas que podrían surgir es que el ancho de banda para todos los usuarios sea

[4]Equipo de respuesta a incidentes de seguridad en computo UNAM, http://www.cert.org.mx.

insuficiente o se trabe el servicio y haya que reiniciarlo. Que el ancho de banda sea insuficiente para el servicio es muy poco probable, ya que al entrar a trabajar al instituto dejé un hilo dedicado a la VPN y al servicio de videoconferencias.

En un par de ocasiones el servicio colapsó haciendo que dejara de funcionar la red virtual, la solución simplemente fue entrar al panel de control de Mac Server y reiniciar el servicio.

2.2. Mejoramiento de servicios

Sustituir, adquirir y dar de baja el equipo es una labor que no se debe de tomar a la ligera. Generalmente mucho equipo que parecería obsoleto realiza operaciones muy importantes, un ejemplo es el de la computadora encargada de manejar el microscopio de un laboratorio, como se mencionó en la parte de Administración de sistemas.

De igual forma que la sección anterior, esta sección se dividirá en dos partes, físico y lógico.

2.2.1. Físico

En la época que laboré se tuvo mucho presupuesto para adquirir dispositivos y pensar en nuevos proyectos. A continuación se hablará un poco de las innovaciones que hice con ese presupuesto.

2.2.1.1. Telecomunicaciones

Desde el inicio de mis labores en el instituto tuve la necesidad de cambiar varios dispositivos. La constante mejora de telecomunicaciones me obliga a la actualización de los productos con los que cuenta el instituto, para ofrecer siempre un acceso fluido a las innovaciones informáticas.

La mayoría de los puntos de acceso inalámbricos en el instituto son estándar IEEE 802.11b/g, por lo que propuse mejorar al nuevo estándar IEEE 802.11n, el cual la gran mayoría de las computadoras nuevas ya incorporan, así como también dispositivos móviles como celulares y tabletas[11]. El uso de este nuevo estándar está por demás justificado, ya que tenemos una red interna con ancho de banda de 1000mbps y deberíamos aprovecharla inalámbricamente. Por tal motivo se han pedido alrededor de 20 puntos de acceso con este nuevo estándar y se sustituyeron los principales puntos de acceso.

Por otra parte también se debían de cambiar los switches del edificio de neurociencias para mejorar la conexión entre ambos institutos, así que pedí 3 switches Dell con capacidad para fibra óptica. De está forma se reemplazaron los switches obsoletos del edificio de neurociencias por unos de mayor velocidad. Además para los IDF se pidieron switches Dell de 48 puertos, con velocidad de 1000mbps, nuevos.

Pensando en el desarrollo del instituto, y con visión en el futuro, también hicimos un pedido de 2 switches con velocidad de 10gbps para conectar los edificios principales del instituto entre si, y tener un buen desempeño en la comunicación de ambos. Esto lo pensé y desarrollé aprovechando la fibra óptica, la cual puede soportar fácilmente los 10gbps.

Como se puede observar, mis decisiones en el área de telecomunicaciones han sido viendo hacia el futuro y con la intención de aprovechar los recursos con los que cuenta el instituto, utilizando lo más avanzado que existe en el área.

2.2.1.2. Almacenamiento

De la misma forma que las velocidades en los dispositivos de telecomunicaciones crecen, también avanza el espacio de almacenamiento de los discos duros. Es por eso que es necesario reemplazar los discos cada que sufran averías por otras de mucho más capacidad para no quedarnos con tecnología obsoleta.

Mi regla para decidir qué discos duros encargar era tomar un margen de precio para comprar, generalmente tomaba un rango para comprar discos de gama alta. El rango de precios que tomaba era de entre $850 y $900 pesos. El disco duro que estuviera dentro de ese margen era encargado para ser reemplazado. Desde que llegue pedí discos duros desde 500Gb hasta 2TB, que fueron los últimos para un servidor NAS del Dr. Gabriel del Río.

En relación a los arreglos de discos tuve que decidir que NAS comprar en base al presupuesto disponible. Preferí NAS porque en ocasiones es más fácil montar los servicios directamente en el hardware. Además, como este tipo de dispositivos generalmente ya tienen los servicios implementados en su sistema operativo nativo, es más fácil compartir archivos. La marca que preferimos en el departamento de cómputo es Aberdeen.

Hice el pedido a finales del año 2010 de un Aberdeen de 24TB de espacio de disco duro, el cual debe ser suficiente para cubrir las necesidades de almacenamiento de todo el personal de cómputo por aproximadamente 3 años.

2.2.1.3. Servidores

Al tener nuevos proyectos se debe dar a cada uno de ellos nuevos instrumentos de trabajo para darles un espacio y características dedicadas. Es por eso que se han hecho varios pedidos de servidores de gama alta. No solamente me tengo que preocupar por los servicios básicos que se deben de tener, como correo electrónico o web por ejemplo. También debo de tomar en cuenta todos los proyectos de investigación y sus necesidades.

El encargado del departamento de cómputo me pidió encontrar la forma más económica y rápida de comparar cadenas de genes. El IFC cuenta con un FPGA para realizar estas comparaciones, sin embargo estos no son asequibles y se requiere nueva tecnología que supere la actual solución. Investigando en diversas fuentes me dí cuenta de que el problema es apto para ser paralelizado[12]. Además encontré una implementación del algoritmo en CUDA que muestra resultados muy aceptables[13]. Con toda esta información creé un plan de compra para adquirir el hardware necesario para realizar las respectivas pruebas. Claramente el precio de este hardware comparado con el precio del FPGA es mucho menor, sin embargo no se ha adquirido tal hardware, ya que se retuvieron los fondos para esta mejora.

En el aspecto de servidores de uso cotidiano también se debe de pensar en el reemplazo. Ciertos servicios que tenemos como DHCP, DNS, VPN, LDAP etc., se podrían virtualizar y con ello ganar más espacio en el rack y ahorrar energía eléctrica. Afirmo esto ya que son servicios que no necesitan mucho poder de cómputo o no tienen la suficiente afluencia como para dedicarle un servidor para su tarea. Es por eso que también pedí un servidor de gama alta para que en un futuro se pudiera realizar esta tarea. El servidor en cuestión tiene 16 núcleos y 16 gigabytes de memoria RAM, lo cual es suficiente para este tipo de tareas. Desafortunadamente no pude hacer esta migración, ya que opté por continuar con mis estudios, pero la persona que quedó encargada de la administración de sistemas en el instituto ya conoce cuál es el propósito de ese servidor y estoy seguro implementará mi idea.

2.2.1.4. Estaciones de trabajo

La mayoría de los investigadores y estudiantes del instituto no tienen los suficientes recursos para tener una computadora en su laboratorio, ya sea porque no tienen beca o porque simplemente los recursos otorgados por el instituto para la investigación son insuficientes.

Por ese motivo pedí en todas las ocasiones computadoras portátiles y de escritorio para dar a los estudiantes, trabajadores e investigadores.

Para los investigadores generalmente pedí un nivel intermedio de computadoras, por ejemplo Intel i5. Para ellos pido entre 2 o 3 computadoras de escritorio. Para los estudiantes pedí computadoras de nivel bajo-medio, por ejemplo Intel i3. Las computadoras portátiles generalmente son de nivel medio, ya que se otorgan a investigadores y el modelo fue variable, aunque generalmente pedí de la marca Toshiba.

2.2.1.5. Energía

Como mencioné anteriormente, cuando ingresé al instituto a laborar hacían falta conexiones para las fuentes redundantes de los servidores. Al inicio los UPS estaban trabajando a su máxima capacidad, lo cual podría provocar un incendio. Otro problema que existía era el poco espacio en los racks, por lo que pedí dos UPS APC 2U de 2.7KVa, que ahora satisfacen completamente la demanda de energía en los servidores.

Con estos UPS pude conectar alrededor de 50 dispositivos de alta prioridad en el departamento de cómputo y hacer que estos UPS trabajen a la mitad de su capacidad, por si en algún momento se adquieren dispositivos nuevos exista lugar en donde conectarlos. Además, con los UPS trabajando a menos de su máxima capacidad se evitan posibles incendios.

Por otra parte, también se necesita ofrecer un respaldo a todas esas personas a las cuales les ofrecimos computadora de escritorio para su laboratorio, es por eso que he pedido aproximadamente 10 equipos de respaldo de energía en todo este tiempo. Estos respaldos no satisfacen completamente la demanda en el instituto pero si ayudan a la gran mayoría que no cuentan con al menos uno de ellos.

2.2.2. Lógico

En esta parte explico de manera más profunda algo muy importante para el crecimiento del instituto; lo cual fue la migración al nuevo correo electrónico. Es necesario abarcar este tema para que el administrador de sistemas que me sustituya tenga esta información acerca de la instalación y migración, de las múltiples plataformas que utilizábamos para dar el servicio de correo, a Zimbra.

2.2.2.1. Mejoramiento del servicio de correo electrónico

Muchos de los servicios del instituto son muy viejos y por más que se actualicen, en algunas situaciones ya no son aptos para soportar las cargas actuales de trabajo. Es por eso que en gran parte del tiempo buscaba nuevas implementaciones

de los servicios que se ofrecen en el instituto. Uno de los más representativos y envolventes fue Zimbra, el cual es un conjunto de servicios dedicados al correo electrónico; pero que sin embargo se pueden utilizar para diversos propósitos dentro del instituto, como aprovechar el directorio de personas que se instala por defecto.

El correo electrónico será reemplazado por Zimbra en un futuro próximo, por lo que se convertirá en la parte más importante del instituto, después de la infraestructura de red. Por esta razón, a continuación se expondrá la forma en la que se realizó la migración de una plataforma de correo a otra.

2.2.2.1.1. Análisis de los beneficios de Zimbra

Primeramente se debe de hablar de las diferencias entre Zimbra y MailScanner, que es la plataforma que se utiliza actualmente para el correo. Estas diferencias se mostrarán en el Cuadro 2.1 y el Cuadro 2.2.

Cuadro 2.1: Comparación de funcionalidades entre Zimbra y Sendmail[16, 9].

Características/Plataforma	**Zimbra Opensource**	**Sendmail**
Linux/UNIX	Si	Si
SMTP	Si	Si
POP3	Si	No
IMAP	Si	No
IMAP IDLE	Si	No
POP sobre TLS	Si	No
SMTP sobre TLS	Si	Si
Webmail	Si	No
ActiveSync	Si	No
Base de datos	Si	No
Sistema de archivos	Si	Si
Autenticación por LDAP	Si	No
Autenticación por SMTP	Si	Si
Otro tipo de autenticación	Cyrus SASL y externa	Interno, Open LDAP Active Directory
Configuración gráfica	Si	No
CLI	Si	No
Licencia	Código abierto	Código abierto

Como podemos observar, las características de Zimbra son mejores que las de Sendmail, esto se debe a que Sendmail fue pensado hace más de una década, donde la demanda de correo electrónico era diferente a la actual. Decidí usar

Zimbra porque contiene todas las nuevas características que se requieren para administrar la información de bastantes usuarios de una manera sencilla. Tuve la oportunidad de asistir al seminario de administradores de sistemas "Admin-UNAM", en el que me corroboraron que Zimbra es una herramienta robusta en base a la experiencia de los demás administradores.

Cuadro 2.2: Comparación de características antispam entre Zimbra y Sendmail[16, 9].

Características/Plataforma	**Zimbra Opensource**	**Sendmail**
DNSBL	Si	No
Antivirus incorporado	Si - Clamav	No
Antispam incorporado	Si - SpamAssassin	No
Listas negras	Plugin	Si

Como podemos observar, las características de Zimbra son superiores a las de Sendmail. Además de todos los puntos mencionados en las anteriores tablas, también tomé en cuenta que instalar, hacer backups y reparar Zimbra es fácil.

2.2.2.1.2. Instalación

Instalar Zimbra es sumamente sencillo, sin embargo se debe de mencionar para documentar todo de una manera completa. Primeramente se debe de bajar el archivo comprimido directamente de la página oficial de Zimbra y ejecutar el instalador. Este mismo instalador configura el sistema para que se pueda iniciar, reiniciar y parar en la terminal, con el comando `services`.

Zimbra fue instalado en una computadora de 4 núcleos y 8 gigas de RAM, lo cual es suficiente para poder administrar el correo de todo el personal del instituto. Una vez instalado Zimbra, lo único por lo que me debí de preocupar fue la migración entre las dos plataformas que son muy diferentes.

2.2.2.1.3. Migración

Se deben utilizar varios elementos para poder migrar correos, agendas y contraseñas. Lo primero que debía ser migrado son los usuarios y sus contraseñas. Para esto realicé un script que tomaba los nombres de los usuarios y la suma hash de sus contraseñas ubicadas en el archivo `/etc/shadow`. Inserté en Zimbra cada uno de los usuarios por medio del CLI como se muestra en la Figura 2.2.1.

Figura 2.2.1: Código de migración de usuarios y contraseñas en `/etc/shadow` a Zimbra mediante su CLI[6].

```
#!/bin/bash

################################################################################
################################################################################
#                              Instituto de Fisiologia Celular
#                                    Michael Cruz Rojas
#                                         Abril 2011
##Migracion de usuarios de sistema desde un archivo /etc/passwd
#                            a Zimbra mediante CLI
################################################################################
################################################################################


dominio="ifc.unam.mx"
shadow="/proc/zimbra/shadow"
script="shadow_to_zimbra.sh"


x=0


echo '' > $script


for linea in `cat $shadow`

do

  usuario=`echo $linea|cut -f1 -d":"`
  contrasena=`echo $linea|cut -f2 -d":"`


  if [ "x$contrasena" != "x*" ]
  then


   if [ "x$contrasena" != "x$!" -a "x$contrasena" != "x$!!" ]
    then


      echo "zmprov ca $usuario@$dominio temppasswordQAZXSW displayName
            $usuario" >> $script
      echo "zmprov ma $usuario@$dominio userPassword
            '{crypt}$contrasena'" >> $script
      x=$[x+1]


     fi


  fi


done
echo ""
echo ""
echo "Hecho"
```

Al haber migrado a los usuarios lo que sigue es utilizar imapsync para migrar todos los correos. Esta herramienta es muy versátil y soporta todos los protocolos de transferencia de correo en sus modalidades no seguras y seguras.

Antes de migrar todos los correos, listas y libros de direcciones, me encargué de clonar el servidor de correo principal en otro servidor alterno para no dañar el desempeño del servidor principal. El servidor que utilicé como respaldo fue tequila.ifc.unam.mx.

La copia que realicé en tequila.ifc.unam.mx obviamente está desactualizada, sin embargo al momento de poner en producción Zimbra se puede volver a sincronizar con mail.ifc.unam.mx y tardaría una fracción del tiempo que tomó respaldar todos los correos por primera vez, ya que se cuenta con la mayoría de los correos en Zimbra.

Para clonar mail.ifc.unam.mx en tequila.ifc.unam.mx escribí el script mostrado en la Figura 2.2.2.

Figura 2.2.2: Código para clonar mail.ifc.unam.mx en tequila.ifc.unam.mx.[6]

```
#!/bin/bash

################################################################################
################################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                    Abril 2011
#             Clonación de mail.ifc.unam.mx en tequila.ifc.unam.mx
################################################################################
################################################################################


destino="tequila.ifc.unam.mx"
usuarios="/root/usuarios"
dominio="ifc.unam.mx"
lineas=`cat /root/usuarios | wc -l`
let lineas=lineas+1
i=1
while [ $i -lt $lineas ];
do

    linea=`head -$i $usuarios | tail -1`
    nuevo_usuario=`echo $linea | cut -d: -f1`


################################################################################
#                  Se migran las carpetas de usuario
################################################################################


    rsync --verbose --rsh=/usr/bin/ssh --recursive
  --times --perms --links --exclude ".*" /home/$nuevo_usuario/
    $destino:/home/$nuevo_usuario/


################################################################################
#           Se migran las bandejas de entrada de los usuarios
################################################################################

    rsync --verbose  --rsh=/usr/bin/ssh --recursive
  --times --perms --links /var/spool/mail/$nuevo_usuario
    $destino:/home/$nuevo_usuario/$nuevo_usuario.inbox


    let i=i+1

done

echo ""
echo ""
echo "Hecho."
```

En la Figura 2.2.3 muestro el script con el cual migré los correos a Zimbra desde tequila.ifc.unam.mx.

Figura 2.2.3: Código para migrar el correo electrónico desde Sendmail a Zimbra mediante imapsync. Este script se ejecutó en tequila.ifc.unam.mx [6, 17].

```
#!/bin/bash

################################################################################
################################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                     Abril 2011
#Migracion de correo electrónico desde Sendmail a Zimbra mediante imapsync
################################################################################
################################################################################

lista_de_usuarios="/root/usuarios_a_migrar"
destino="correo.ifc.unam.mx"
origen="tequila.ifc.unam.mx"
contrasena_origen="xxxx"
usuario_origen="root"
contrasena_destino="yyyy"
usuario_destino"admin"


x=0


for usuario in `cat $lista_de_usuarios`
do


  imapsync --syncinternaldates --subscribed
--host1 $origen --host2 $destino
  --user1 $usuario --authuser1 $usuario_origen
--password1 $contrasena_origen
  --user2 $usuario --authuser2 $usuario_destino --password2 $contrasena_destino


done


echo ""
echo ""
echo "Hecho"
```

Cabe aclarar que se debe de activar en Zimbra la modalidad super usuario y el modo de autenticación plana para poder ejecutar imapsync de la manera en la que mostré.

Después de haber migrado los correos electrónicos de todos los usuarios desde tequila.ifc.unam.mx a Zimbra, lo que sigue es agregar las listas de distribución de correo. Para crearlas primero necesitamos extraerlas de mailman. Supongamos que los nombres de las listas fueron extraídos mediante un script y almacenados en el archivo `listas`. También por cada lista de correo existe un archivo llamado `lista-XXXXXXX`, el cual contiene todos los correos dentro de la lista llamada

XXXXXXX. Después de ejecutar el script descrito en la Figura 2.2.4, se agregan automáticamente las listas y los correspondientes usuarios a cada una de ellas.

Figura 2.2.4: Código para migrar las listas de distribución de correo electrónico mediante el CLI . Este script se ejecutó en Zimbra[15].

```
#!/bin/bash

################################################################################
################################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                     Abril 2011
#Migracion de listas de distribución de correo mediante el CLI de Zimbra
################################################################################
################################################################################

for lista in `cat /root/listas` do

        echo "" > /root/lists/zm_lista_$lista.sh

        chmod +x /root/lists/zm_lista_$lista.sh

    echo "zmprov cdl $lista@ifc.unam.mx" >> /root/lists/zm_lista_$lista.sh


        for member in `cat /root/lists/lista_$lista`

        do

                echo "zmprov adlm $lista@ifc.unam.mx" $member >>
              /root/lists/zm_lista_$lista.sh

        done

        /root/lists/zm_lista_$lista.sh

done


echo ""
echo ""
echo "Hecho"
```

Una vez agregadas todas las listas de correo, lo último a migrar son los libros de direcciones de cada usuario. Los libros de direcciones están almacenados en una base de datos MySQL porque Horde los administra. Sólo se pueden migrar los libros de las personas que hayan utilizado el cliente de correo electrónico web, ya que los que utilizaban los clientes Mail, Thunderbird o Outlook pueden hacerlo ellos mismos sin ningún problema, usando las herramientas gráficas de migración implementadas en Zimbra. Para Horde no existe ningún tipo de herramienta de migración, por lo que son las que preocupa migrar unicamente.

El método de migración consiste en realizar una búsqueda en la base de datos para obtener toda la información de los libros y después darles el formato que Zimbra requiere para agregarlos a la base de datos. Este formato es un archivo

CSV con la primera linea indicando el nombre de cada columna, las siguientes lineas tendrán la información de los contactos. En la figura 2.2.5 se muestra un ejemplo del formato de los archivos CSV aceptados por el CLI de Zimbra.

El archivo CSV debe cumplir las siguientes condiciones también:

1. Cada entrada debe ser abierta y cerrada unicamente por comillas.
2. El separador de entradas debe de ser una coma.
3. Se debe de utilizar el estándar de UNIX para el salto de linea, es decir "\n".
4. La codificación de caracteres debe de ser UTF-8.

Decidí hacer un archivo para cada libro porque es necesario revisar ciertas irregularidades, como son los caracteres de uso latino y caracteres que pudieran hacer que Zimbra no reconozca una nueva entrada. Esto es muy común ya que en ocasiones se agregan automáticamente las direcciones a los libros y los nombres de las personas suelen estar con caracteres poco comunes, por ser moda entre jóvenes o venir en una codificación diferente a la que soporta Horde. Por esta razón hay que corregir cada uno de los libros manualmente, ya que no se puede automatizar el proceso porque no se sabe con seguridad que caracteres hay que reemplazar.

Figura 2.2.5: Ejemplo de archivo CSV con un libro de direcciones. Este script se ejecutó en Zimbra.

```
"Extra","anniversary","assistantPhone","birthday","callbackPhone",
"carPhone","company","companyPhone","department","email","fileAs",
"firstName","homeCity","homeCountry","homeFax","homePhone",
"homePostalCode","homeState","homeStreet","homeURL","imAddress1",
"imAddress2","imAddress3","imAddress4","imAddress5","jobTitle",
"lastName","maidenName","middleName","mobilePhone","namePrefix",
"nameSuffix","nickname","notes","otherCity","otherCountry","otherFax",
"otherPhone","otherPostalCode","otherStreet","pager","workCity",
"workCountry","workFax","workPhone","workPostalCode","workState",
"workStreet"


"a","2011-01-01","a","2011-01-01","a","a","a","a","a","a","2","a",
"a","a","a","a","a","a","a","other://a","local://a","yahoo://a",
"aol://a","msn://a","a","a","a","a","a","a","a","a","a","a","a","a",
"a","a","a","a","a","a","a","a","a","a","a"
```

Una vez que se crearán los archivos CSV los inserté en la base de datos de Zimbra utilizando `curl`, con el siguiente script descrito en la Figura 2.2.6.

Figura 2.2.6: Código para agregar los libros de direcciones mediante curl en Zimbra . Este script se ejecutó en Zimbra.

```
#!/bin/bash

################################################################################
################################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                    Abril 2011
#Script para agregar los libros de direcciones mediante curl en Zimbra
################################################################################
################################################################################

for usuario in `cat $lista_de_usuarios`

  curl --insecure -u admin:contrasenaXXXX --data-binary
       /opt/zimbra/address_books/$usuario.csv
       https://correo/service/home/$usuario@ifc.unam.mx/contacts?fmt=csv

done


echo ""
echo ""
echo "Hecho"
```

Con esto último se consigue tener una migración completa de una plataforma a otra, totalmente diferentes. Lo único que resta por hacer es cambiar la IP actual de Zimbra, que es 132.248.16.55, por 132.248.16.2, para correo de entrada y crear un alias en la tarjeta de red para 132.248.16.18, que es el correo de salida. De esta forma garantizamos que los usuarios no tendrán que cambiar nada en su configuración.

Otro punto importante es cambiar la IP de los antiguos servidores de correo. Mi idea es invertir las IP en el caso del servidor de correo de entrada y ponerle otra IP al de salida ya que ahí se encuentra el servicio DHCP.

2.3. Conclusión

Este capítulo solo habla de lo extraordinario que se pudiera presentar durante el mantenimiento. Las situaciones no críticas no son contempladas ya que, de lo que se desea hablar en este reporte es del extra que realicé en mi época laboral para justificar que este trabajo es suficiente para obtener el titulo de Licenciado en Ciencias de la Computación.

La conclusión más importante que se debe de tener de este capítulo es la confianza que tuvieron en mi para realizar los pedidos y las innovaciones a la infraestructura del instituto. Esto habla de que había demostrado estar preparado para el puesto en el que laboré.

Me esforcé todos los días en mantener los servicios y dispositivos funcionando lo mejor posible, siempre tratándolos con afecto especial, ya que era la única persona autorizada que podía modificarlos o repararlos. Por esta razón, pocas veces tuve que estar en situaciones críticas para salvar servicios o dispositivos; siempre trataba de mantener todo al corriente y en orden para saber qué falló y cómo se debe de arreglar en una de estas situaciones críticas.

Además, todas las innovaciones que hice fueron pensadas en crecimientos de población repentinos en el instituto, ya que de esta manera hasta en los momentos de exceso de tráfico se puede garantizar que no colapsará ningún servicio y los dispositivos seguirán funcionando correctamente.

Todo esto habla de que mi aprendizaje durante la carrera de ciencias de la computación fue satisfactorio porque pude ejercer un empleo y sacarlo adelante sin mayor dificultad, gracias a los conocimientos adquiridos previamente en las aulas.

Capítulo 3

Desarrollo

En esta sección explicaré una de las partes más interesantes de mi trabajo que es el manejo e implementación de software. He participado en proyectos de programación web grandes, como la creación del programa web para la automatización del informe de labores anual en el instituto. Todos estos aportes y participaciones se explicarán a continuación uno por uno.

3.1. Proyectos web

En esta sección describiré proyectos web en los cuales me vi involucrado y algunas mejoras a la página oficial del instituto.

El objetivo de haber incluido estos resumenes sobre las aportaciones que hice, es hacer notar que además de administrar sistemas y optimizarlos, también estaba en proyectos de programación todo el tiempo y por lo tanto creaba nuevas herramientas para toda la comunidad. Es parte de ser administrador saber bastante de programación para reparar los desperfectos en las páginas web y dar opiniones en los nuevos proyectos para aprender de la comunidad en general. Además, es muy importante conocer los proyectos de programación en los que se trabaja dentro del instituto, para saber exactamente que está alojado en los servidores que administro.

3.1.1. Informe de labores

Este trabajo fue uno de los últimos en los cuales estuve involucrado. Se trata de un programa web el cual registra todas las actividades de los investigadores de

una manera rápida, dando como resultado un archivo con el formato indicado para entregarse al personal administrativo. De esta manera los investigadores ahorran bastante tiempo y todos siguen el mismo formato evitando dolores de cabeza.

El funcionamiento del programa es simple. El programa recopila todos los datos de los investigadores, los inserta en una base de datos y muestra el resultado con el formato que indica la dirección del IFC.

Mi primera participación en este proyecto fue darle un espacio, un alias y permisos dentro de algún servidor web. El primer planteamiento fue dejarlo en el servidor web principal, sin embargo, pensando en la afluencia que tendría. al final de año decidí dejarlo en el servidor Devel-Vasili[1].

La siguiente aportación fue desarrollar el código para crear sesiones y poder autenticar a los usuarios mediante IMAP, ya que como se ha mencionado con anterioridad, la base de datos de usuarios por el momento sigue siendo el correo electrónico, así que la forma más fácil de autenticar a los usuarios es vía IMAP.

La explicación de cómo funciona este código para autenticar a los usuarios que deseen registrar su informe de labores es muy simple. Primero se obtiene el nombre de usuario y la contraseña que el usuario envía en $_POST. Después se realiza una verificación en el servidor de correo electrónico con el usuario y contraseña obtenidos. Si la autenticación es correcta se procede a recuperar los datos guardados en la base de datos de su sesión anterior, para que siga trabajando o los imprima.

El código para autenticar y crear las sesiones es muy simple y lo incluyo en Figura 3.1.1:

[1] Apéndice B.15

Figura 3.1.1: Código para autenticar investigadores vía IMAP[4].

```
<?php

##############################################################################
##############################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                   Octubre 2011
#                  Código para autenticar investigadores vía IMAP
##############################################################################
##############################################################################

  session_start();
  include('conectar.php'); #Se conecta a la base de datos
  $mailbox= "{inmail.ifc.unam.mx:143/notls}INBOX";
  $user_investigador = $_POST["usuario"];
  $password_investigador = $_POST["password"];
  $connection = imap_open($mailbox, $user_investigador, $password_investigador);
  $conexion_inforlabo=conectar("inforlabo");
  $cadena_query="select id_investigador from usuario_nombre
                                  where usuario='$user_investigador';";
  $result=mysql_query($cadena_query,$conexion_inforlabo);
  $numero=mysql_num_rows($result);
  if($connection && $numero){
          $_SESSION["autentificado"]=1;
          $_SESSION["errordatos"]=0;
          $id=$array['id_investigador'];
          $_SESSION["id"]=$id;
          $conexion_ifcweb=conectar("ifcweb");
          $cadena_query01="select nombre_investigador from ifc_investigadores
                                                  where id_investigador=$id ;";
          $result_j=mysql_query($cadena_query01,$conexion_ifcweb);
          $array=mysql_fetch_array($result_j);
          $_SESSION["nombre"]=$array['nombre_investigador'];
          header("Location:  bienvenida.php");
  }else{
          $_SESSION["autentificado"]=0;
          $_SESSION["errordatos"]=1;
          header("Location: index.php");
  }

?>
```

Otra aportación que tuve en este proyecto fue todo lo referente a actualizar y eliminar entradas nuevas en la base de datos del informe así como también conectarse a ella. El código esta descrito en la Figura 3.1.2.

Figura 3.1.2: Código para hacer operaciones en la base de datos del informe de labores[4].

```
<?php

##############################################################################
##############################################################################
#                          Instituto de Fisiologia Celular
#                                Michael Cruz Rojas
#                                   Octubre 2011
#          Código para manipular la base de datos del informe anual
##############################################################################
##############################################################################

function conectar($base){
        $conectar=mysql_connect("localhost","root","guasita",true);
        if(!$conectar){
                echo "error al intentar conectarse con el servidor MYSQL";
        }
        mysql_select_db($base,$conectar) or die("no se conecto con la DB");
        return $conectar;
}
function conectarRemoto($base){
        $conectar=mysql_connect("www.ifc.unam.mx","root","guasita",true);
        if(!$conectar){
                echo "error al intentar conectarse con el servidor MYSQL";
        }
        mysql_select_db($base,$conectar) or die("no se conecto con la DB");
        return $conectar;
}
function liberar($conexion,$tabla){
        mysql_free_result($tabla);
        // libera los registros de la tabla
        mysql_close($conexion);
        // cierra la conexion con la base de datos
}
//borra un registro de la tabla con el id que se le pasa
//uso la funcion de conectar.php
function borrarRegistro($tabla,$id){
        $conexion=conectar("inforlabo");
        $cadena="delete from $tabla where id_$tabla = $id";
        mysql_query($cadena,$conexion);
        mysql_close($conexion);
}
function actualizarRegistro($tabla,$id,$sets){
        $conexion=conectar("inforlabo");
        $cadena="update $tabla set $sets  where id_$tabla =$id;";
        echo $cadena;
        mysql_query($cadena,$conexion);
        mysql_close($conexion);
}
?>
```

Además de haber creado la parte de autenticación, también di formato al código HTML y otras pequeñas correcciones en el código, ya que la persona contratada para codificar no terminó al cien por ciento el programa por cuestiones de fondos del instituto y tuve que detallar el programa final.

3.1.2. SMYTE

El aporte hacia esta página web fue más de carácter urgente que de dificultad. Quiero llegar con esta parte a recalcar la importancia de estar presente en ciertos momentos y la importancia de tener conocimientos no solo de redes de computadoras, también de lenguajes de programación para responder a los imprevistos de manera rápida.

La página web del SMYTE (Small Meeting on Yeast Transport and Energetics) fue encargada a diseñadores gráficos y no a programadores, por lo cual el resultado fue pésimo. Las personas encargadas de la página me abordaron con el problema un par de semanas antes de su congreso, por lo que era urgente modificar la página para agregar los programas de las reservaciones y pagos por PayPal.

Tuve que modificar y agregar información de esta página en muy poco tiempo y en una época donde había problemas en la red del instituto, por lo que la presión fue bastante. Además en la semana del congreso la modifiqué varias veces para agregar y quitar horarios dentro del programa.

Toda esta página web fue diseñada en HTML a excepción de la aplicación de registro, que es un simple formulario programado en PHP que sirve para agregar la información a una base de datos y enviar un correo electrónico a las personas organizadores, con el fin únicamente de informar. Este código lo programé con PHP.

Como mencione antes, el fin de relatar lo acontecido sobre la página del SMYTE no es para afirmar que fue un proyecto que me costó mucho trabajo. El motivo es dar a conocer que pueden llegar proyectos totalmente ajenos a tu trabajo y que se tienen que desarrollar indudablemente, como apoyo a la comunidad del instituto.

3.1.3. Mejoras a la página oficial del instituto

Además de dar soporte a la página oficial del instituto y agregar pequeñas cosas que se necesitan para detallarla bien, también le he tenido que hacer mejoras importantes. La que vale más la pena de mencionar es la modificación del sistema de noticias, el cual era muy rudimentario. Además agregué Twitter a las noticias para una mejor difusión de las mismas.

En Twitter, para las noticias del instituto solamente se pública el encabezado y una liga que conduce a la noticia en la página del instituto. Decidí incorporar Twitter al servicio de noticias porque Google agrega los tweets en los resultados

de sus búsquedas y con esto el instituto gana mucho al tener todas estas noticias indexadas en los buscadores más utilizados.

Con la justificación de por que entrar al ámbito de las redes sociales explicada anteriormente, obtenemos el principal objetivo de las noticias el cual es la difusión del trabajo que se realiza en el instituto al mundo. Para mostrar las noticias agregué un widget a la pagina inicial del instituto.

Sin embargo agregar un widget a la pagina principal del instituto no fue realmente el trabajo más importante dentro del programa de noticias. Tuve que modificar completamente la sección de noticias para enviar el encabezado a Twitter y agregar la información a una base de datos. En la Figura 3.1.3 muestro lo que agregué al código original de las noticias.

Figura 3.1.3: Código para realizar un tweet con el encabezado de la noticia y guardarlo en la base de datos[4].

```
<?php

##############################################################################
##############################################################################
#                        Instituto de Fisiologia Celular
#                              Michael Cruz Rojas
#                               Septiembre 2010
#      Código para realizar un tweet con el encabezado de la noticia y
#                        guardarlo en la base de datos.
##############################################################################
##############################################################################

$guarda = $_POST['guarda'];
if($guarda==1){
        $titulo_noticia= mysql_real_escape_string($_POST["titulo_noticia"]);
        $texto_noticia= mysql_real_escape_string($_POST["texto_noticia"]);
        $fecha_noticia= mysql_real_escape_string($_POST["fecha_noticia"]);
        //SUBIR FOTOGRAFIA
        if (is_uploaded_file($_FILES['foto']['tmp_name']))
                {
                        copy($_FILES['foto']['tmp_name'],
                    "../images/seminarios/".$id_seminario.".jpg");
             $imagen_noticia=1
        }
        mysql_query("INSERT INTO ifc_noticias (titulo_noticia, texto_noticia,
                        fecha_noticia, imagen_noticia) values ('$titulo_noticia',
                        '$texto_noticia', '$fecha_noticia', '$imagen_noticia')");
        $result = mysql_query("SELECT id_noticia FROM ifc_noticias
                                WHERE titulo_noticia LIKE '%".$titulo_noticia."%'");
        $row = mysql_fetch_array($result);
        $id_noticia =  $row['id_noticia'];
        if($id_noticia != null){
                exec("../twitter_oauth/tweet_post.py '".$titulo_noticia.",
          ".'http://www.ifc.unam.mx/post.php?id_post='.$id_noticia.
          '&lang='.$idioma."'");
        }
}
$fechahoy=date("Y-m-d G:i:s");
?>
```

Para enviar el encabezado de la noticia a Twitter utilizo un script programado en Python el cual yo no programé, lo conseguí de la red. La primera vez que agregué la funcionalidad de mostrar las noticias con Twitter utilicé los métodos básicos para publicar desde una página web. Sin embargo, al poco tiempo Twitter cambio su método normal de autenticar usuarios por el método OAuth, lo cual requiere tokens y ya no hace uso de contraseña ni usuario. Por ese motivo se me hizo más práctico conseguir un script que ya hiciera la autenticación de manera automática.

También tuve que modificar el script de autenticación ya que solo hacia eso, autenticar. Le agregué la función para que inmediatamente después de autenticar realizara el tweet. En realidad no queremos más que hacer un simple tweet, por lo que eliminé todas las demás funciones y utilizando el API de Twitter y un poco de lenguaje en Python programé dicha función. El resultado fue un código muy breve y limpio. En la Figura 3.1.4 se muestran las modificaciones.

Figura 3.1.4: Código para autenticar en Twitter y publicar un tweet[5].

```
#!/usr/bin/env python

################################################################################
################################################################################
#                        Instituto de Fisiologia Celular
#                              Michael Cruz Rojas
#                                Septiembre 2010
#          Script para autenticar en Twitter y publicar un tweet
################################################################################
################################################################################

import sys
import tweepy

auth=tweepy.OAuthHandler(CONSUMER_KEY,CONSUMER_SECRET)
auth.set_access_token(ACCESS_KEY, ACCESS_SECRET)
api = tweepy.API(auth)

#### Como invoqué el script desde php con "exec" el parametro uno es lo
#### público en twitter.

api.update_status(sys.argv[1])
```

De esta manera la noticia queda registrada en la base de datos y en Twitter para su difusión.

Capítulo 4

Conclusión

Las materias de la carrera que utilicé para realizar mi trabajo fueron generalmente las del área de sistemas y redes computacionales. Al tener este trabajo me di cuenta que me quiero dedicar a la investigación en este ramo o en el de cómputo científico.

Realizar este trabajo por dos años fue muy gratificante en todos los sentidos. Apliqué conocimientos teóricos en sistemas críticos y de alto nivel; tuve toda la responsabilidad de manejar una red con una infraestructura de alto rango; obtuve conocimientos que nunca hubiera podido adquirir en las aulas, ya que no se cuenta con la infraestructura para darse cuenta de lo que en realidad pasa en una red de alto rendimiento como la del IFC; aprendí a trabajar bajo mucha presión y dar resultados positivos en muy poco tiempo; conocí dispositivos diseñados para el cómputo científico, ya que esos conocimientos me servirán posteriormente en mi carrera profesional; aprendí a manejar dispositivos dedicados a la investigación y a tomar decisiones sobre cuál de ellos son los óptimos para ciertos trabajos, es decir diferenciar entre plataformas para tomar la mejor decisión de compra. Lo más importante que aprendí fue a aplicar mis conocimientos adquiridos en la carrera con un propósito practico.

Me fue muy difícil al principio sacar adelante toda la infraestructura del IFC. Sin embargo, gracias a todos los conocimientos adquiridos en la licenciatura, no fue mayor problema sobrellevar toda la carga de trabajo en poco tiempo. Tuve que optimizar y automatizar muchas de las labores para mantener funcionando los servicios y la red del IFC correctamente, lo cual era mi objetivo principal. Al adquirir el control de los servicios del IFC y mantenerlos funcionando constantemente, pude al fin realizar trabajos de mejoras e innovaciones dentro del instituto.

Es difícil obtener el control de mi objetivo principal, ya que me enfrenté a una red muy grande con muchas cosas que debía conocer con exactitud, como ubicaciones, usuarios, contraseñas, tipos de servicios, infraestructura, métodos de acceso, comprender la manera en la que interactúa en la red cada dispositivo, configuración de todos los servicios y la forma que se debe de manipular todo este conjunto de sistemas para tener un óptimo desempeño

Por toda la información expuesta anteriormente, considero que el trabajo que realicé en el IFC hizo que aplicará muchos de los conocimientos adquiridos en la carrera, además de aprender cosas nuevas.

Apéndice A

Redes

192.168.1.0/24 Reservado para virtualizadores, servidores con implementaciones del protocolo de archivos compartidos de Microsoft Windows e impresoras, switches y puntos de acceso.

192.168.2.2/24 Reservado para impresoras. Se divide en dos grupos: 192.168.2.0/28 para el edificio de neurociencias y 192.168.2.128/28 para el edificio principal.

192.168.3.0/24 Reservado para switches y puntos de acceso inalámbricos. Se divide en dos grupos: 192.168.2.0/28 para el edificio de neurociencias y 192.168.2.128/28 para el edificio principal.

192.168.16.0/24 Reservada para el servicio DHCP.

192.168.17.0/24 Reservada para el servicio DHCP.

192.168.212.0/24 Reservada para el servicio DHCP.

132.248.16.0/24 Reservada para los servicios en linea que brinda el IFC.

132.248.212.0/24 Reservada para los servicios de videoconferencia y VPN que brinda el IFC.

Apéndice B

Servidores

B.1. WWW

- Descripción: Servidor de paginas web.
- IP: 132.248.16.1
- Hardware: Intel Xeon 3.40GHz dos núcleos y 2GB de memoria RAM
- Software: Fedora core 11 x86_64, PHP 5.2.13, Apache 2.2.15 y mysql 14.14.
- Observaciones: Además de albergar la pagina principal del instituto se mantienen diferentes páginas, como la del posgrado de neurociencias, cursos, software creado por el instituto, entre otras.

B.2. Mail

- Descripción: Servidor de correo electrónico de entrada.
- IP: 132.248.16.2
- Hardware: Intel Xeon 2.33GHz, cuatro núcleos y 12GB de memoria RAM
- Software: CentOS 5.4 x86_64, Perl 5.8.8, MailScanner 4.79.11, UW IMAP4rev1 2007e.404 (IMAP de la Universidad de Washington), FreeRADIUS 1.1.3.
- Observaciones: Este servidor contiene una copia de las contraseñas y nombres de usuarios de toda la comunidad del instituto. El servidor de VPN depende directamente de Mail para autentificar. Se puede autentificar con IMAP o Radius.

B.3. NAS-Titan

- Descripción: NAS
- IP: 132.248.16.3
- Hardware: Intel Xeon 2.13GHz, cuatro núcleos, 3GB de memoria RAM y 16TB de almacenamiento en RAID 5.
- Software: Aberdeen SO 1.1 basado en CentOS 5.4
- Observaciones: Mantiene en constante funcionamiento los servicios NFS, ISCSI, AFS, SAMBA. Contiene la base de datos del servidor de correo Zimbra e información que los usuarios comparten.

B.4. NAS-Pantagruel

- Descripción: NAS
- IP: 132.248.16.4
- Hardware: Intel Xeon 2.13GHz, dos núcleos, 2GB de memoria RAM y 4TB de almacenamiento en RAID 5.
- Software: Aberdeen SO 1.1 basado en CentOS 5.4
- Observaciones: Mantiene en constante funcionamiento los servicios NFS, ISCSI, AFS, SAMBA. Este NAS guarda los correos electrónicos de Mail e información que los usuarios comparten.

B.5. NAS-Gargantua

- Descripción: NAS
- IP: 132.248.16.5
- Hardware: Intel Xeon 2.13GHz, dos núcleos, 2GB de memoria RAM y 4TB de almacenamiento en RAID 5.
- Software: Aberdeen SO 1.1 basado en CentOS 5.4
- Observaciones: Está reservado para almacenar la información de las futuras investigaciones con la tarjeta GPU nVidia Tesla c1070.

B.6. VPN-P

- Descripción: VPN edificio principal.
- IP: 132.248.16.6
- Hardware: Intel Core Duo 1.66GHz, 512MB de memoria RAM
- Software: MAC OS X 10.4, OpenVPN 2.4.2
- Observaciones: Autentifica con LDAP en el servidor Zimbra

B.7. Webmail

- Descripción: Interfaz web para el correo electrónico
- IP: 132.248.16.10
- Hardware: Intel Xeon 3.20GHz, dos núcleos, 4GB de memoria RAM
- Software: Fedora Core 10 x86_64, Horde 2.13.10.2, Apache 2.2.14, PHP 2.2.0
- Observaciones: Autentifica a los usuarios en el servidor Mail por medio de IMAP.

B.8. Outmail

- Descripción: DHCP y correo de salida.
- IP: 132.248.16.18
- Hardware: Intel Xeon CPU 2.40GHz, dos núcleos, 2GB de memoria RAM
- Software: Red Hat 9, MailScanner 4.63.5, Open DHCP Server 3.1.0
- Observaciones: En este servidor se guardan las direcciones MAC asociadas a cada computadora conectada a la red del instituto. Es una buena herramienta para detectar máquinas problemáticas.

B.9. Posgrado

- Descripción: Base de datos de estudiantes de postgrado y software para alinear cadenas de genes.
- IP: 132.248.16.25
- Hardware: Intel Xeon 1.80GHz, un núcleo, 1GB de memoria RAM
- Software: Fedora 9, Postgres 7.2.4, software de búsqueda de estudiantes de posgrado, Apache 1.3.27, EMBOSS (European Molecular Biology Open Software Suite)
- Observaciones: EMBOSS y el software de búsqueda de estudiantes utilizan Perl

B.10. DNS-Biotux

- Descripción: DNS local, respaldos, almacenamiento para los usuarios de microarreglos.
- IP: 132.248.16.28
- Hardware: AMD Athlon 1.66GHz, un núcleo, 512MB de memoria RAM.
- Software: Fedora 9, BIND 9.3.1, Apache 2.0.54.
- Observaciones: Los respaldos de los servidores listados en este Apéndice se hacen por NFS y se guardan en Titan.

B.11. Firewall-gateway-principal

- Descripción: Es el gateway y el firewall del edificio principal.
- IP: 132.248.16.29 (interna), 132.248.16.30 (externa), 132.248.16.254 y 192.168.0.254 las cuales son las IP's de los gateways.
- Hardware: CentOS 5.4, Intel Celeron 1.80GHz, 1GB de memoria RAM
- Software: IPtables 1.4.1.1
- Observaciones: Bloquea intrusos y es la salida a Internet del edificio principal.

B.12. EMBOSS-Oz

- Descripción: EMBOSS (European Molecular Biology Open Software Suite)
- IP: 132.248.16.31
- Hardware: PowerPC G5 2.0GHz, un núcleo, 3GB de memoria RAM

B.13. KVM

- Descripción: Appliance para poder acceder de manera remota a la salida estándar de video de los servidores.
- IP: 132.248.16.44

B.14. Barracuda

- Descripción: Appliance que sirve como firewall de entrada de correo electrónico.
- IP: 132.248.16.45
- Observaciones: Se debe de renovar la licencia anualmente.

B.15. Devel-Vasili

- Descripción: Utilizada como servidor de pruebas para programación web.
- IP: 132.248.16.47
- Hardware: Intel Xeon, cuatro núcleos 1.6GHz, 4GB memoria RAM.
- Software: Fedora Core 8, Apache 2.2.9
- Observaciones: Actualmente se aloja el programa web para el informe anual de labores.

B.16. FPGA-Decypher

- Descripción: Realiza alineamientos de cadenas de genes
- IP: 132.248.16.51
- Hardware: Intel Xeon, cuatro núcleos 3.0GHz, 4GB memoria RAM.
- Software: CentOS 5.4
- Observaciones: Contiene un FPGA con el algoritmo Smith-Waterman para alinear cadenas de genes.

B.17. VPN-N

- Descripcion: VPN del edificio de neurociencias.
- IP: 132.248.212.5
- Hardware: Mac Mini Intel Core Duo 1.66GHz, 512MB de memoria RAM
- Software: MAC OS X 10.4, OpenVPN 2.4.2
- Observaciones: Servicio principal de VPN en el IFC

B.18. Firewall-gateway-neurociencias

- Descripción: Bloquea intrusos y es la salida a Internet del edificio de neurociencias.
- IP: 132.248.212.14 (interna), 132.248.212.15 (externa), 132.248.212.254 y 192.168.212.254 las cuales son las IP's de los gateways.
- Hardware: Intel Celeron 1.80GHz, 1GB de memoria RAM.
- Software: IPtables 1.4.1.1.
- Observaciones: Es el gateway y el firewall del edificio principal.

B.19. Virtual-IFC

- Descripción: Virtualiza diferentes servicios (SMB-Neuro, Pruebas-HTTP, LDAP)
- IP: 192.168.1.8
- Hardware: Intel Xeon, cuatro núcleos, 3.00GHz, 16GB de memoria RAM.
- Software: VMware Server 2.0
- Observaciones: En el se encuentran servidores de pruebas de programación web, los servidores SAMBA y un servidor OpenLDAP de prueba.

Bibliografía

[1] James F. Kurose, Keith W. Ross, "Computer Networking", 5ª edición, Addison-Wesley, 2009. ISBN: 0136079679

[2] Andrew S. Tanenbaum, "Redes de Ordenadores", 4ª edición, Pearson, 2003, ISBN: 9702601622

[3] Abraham Silberschatz, Peter B. Galvin, Greg Gagne, "Operating System Concepts", 7ª edición, Wiley, 2004 ISBN: 0471694665

[4] Kevin Tatroe, "Programming PHP", 2ª edición, O'REILLY, 2006, ISBN: 0596006810

[5] Mark Lutz, "Programming Python", 3ª edición, O'REILLY, 2011, ISBN: 0596158106

[6] Cameron Newham, "Learning the bash Shell: Unix Shell Programming", O'REILLY, 2005, ISBN: 0596009658

[7] ISECOM, "Hacking Exposed Linux", 3ª edición, McGraw-Hill, 2008, ISBN:0072262575

[8] Thomas A. Limoncelli, "The Practice of System and Network Administration", 2ª edición, Pearsons, 2007, ISBN: 0321492668

[9] Bryan Costales, "Sendmail", 4ª edición, O'REILLY, ISBN: 0596510292

[10] RFC 5321, SMTP, http://tools.ietf.org/html/rfc5321

[11] IEEE 802.11: Wireless LAN Specifications, http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[12] CUDASW++: optimizing Smith-Waterman sequence database searches for CUDA-enabled graphics processing units, http://www.biomedcentral.com/1756-0500/2/73

[13] Código fuente de CUDASW++: http://cudasw.sourceforge.net/

[14] 160-fold acceleration of the Smith-Waterman algorithm using a field programmable gate array (FPGA), http://www.biomedcentral.com/1471-2105/8/185

[15] Documentación de Zmprov, http://wiki.zimbra.com/wiki/Zmprov

[16] Características de Zimbra Open Source Edition, http://www.zimbra.com/products/zimbra-open-source.html

[17] Documentación de imapsync, http://imapsync.lamiral.info/

[18] http://microarrays.ifc.unam.mx/, Unidad de Microarreglos del Instituto de Fisiología Celular

[19] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest, Introduction to Algorithms