Capítulo 4.- Recomendaciones para un Servidor web y de bases de datos seguro.

Este capítulo explica las características que un servidor web y de bases de datos seguro debe tener. Esto es esencial para que nuestras aplicaciones web sean seguras, robustas y funcionen de una manera correcta, además de garantizar la amplia disponibilidad de los servicios.

4.1.-Recomendación del Hardware.

El CDMIT cuenta actualmente con un equipo dedicado a servidor web y de bases de datos con las características mencionadas en la tabla 6.

Para que el CDMIT cuente con un servidor web y de bases de datos seguro, se hace la siguiente propuesta en cuanto a hardware:

Marca	Dell
Modelo	Poweredge 1950 III
Procesador	Intel Xeon cuádruple
Memoria RAM	4 GB
Disco Duro	250 GB
Sistema Operativo	Ubuntu 9.04 Server
Servidor Web	Apache 2.0.3
Motor de bases de datos	MySQL 5.1 Community Server
Administrador de MySQL	phpMyAdmin 3.1.3
Lenguaje de scripting	PHP 5.2.9

Tabla 7. Características del hardware propuesto para el CDMIT.

Con base en la comparativa de hardware del capítulo 1, se considera que el producto que cubre mejor las necesidades del CDMIT es el servidor Dell Poweredge 1950 III, ya que a pesar de ser el de mayor precio, tiene mayores ventajas que los otros 2 (HP ProLiant BL260c G5 e IBM x3200).

En comparación con el producto de Hp, cuenta con 3 años de garantía, cuenta con disco duro, cuenta con una mejor capacidad de escalabilidad y mayor capacidad en memoria RAM, aunque es más caro.

Si lo comparamos con el producto de IBM, el precio es prácticamente el mismo, con la ventaja para el producto de Dell, que cuenta con un disco duro, soporta un mayor número de núcleos, tiene una mayor capacidad de escalabilidad, y mayor capacidad de memoria RAM.

4.2.-Selección de Plataformas.

Como resultado del análisis que se realizó de sistemas operativos para servidores, los que se consideran más adecuados para cumplir con los objetivos trazados en este trabajo son:

- Ubuntu Server 9.04.
- Microsoft Windows Server 2003 Web Edition.

Característica.	Microsoft Windows Server 2003 Web Edition.	Ubuntu Server 9.04.
Sistema de Archivos.	NTFS.	Ext3.
Versión Actual.	R2	9.10
Licencia	Propietaria.	GPL.
Precio Promedio.	$399 USD.	Gratuito.
Principales Servicios.	HTTP, FTP, SSH, DNS, DHCP, HTTPS.	HTTP, FTP, SSH, DNS, DHCP, HTTPS.
Versión Estable.	R2	9.04
Sistema de gestión de paquetes.	Windows Installer 3.1.	Aptitude.
Principal ventaja.	Soporte de Microsoft.	Es gratuito.
Principal desventaja.	No es gratuito.	Menor compatibilidad con hardware comparado con Windows.

Tabla 8. Selección de plataformas.

La plataforma que proponemos es Ubuntu Server, ya que Ubuntu es gratuito, de código abierto, robusto y brinda todo el soporte que se requiere. Posee un repositorio de software muy completo y es una versión especializada en servidores. Cuenta con una mejor integración con manejadores de bases de datos de código abierto (MySQL y PostgreSQL) y con el servidor web Apache. Se actualiza continuamente, consume muy pocos recursos, es rápido y muy sencillo de usar.

El servidor web que proponemos utilizar es Apache, ya que es el servidor web más completo, tiene compatibilidad con múltiples plataformas de sistemas operativos, es gratuito, es el servidor web más utilizado en el mundo, cuenta con un gran soporte y tiene muy buena integración con lenguajes de programación y manejadores de bases de datos muy usuales en el CDMIT.

El manejador de bases de datos que consideramos más adecuado para cubrir los objetivos del trabajo es MySQL, ya que hace un buen complemento con Linux, Apache y PHP (LAMP), es soportado por Sun Microsystems, además de ser el manejador de bases de datos que se utiliza en el CDMIT, también es posible ejecutarlo en máquinas con bajos recursos y la versión gratuita es ideal para bases de datos de tamaño mediano.

4.3.-Instalación y configuración de las plataformas.

Como lo hemos mencionado anteriormente, el sistema operativo que se propone utilizar es Ubuntu Server 9.04 con el servidor web Apache 2.0.3 y el manejador de bases de datos MySQL 5.1 Community Server.

Se recomienda que al realizar la instalación del sistema operativo, se instale sólo el software mínimo necesario para su inicio y que posteriormente se instalen los paquetes de software que se requieran para prestar los servicios que se desean proporcionar. Esta medida ayudará a que el funcionamiento del servidor sea eficiente, ya que no se

desperdiciarán recursos en servicios que no se utilizan y se reducirán vulnerabilidades que pudieran conllevar estos servicios no utilizados.

En la sección A del anexo de este trabajo se muestra la propuesta de cómo instalar el sistema operativo con el software mínimo necesario para su inicio.

Recomendamos la instalación de los siguientes paquetes de software:

- Cliente y servidor OpenSSH.
- Servidor web Apache 2.
- Cliente y servidor MySQL Community 5.1.
- Módulo MySQL para Apache.
- PHP 5.2.9.
- Módulo de PHP para Apache.
- OpenSSL.
- Módulo SSL para Apache.
- phpMyAdmin 3.1.3

Además recomendamos la habilitación del Firewall de Ubuntu, el cuál viene instalado por defecto con el sistema operativo, pero se encuentra desactivado.

Con la instalación de estos paquetes de software, pretendemos tener los servicios web y de bases de datos, además de contar con soporte para PHP y HTTPS. El servidor SSH nos permitirá administrar al servidor web de manera remota y el paquete phpMyAdmin nos permitirá administrar nuestras bases de datos remotamente por medio de una interfaz web.

El procedimiento para la instalación y configuración de estos paquetes de software se encuentra detallado en el anexo de este trabajo.

4.4.-Recomendaciones para la administración del servidor web y de bases de datos.

Es recomendable para un buen funcionamiento del servidor web y de bases de datos realizar las siguientes tareas:

- Realizar respaldos continuos de los archivos importantes en el servidor y almacenarlos en un lugar seguro.

- Actualizar de manera periódica los programas críticos y el sistema operativo con los parches de seguridad más actuales disponibles.

- Crear cuentas de usuario con privilegios mínimos necesarios.

- Llevar un control de accesos y uno de sucesos en el servidor web: un *Access Log* (Control de accesos) y un *Activity Log* (Control de sucesos).

- Llevar un control de las acciones de los usuarios, para saber si realizan tareas acordes a los fines para los que funciona el servidor o no.

- Revisar continuamente los *logs* del sistema para detectar problemas y darles una solución.

- Utilizar software especializado para el monitoreo del servidor y la detección de *exploits* o programas que comprometan la seguridad del servidor web y de bases de datos.

- Revisar el estado del hardware, para detectar anomalías y evitar una posible suspensión del servicio.

- Si se desean añadir servicios al servidor, hay que verificar que se instalen sólo los paquetes necesarios.

- Se debe procurar el uso de servidores dedicados en actividades críticas, para evitar un daño de grado mayor en caso de un incidente.

- Utilizar el protocolo seguro (HTTPS) cuando se maneje el intercambio de información confidencial a través de la red.

4.5.- Recomendaciones de seguridad para aplicaciones que utilizan bases de datos.

Aquí presentamos algunos puntos a tomar en cuenta para que las aplicaciones hospedadas en el servidor web del CDMIT se encuentren seguras:

- Si se hace uso de contraseñas, éstas deberán almacenarse cifradas en la base de datos.

- Al realizar consultas para obtener datos, se deberán traer solamente los datos que se necesitan y evitar en lo posible el uso del comodín (*).

- La longitud de valores que se le asigna a cada campo de una base de datos debe ser la necesaria y se debe validar desde el código de la aplicación que ésta no se exceda.

- Se deberá llevar un registro de accesos a las aplicaciones, con los datos de quien accede, como accede, IP, hora y fecha.

- Todo el código que se comunique con la base de datos deberá ser filtrado.

- No se deberán referenciar archivos con una ruta absoluta, en especial si se comunican con la base de datos.

- La información que se obtiene de la base de datos o que se inserta en la base de datos deberá ser enviada por el método POST o bien si se hace uso del método GET, la información deberá ir cifrada.

- No se recomienda el uso del método REQUEST, ya que es un método genérico que puede recibir valores por POST, GET o desde las COOKIES.

4.6.- Recomendaciones generales.

En esta parte se presentan una serie de recomendaciones importantes de carácter general que sería provechoso llevar a cabo para tener un servidor web y de bases de datos seguro:

A continuación se muestra una propuesta para la sección de cómputo en el CDMIT:

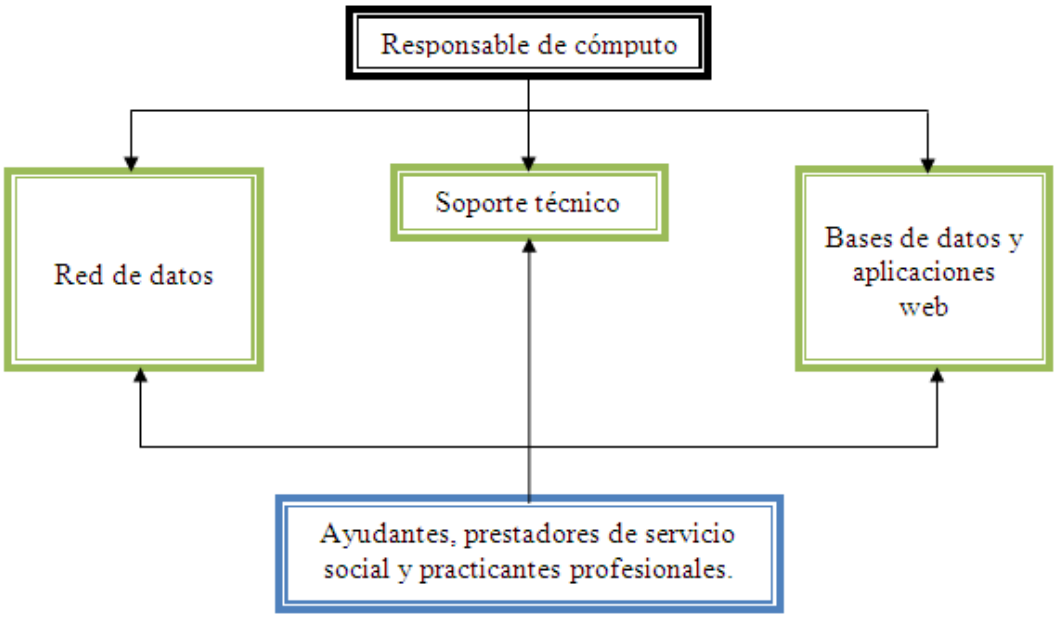

Figura 4. 1.-Estructura propuesta para la sección de cómputo del CDMIT.

Se propone que dentro de la sección de cómputo del CDMIT existan tres grupos:

Red de datos: Grupo donde deberá existir un responsable o administrador de red, quien supervisará el buen funcionamiento de la misma, las configuraciones de los equipos que la integran, así como resolver los incidentes de seguridad que se llegaran a presentar.

Soporte técnico: Grupo que se encargará de dar mantenimiento preventivo y correctivo menor a los equipos de cómputo, así como apoyar en instalaciones y configuraciones de software y hardware.

Bases de datos y aplicaciones web: Grupo donde deberá existir un responsable o administrador del servidor web y de bases de datos, responsable de las configuraciones, adecuaciones y respaldos.

Con esta estructura, el responsable de la sección de cómputo del CDMIT podrá delegar responsabilidades y responderá a las necesidades del CDMIT de una manera más adecuada.

Otras recomendaciones que se hacen son:

- Hacer la limpieza de la sala de cómputo frecuentemente.
- Asignar a una persona para realizar el mantenimiento del servidor web y de bases de datos.
- Elaborar una guía para los usuarios sobre la buena programación de aplicaciones.
- Delegar la responsabilidad a varias personas para administrar la seguridad en el CDMIT.
- Asignar a alguien que se encargue de difundir las vulnerabilidades y los riesgos que encontramos en Internet a través de artículos, cursos, etcétera sobre la seguridad de la información.
- Crear una cultura en seguridad en los miembros de la organización.
- Se necesita más personal en el área de cómputo para el apoyo de problemas en los equipos o en las redes de datos, que pueden ser becarios, prestadores de servicio social o prácticas profesionales.
- Delegar las responsabilidades a las personas que ayudan al área de cómputo dependiendo de la dificultad de estas, así como de su capacidad para realizarlas.
- Elaborar Políticas de Seguridad propias del CDMIT cumpliendo con las de la Facultad de Ingeniería, así como asignar a alguien que verifique su cumplimiento.
- Elaborar un Plan de Contingencia.
- Informar a los miembros de la organización sobre las personas que prestarán servicios y/o apoyaran al área de cómputo y avisar cuando la persona ya no preste servicios.
- Dar capacitación a las personas que prestan su servicio en el área de cómputo para que el área siga con su mejor funcionamiento.
- Hacer documentación de las configuraciones que se le hacen a los servidores.
- Quitar los dispositivos de la sala de cómputo que no se estén utilizando.

- Reportar cualquier anomalía en la red.

- Verificar que los dispositivos funcionen correctamente, es decir, no-break, router, switch, etcétera.

- Hacer un registro de las personas que visitan el CDMIT, para evitar algún incidente.

- Resguardar muy bien las claves de administrador, para evitar que alguna persona ajena al Centro haga mal uso de estas.

- Asignar una persona que verifique el cumplimiento del reglamento interno del CDMIT.

- Toda la información obsoleta debe ser destruida, de lo contrario, debe ser archivada en un lugar seguro.

- Conocer donde se encuentran los discos de respaldos del software que se utilice en el CDMIT.

- Dejar a alguien encargado en el CDMIT en la hora de la comida para mantener el control de acceso.

Se recomienda la existencia de un administrador de redes de datos, un administrador de bases de datos y aplicaciones web, una persona del soporte técnico, así como ayudantes, prestadores de servicio social y los que realizan prácticas profesionales.

Una vez hecho el análisis de riesgos la información obtenida servirá para realizar las políticas de seguridad para el servidor web y de bases de datos que se tuvo como objeto de estudio, así como, las recomendaciones para garantizar la protección del mismo.