Capítulo 3.- Análisis de riesgos.

Un análisis de riesgos es el proceso de estimar la probabilidad de que ocurra un acontecimiento y la magnitud probable de sus efectos adversos (consecuencias).

La información que se recopiló ha permitido identificar que problemas han existido en el área de cómputo del CDMIT, y permite recomendar los posibles mecanismos que deben aplicarse para contar con una mejor seguridad informática en el CDMIT.

Parte de la información que se ha adquirido se encuentra evidenciada por encuestas realizadas al personal del área de cómputo del CDMIT y desarrolladores de aplicaciones que utilizan el servidor web y de bases de datos.

3.1.- Identificación de los activos.

Se realizó el análisis de riesgos para uno de los activos del Centro de Diseño Mecánico e Innovación Tecnológica (CDMIT): el servidor web y de bases de datos, el cual cuenta con las siguientes características:

Marca	Compaq
Procesador	Intel Pentium III
Arquitectura	i386
Memoria RAM	256 MB
Disco duro	160 GB
Sistema operativo	Fedora Core 4.
Versión del kernel	2.6.17-1.2142_FC4
Servidor web	Apache
Versión del servidor web	2.0.54
Motor de bases de datos	MySQL
Versión del motor de bases de datos	4.1.18
Administrador de MySQL	phpMyAdmin 2.8.0.1
Version de PHP	4.4.2

Tabla 6. Características del servidor web del CDMIT.

Es muy importante el servidor web y de bases de datos del CDMIT porque almacena la información de proyectos, cursos, trabajos, calificaciones y material de apoyo para clases de los profesores, entre otros.

En un principio, el servidor web y de bases de datos era un servidor de pruebas, que después con las necesidades del personal del CDMIT, se convirtió en un servidor web y de bases de datos fundamental. Este es el motivo por el que se requiere identificar que eventos podrían ocurrir, las posibles consecuencias, y el impacto en las actividades cotidianas del CDMIT.

3.2.-Identificación de las amenazas y vulnerabilidades.

Se realizaron una serie de encuestas a los usuarios del servidor web y de bases de datos y también con algunas otras evidencias se obtuvo la siguiente información:

- Existe falta de comunicación entre las áreas del CDMIT, lo cual puede provocar que en caso de que ocurra un incidente no se siga un solo procedimiento para resolverlo y se pueden duplicar actividades en lugar de trabajar conjuntamente para resolverlo.

- El servidor no se encuentra en un lugar restringido.

- No hay una señalización adecuada en el lugar de trabajo que permita a los miembros del CDMIT tomar precauciones al ingresar al área de servidores.

- No se cuenta con clima controlado especial para un área de servidores.

- No se cuenta con un extintor en el área donde está situado el servidor web y de bases de datos.

- No se le da mantenimiento al servidor web y bases de datos, es decir, no se revisan los registros, las bitácoras y aquellas aplicaciones o servicios que hacen vulnerable al mismo, así como la probabilidad de ser atacado.

- Los responsables de cómputo no hacen respaldos de los archivos de configuración de la información.

- El servidor no es seguro, ya que presenta diversas vulnerabilidades que podrían ser explotadas y así comprometer la información de los usuarios.

- No se hacen las actualizaciones de seguridad de los sistemas.

- Los desarrolladores no hacen aplicaciones seguras porque no tienen una metodología de desarrollo que considere la programación de aplicaciones de manera segura.

- Los usuarios no utilizan protocolos seguros para el intercambio de la información en los sistemas, que en algunos casos, puede provocar una pérdida de información importante.

- Los usuarios confían de más en los mecanismos de control de acceso en la entrada del CDMIT.

- No se cuenta con políticas de seguridad propias ni un plan de contingencia en el CDMIT.

- No se contaba con una adecuada infraestructura de red de datos, pero actualmente se está reestructurando.

A continuación se muestra la estructura funcional actual de la sección de cómputo en el CDMIT:

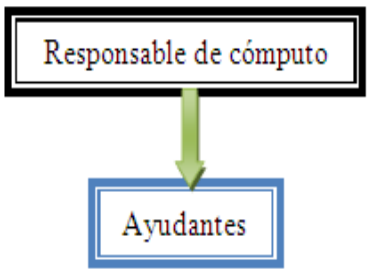

Figura 3.1.- Estructura actual de la sección de cómputo del CDMIT.

Con esta estructura, los ayudantes, quienes pueden tener algunas horas contratadas o son prestadores de servicio social, participan en todas las actividades de cómputo, pero

no hay nadie dedicado a una sola tarea o función, como por ejemplo, ser el administrador del servidor web y de bases de datos, y realizar todas las actividades que requiere el servidor para ser seguro.

3.3.-Determinación del impacto de la ocurrencia de una amenaza.

Si una amenaza se llegara a llevar a cabo, se debe evaluar lo que se puede suscitar y lo que implicaría para la organización tal suceso:

- Si no se tiene un extintor en el área de servidores y se llegara a presentar un incendio, la respuesta del personal del CDMIT sería tardía y esto pudiera provocar una pérdida mayor para la organización, dígase en cuanto a infraestructura e incluso en cuanto a personas.

- El no dar mantenimiento al servidor web y de bases de datos podría provocar que el servidor fuese vulnerable y por lo tanto que alguien explotara las vulnerabilidades y hubiera pérdida, robo o corrupción de información y/o afecte la disponibilidad de los servicios.

- El desconocer que personas ingresan al área de servidores es peligroso, pues si ocurriera la pérdida de algún equipo de cómputo o un daño físico provocado, no se sabría quien fue la persona responsable. Además, se tiene que hacer la limpieza para retirar el polvo que puede causar anomalías en el funcionamiento de los equipos de cómputo y demás dispositivos que se encuentran en el área. No es correcto que cualquier persona de la organización tenga acceso al área de servidores, ya que el acceso de cualquier persona podría provocar que personal ocioso dañara el servidor o hiciera mal uso de la información que en el se resguarda.

- La falta de comunicación entre las áreas puede provocar que en caso de que ocurra un incidente no se siga un solo procedimiento para resolverlo y pueden duplicar actividades en lugar de trabajar conjuntamente para resolverlo.

- Una sola persona no debería de hacer las cosas de varias personas porque nunca terminaría de cubrir todas las necesidades del CDMIT.

- Si se llegará a descomponer el no-break del servidor y hubiera una descarga eléctrica que provocara un daño irreparable al mismo, no sé podría adquirir prontamente otro servidor o estación de trabajo que lo supliera.

- Al no tener una organización de red adecuada, en caso de alguna falla, no sería posible detectarla de inmediato y esto causaría que el CDMIT dejara de realizar sus actividades normales.

- Al no revisar los registros, las bitácoras del servidor o no monitorearlo, si se presentan ataques, estos no serían detectados hasta que ocurriera pérdida de información o falta de disponibilidad en el servicio.

- El realizar aplicaciones con vulnerabilidades en código puede comprometer la información de los usuarios o incluso la operación del servidor web y de bases de datos.

- Se cuenta con un reglamento antiguo y obsoleto, que ya no se respeta, lo que puede provocar que ocurran incidentes de toda índole como mal uso del servidor, de la infraestructura de red o de las instalaciones y esto puede comprometer la información y la disponibilidad de los servicios del servidor.

- Al no contar con un dispositivo de control de temperatura adecuado se puede provocar que el hardware falle por causa de la temperatura ambiente y por lo tanto que los servicios no se encuentren disponibles.

- El no realizar respaldos de la información de los usuarios o de archivos importantes de los sistemas del servidor, existe el riesgo de que al suceder un desastre, esta información se pierda y no se pueda recuperar.

- La falta de señalización puede provocar que los miembros del CDMIT no tengan las precauciones debidas con activos importantes del área de cómputo del centro.

3.4.-Identificación de controles.

A continuación se muestran los controles que actualmente se llevan a cabo en el CDMIT:

- El personal del CDMIT cuenta con la identificación que los acredita como miembros del mismo.

- Los controles de seguridad con los que cuenta el CDMIT son: el acceso por huella digital o autorización en la entrada por parte de las secretarías en su horario de trabajo.

- El administrador asigna las contraseñas a los usuarios en el servidor web y de bases de datos.

- Los usuarios no pueden tener más de una cuenta en el servidor web y de bases de datos.

- Se dan de baja del servidor las cuentas de los usuarios que dejan de pertenecer al CDMIT.

- Los privilegios con los que cuentan los usuarios en el servidor web son: solo pueden leer, ejecutar y escribir en su directorio.

- El servidor web y de bases de datos cuenta con No-Break.

- Se sanciona a los usuarios que hacen uso indebido de sus cuentas en el servidor.

Lo que se puede decir de este análisis de riesgos, es que en el CDMIT existen vulnerabilidades que pueden ser explotadas en el servidor web y de bases de datos y en la propia organización.

Se propone realizar un análisis de riesgos de los demás activos que considere la organización como importantes, hacer las políticas de seguridad y hacer un plan de contingencia que consideré todos los aspectos de seguridad de la organización.

A continuación se presenta una propuesta de un servidor web y de bases de datos que cubra las necesidades del CDMIT con los recursos disponibles.