

Introducción

Contexto.

En la actualidad, el cómputo se ha extendido prácticamente a todas las actividades cotidianas, es por esto que la necesidad de proteger los recursos de cómputo (hardware, software e información) ha retomado importancia.

Para una organización la información y los recursos que ésta posee son de suma importancia, por lo que salvaguardarlos es una medida crítica que se debe aplicar para que la organización siga operando de una manera normal.

El Centro de Diseño Mecánico e Innovación Tecnológica (CDMIT) de la Facultad de Ingeniería de la UNAM, fue fundado en 1976, y desde su creación ha formado y capacitado a un gran número de profesores y alumnos de esta Facultad en el diseño de máquinas industriales. El centro ha sido pionero en el desarrollo de máquinas en nuestro país.

La protección de la información y de los recursos que la contienen es de gran importancia para el CDMIT por el valor que tales bienes representan. Dado el crecimiento y evolución que ha tenido el centro en los últimos 10 años, se ha visto en la necesidad de incorporar nuevos activos, entre ellos un servidor web y de bases de datos propio, el cual fue creado en un inicio sin ninguna medida de seguridad, por lo que el CDMIT decidió implementar medidas de seguridad en este servidor, para lo cual se formalizaron las siguientes tareas:

- i. Realizar las configuraciones correspondientes para que este servidor sea seguro.
- ii. Proponer las medidas de seguridad que se deban llevar a cabo por parte de los administradores para que la información que se almacena en este servidor esté segura, incluyendo un esquema de respaldos.
- iii. Elaborar una guía básica de recomendaciones para que las aplicaciones web y de bases de datos que generan los usuarios cumplan con la seguridad mínima requerida.
- iv. Elaborar una propuesta tecnológica para actualizar el equipo que actualmente funge como servidor.
- v. Elaborar una propuesta de políticas de seguridad para el servidor Web del CDMIT.

Estructura de la tesis.

La presente sección describe la organización de este trabajo:

En el primer capítulo (marco teórico) se presentan los conceptos básicos referentes a la seguridad informática, análisis de riesgos, políticas de seguridad, sistemas operativos para servidor, bases de datos y servidores web.

En el segundo capítulo (vulnerabilidades en aplicaciones web) se presentan las vulnerabilidades más comunes que pueden tener las aplicaciones web y de bases de datos.

En el tercer capítulo (análisis de riesgos) se presentan los resultados del análisis de riesgos que se hizo para el servidor web y de bases de datos del CDMIT.

En el cuarto capítulo (recomendaciones para un servidor web y de bases de datos seguro) se presenta la propuesta tecnológica para contar con un servidor web y de bases de datos robusto en cuanto a seguridad se refiere.

En el quinto capítulo (propuesta de políticas de seguridad) se presenta la propuesta de políticas de seguridad para el servidor web y de bases de datos del CDMIT generadas con base en el análisis de riesgos realizado.

Finalmente se presentan las conclusiones y un anexo con las configuraciones de seguridad propuestas para los servidores web y de bases de datos del CDMIT, para que los administradores o responsables de cómputo del CDMIT cuenten con un documento de consulta y de referencia rápida referente al servidor. Así mismo, para que los usuarios que desarrollan sus aplicaciones web o de bases de datos sepan las medidas básicas de seguridad que deben cumplir sus aplicaciones.