Capítulo 5.- Propuesta de Políticas de Seguridad.

En este capítulo se presentan una serie de políticas de seguridad, propuestas para el uso y la operación del servidor web y de bases de datos del CDMIT. Dichas políticas han sido diseñadas tomando en cuenta las políticas de seguridad en cómputo de la Facultad de Ingeniería y con base en un análisis de riesgos realizado en el CDMIT acerca de la situación actual del servidor web y de bases de datos perteneciente al Centro. Dicho análisis ha considerado aspectos como la infraestructura, la configuración del servidor, los hábitos de los usuarios y algunos otros aspectos importantes que nos permitieron hacer una propuesta adecuada al CDMIT.

5.1.-Políticas de seguridad física.

a) Restringir el acceso a la sala de servidores a personal no autorizado.

b) La sala de servidores deberá contar con puertas cerradas con chapas y con ventanas selladas.

c) Queda prohibido introducir y consumir alimentos y bebidas a la sala de servidores.

d) Queda prohibido fumar en la sala de servidores.

e) Hacer uso de Reguladores y/o No-Breaks para proteger a los servidores de fallas eléctricas que puedan causar un daño físico.

f) En la sala de servidores deberá haber un extintor visible y listo para ser utilizado en caso de incendio.

g) Deberá mantenerse una temperatura adecuada en la sala de servidores para la correcta operación de estos.

h) Cuando se realice limpieza en la sala de servidores, se deberá hacer bajo la supervisión de una persona autorizada y capacitada.

5.2.-Políticas de cuentas.

i) Las cuentas de usuario en los servidores serán únicamente otorgadas a miembros de la DIMEI o del CDMIT o en su defecto a personas que las requieran para realizar una labor acorde dichas organizaciones.

j) Las cuentas de usuario en servidores serán únicamente asignadas por un administrador autorizado.

k) Las cuentas de usuario contarán con los privilegios suficientes para realizar la actividad para la cual fueron creadas.

l) Las cuentas de usuario que se encuentren inactivas deberán ser dadas de baja por el administrador.

m) Las cuentas de usuario son personales e intransferibles.

n) Las cuentas de usuario serán utilizadas únicamente para fines académicos y de investigación y no con otros fines diferentes al giro del CDMIT.

5.3.-Políticas de contraseñas.

o) Las contraseñas de las cuentas son asignadas únicamente por el administrador de los servidores.

p) El usuario puede solicitar elegir su contraseña, siempre y cuando esta cumpla con los criterios para contraseñas robustas y esta solicitud tenga el visto bueno del administrador.

q) Las contraseñas deben ser robustas, es decir: contarán con al menos 8 caracteres, que contengan combinaciones de caracteres numéricos, alfanuméricos y símbolos y se deberá evitar que sean palabras de diccionario.

r) Las contraseñas deben ser cambiadas al menos cada semestre, excepto las de administrador que deberán ser cambiadas cada 3 meses.

5.4.-Políticas de control de acceso (lógico y físico).

s) El acceso remoto a los servidores se hace utilizando el protocolo SSH exclusivamente.

t) Queda restringido el acceso remoto por medio de protocolos como RSH, FTP, Telnet y aquellos protocolos que se consideren inseguros o que no manejen conexiones cifradas y de los cuales existan vulnerabilidades conocidas.

u) Cualquier usuario debe autenticarse con su cuenta y queda prohibido hacer uso de sesiones activas de otros usuarios.

v) El acceso físico al área de servidores sólo se encuentra permitido para personal autorizado del área de cómputo del CDMIT.

5.5.-Políticas de uso adecuado.

w) La información que un usuario suba al servidor web debe ser acorde a los propósitos con los que fue creada la cuenta de usuario y por ningún motivo deberá ser utilizada con otros fines.

x) La información que un usuario suba al servidor web debe encontrarse libre de virus, por lo que el usuario deberá asegurarse de que su información se encuentra limpia.

y) Queda prohibido a los usuarios la instalación de paquetes en equipo en el cual reside el servidor web, por lo que de requerir algún programa en especial, deben

solicitarlo al administrador del sistema, quien evaluará si es procedente la petición del usuario.

5.6.-Políticas de mantenimiento.

z) El administrador debe actualizar el sistema operativo y el software necesario con las últimas actualizaciones de seguridad para reducir vulnerabilidades.

aa) Se debe hacer uso de herramientas de seguridad, para encontrar posibles amenazas dentro del sistema (*exploits*, virus, códigos malignos, etc.).

bb) Se debe hacer un monitoreo permanente del servidor web, en donde se detallen los puertos que se encuentran abiertos, los servicios que se están ejecutando y la información de los hosts remotos que están accediendo a los servicios.

cc) Se deben construir bitácoras con toda la información de los cambios de configuración que se han hecho en el sistema a fin de tener un control que permita identificar el origen de posibles contingencias.

dd) Se debe hacer una revisión periódica del estado del hardware, para evitar que una falla de este tipo pueda provocar la no disponibilidad del servicio.

5.7.-Políticas de respaldos.

ee) Cada usuario es responsable de la integridad de su información, por lo que es el único al que le concierne hacer respaldos de tal información.

ff) El administrador debe hacer respaldos, por lo menos semestralmente, de los servidores web del CDMIT (información, configuración y archivos que se consideren importantes).

gg) Los respaldos hechos por parte del administrador deben almacenarse en medios resistentes y confiables, tales como cintas, servidores de respaldos u otros que se consideren convenientes.

5.8.-Sanciones.

Las sanciones que se proponen para cuando se hace uso indebido son las siguientes:

I. Uso de cuentas de usuario ajenas: Primera vez, amonestación. Reincidencia, cancelación de las cuentas de usuario de quien resulte responsable.

II. Cambio de configuración del servidor: Cancelación de la cuenta del usuario.

III. Instalación no autorizada de paquetes: Cancelación de la cuenta de usuario.

IV. Escalada de privilegios: Cancelación de la cuenta de usuario.

V. Uso de servicios con fines no acordes a las actividades del CDMIT: Cancelación de la cuenta de usuario y consignación al tribunal universitario si la falta se considera grave.

VI. Subir archivos infectados por virus: Reducción de privilegios.

VII. Violación de las políticas o reglamentos de cómputo del CDMIT: Amonestación, cancelación de la cuenta de usuario o consignación al tribunal universitario según la gravedad de la falta.

VIII. Ejecución de programas que intenten adivinar contraseñas de otros usuarios o del sistema: Primera vez, amonestación. Reincidencia, cancelación de la cuenta de usuario.

IX. Ejecución de programas que intenten explotar o encontrar vulnerabilidades en el sistema: Cancelación de la cuenta de usuario.

X. Daño de cualquier índole al sistema: Cancelación de la cuenta de usuario y consignación al tribunal universitario según la gravedad de la falta, así como el pago por los daños causados.

Con estas políticas de seguridad se mantendrá seguro el servidor reduciendo los riesgos y las amenazas que hoy en día se hacen más frecuentes y más fuertes por la falta de medidas y controles dentro del CDMIT.