CAPITULO VI

INSTALACION

6. Instalación

6.1. Plan de Contingencia

6.2. Informe de Instalación

6.3. Carta de Aceptación

6. Instalación

6.1 Plan detallado de Contingencias

6.1.1 Introducción

El Sistema SIIAC se basa en un plan que está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en previsión de desastres.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre, lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia. [www.009]

El plan de Contingencia para SIIAC se fundamenta en estos puntos básicos para enfrentar algún desastre:

- Análisis de Riesgos
- Prevención,
- Localización,
- Respaldo de datos
- Recuperación.
- Desastres naturales
- Desastres del entorno

6.1.2 Análisis de Riesgos

En esta fase, la preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo?, ¿qué puede ir mal? y ¿cuál es la probabilidad de que suceda?

¿Que está bajo Riesgo?

La integridad de los datos para eso se sacara respaldo lógico de datos y de la Aplicación Web se debe contar con la seguridad apropiada que corresponde al administrador del sistema y al proveedor del hosting.

¿Qué puede ir mal?

En base a los aspectos citados, podemos establecer planes de contingencia alternativos dependiendo de qué situación se presente y sus magnitudes las cuales puedes ser.

- Parciales; recuperación a corto plazo.
- Considerable; recuperación a mediano plazo.
- Totales; recuperación a largo plazo.

¿Cuál es la probabilidad de que suceda?

Llevar acuerdos con el proveedor del hosting con respuestas inmediatas mediante el servicio de correo para dar posibles alertas de ataques de virus o Hackers que puedan dañar la información del Sistema

El sistema proveedor del hosting cuenta con una bitácora continua para registrar todos los procesos que se efectúan en el Centro de operaciones, que en este caso es el espacio del administrador asignado para alojar la Aplicación Web. Es importante la bitácora, pues la cual contribuye en descubrir cual o cuales fueron las causas que ocasionó la contingencia, cuando se originó y a partir de qué punto ocasionó los problemas.

6.1.3 Prevención.

Para la administración lógica de la documentación de la Aplicación Web y demás servicios que cuenta el mismo, deberá optar por tomar políticas del manejo de contraseñas de alta seguridad; como por ejemplo que sean alfanuméricas (letras, símbolos y números), sea la única persona que tenga acceso a las contraseñas y sea capaz de realizar cambios periódicos de las mismas para evitar un sin número de ataques de virus, Hackers y más elementos ajenos a nuestra Aplicación Web, para ello hay que tomar en cuenta las siguientes sugerencias.

- No olvidar de cerrar sesión cuando esté trabajando directamente con el administrador de la Aplicación Web al ausentarse por tiempos largos.
- No dejar que terceras personas manipulen los password.

- Llevar una bitácora de los cambios realizados tanto en el administrador del hosting, como en el administrador de la Aplicación Web. Se recomienda llevar un archivo de todos los cambios realizados y si es el caso tener en cuenta la persona responsable.

- Tener una segunda persona de confianza que tenga los mismos conocimientos del manejo de la Aplicación Web y del hosting; por ejemplo que sea por lo menos un tecnólogo en Sistemas computacionales, el cual llevará consigo las mismas responsabilidades del administrador.

- Para los servidores de consultas a base de datos, en este caso de consultas de pagos de agua, se debe llevar periódicamente un respaldo de la información, sacando imágenes de la base de datos en discos físicos con la finalidad de que si se produce algún fallo en el hardware o software del servidor hosting tener respaldo de la información y dicha información debe ser guardada físicamente fuera del área de trabajo e inclusive fuera del área de sistemas asignada, esto por seguridad.

6.1.4 Localización

Si la prevención no se puede cumplir en su totalidad por cualquier motivo se considera que un potencial ataque sea detectado lo más pronto, para minimizar sus efectos; para ello sugerimos algunas sugerencias en la localización de fallos lógicos causados por terceras personas:

- Es importante que los administradores de la Aplicación Web y del hosting, tratar de no realizar los ingresos a administrar en sitios que no sean seguros, como por ejemplo centros de computo públicos donde nos pueden estar copiando los datos de ingreso a la parte de administración; para ello se recomienda si se lo hace desde ese tipo de lugares hacerlo con un equipo portátil de propiedad de la Institución o nuestro propio equipo para evitar los famosos cookies.

- Es importante concienciar a todos de su papel en la política de seguridad de software; por ejemplo un usuario (parte de la compañía) detecte algún

problema o vulnerabilidad del Aplicación Web que no haya sido previsto por el administrador sea alertado en forma inmediata para hacer correcciones oportunas.

6.1.5 Respaldo de los datos

En la inmensa mayoría del sistema informático, los datos almacenados en el sistema tienen mucho mayor costo y son mucho más difíciles de recuperar que el sistema en sí. Entre los riegos de pérdida de datos se cuentan los errores en el software, la falla de equipos, el error humano, el daño intencional, las catástrofes naturales. El respaldo de datos es la generación de una copia, en un momento determinado, de los datos del sistema, con vistas a su eventual reposición en caso de pérdida. Todos los sistemas informáticos deben respaldarse cuidadosamente, en momentos predeterminados, siguiendo un cronograma preestablecido.

La información levantada al Hosting tratar de almacenar en dispositivos de tipo magnético. Los respaldos deben mantenerse apartados de dispositivos tales como parlantes de audio, transformadores de pared, acondicionadores de línea, unidades de potencia ininterrumpida (UPSs), unidades de disco o disquetera no confinados en gabinetes metálicos, monitores aún apagados, detectores de metales como los usados en los aeropuertos. El campo magnético terrestre termina, con el tiempo, afectando los medios magnéticos de grabación; esto limita la duración efectiva de los respaldos; para períodos largos, se aconseja usar medios ópticos o regrabar periódicamente. Puede asumirse una duración de 3 años para los medios magnéticos. [www. 010]

En este caso una buena sugerencia es tratar de proteger la información en los denominados backups, es decir, de la protección de los diferentes medios donde residen nuestras copias de seguridad, es recomendable guardar en lugares no cercanos al sitio habitual de trabajo, ya que en caso de producirse un incendio podríamos perder los respaldos.

Otra recomendación de los backups es etiquetar en orden a la fecha de respaldo y algo muy importante luego de etiquetar nuestros disco toda la

información debe ser protegida con contraseñas cifradas de tal forma que si son sustraídas por personas ajenas a la zona de administración no puedan tener acceso a la información almacenada en los backups; se recomienda que el ingreso a la sala de backups se realice con tarjetas de ingreso u otra seguridad sugerida por el administrador.

6.1.6. Recuperación de Software

Si la información es demasiado crítica con el manejo de base de datos podemos hacer por ejemplo lo siguiente:

- Tener presupuesto para tener la información respaldada físicamente en un disco duro extra y/o en disco ópticos, de esta forma mantener la información más relevante almacenada, para realizar recuperaciones inmediatas ante caídas del servicio brindada en la Aplicación Web.

6.1.7 Desastres naturales

Aunque el problema de desastres naturales no se da frecuentemente, es necesario tener en cuenta este tipo de amenaza, que en caso de producirse puede dar más de un inconveniente.

A pesar que la información de la Aplicación Web está alojada en un servidor en otro país y los representantes legales del hosting ya tengan todo este tipo de prevenciones para sus equipos, lo único que nos queda a nosotros es tratar de proteger los backup de la información levantada en el servidor (hosting).

6.1.8 Desastres del entorno

Los incendios son eminentemente un peligro no solo para nuestros equipos es por eso recomendable tener en cuenta lo siguiente.

- Se recomienda siempre tener a mano extintores contra incendios cerca de los equipos, laboratorios y zonas de trabajo.
- Es recomendable tratar de no fumar cerca de equipos informáticos en especial cuando se tiene discos magnéticos y ópticos los cuales pueden sufrir daños irreversibles.

- De igual forma que en las inundaciones es recomendable tener una segunda copia en otro lugar seguro y bajo las mismas condiciones de seguridad.

6.2. Captura de errores

A continuación tipos de errores que se pueden dar al utilizar el Sitio.

Ejemplo o descripción del Error	**Causa**	**Posible Solución**
Nota. main(/www/user/public_html/ includes/ compat.php50x.php): falla en abrir el archivo o directorio.	Observar la diferencia entre /www/user/ public_html/includes/ y c:\apache1\htdocs \joomla. Esto sucede cuando subimos al servidor Remoto la configuración. php quese utiliza en el servidorlocal, o vice versa.	Corregir los paths y url de configuration.php pueden estar direccionados a nuestro localhost. Por lo general no se sucinta este tipo de errores, a menos que el hosting funcione con otro path; se recomienda configurar el archivo *configuration*
Nota: main(includes/joomla.php): falla abriendo la secuencia, Permiso negado en www/joomla/public_html/index.php en la línea 25	Permiso denegado al archivo que ejecuta la sentencia	Revisar los permisos CHMOD de los archivos

Errores del sistema y otros

Ejemplo del error	**Tipo de error**	**Posibles Errores**	**Posibles Soluciones**
Este sitio se encuentra		Joomla no puede conectarse a la base de	Revisar configuration.php

temporalmente fuera de servicio. Por favor notifique al Administrador.	Error del sistema	datos, ya sea porque no hay acceso al usuario, sea porque el servidor de MySql no está operativo o caído.	para ver si los valores de conexión a la base de datos son válidos. Si eso está todo OK, tratar de entrar a la base de datos vía phpMyadmin
Acceso restringido	Error del sistema	Se ha tratado de acceder mediante el navegador a alguno de los archivos de funcionamiento del sistema	Ninguna solución. simplemente no se puede acceder a estos archivos por cuestiones de seguridad
(Error de Login) Advertencia de IE: "Internet Explorer no puede abrir el sitio... Operación anulada"	Navegador	Problema de incompatibilidad del navegador Internet	Probar con otros navegadores, o eliminar las cookies de Internet Explorer, luego cambiar de plantilla del sitio y volver a intentar.

Tabla. 6.1 Descripción de errores y posibles soluciones

6.2.1. Backup de la Base de Datos y Contenidos de la Aplicación Web.

Ingresar al sitio de administración de la siguiente forma.

Ingrese a la administración del hosting adquirido e ingrese la respectiva contraseña suministrada por el administrador del hosting**.** A continuación ingrese a la base de datos MySql y dentro de la carpeta data copie la carpeta comercibarra o a su vez puede sacar un script de la base de datos digitando en el administrador de la base de datos como se nota en el gráfico. [WWW.011]

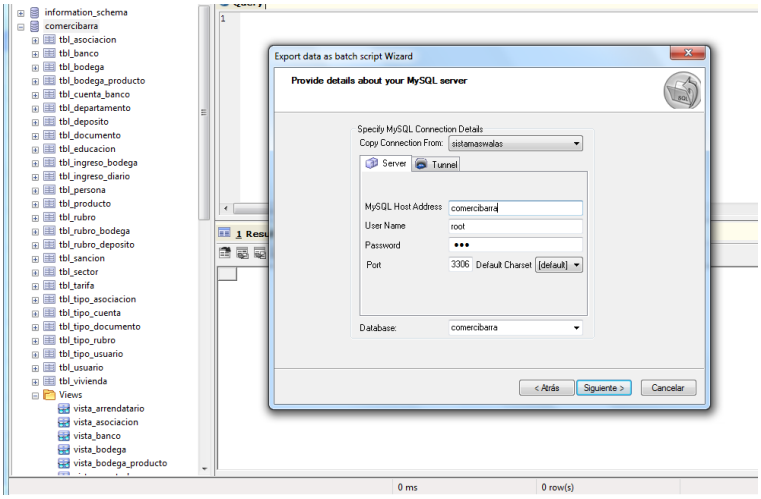

Figura. 6.1 Consola de administración de la base de datos SQLyog

Selección exportar y a continuación escoja las opciones señaladas en la fig.6.2

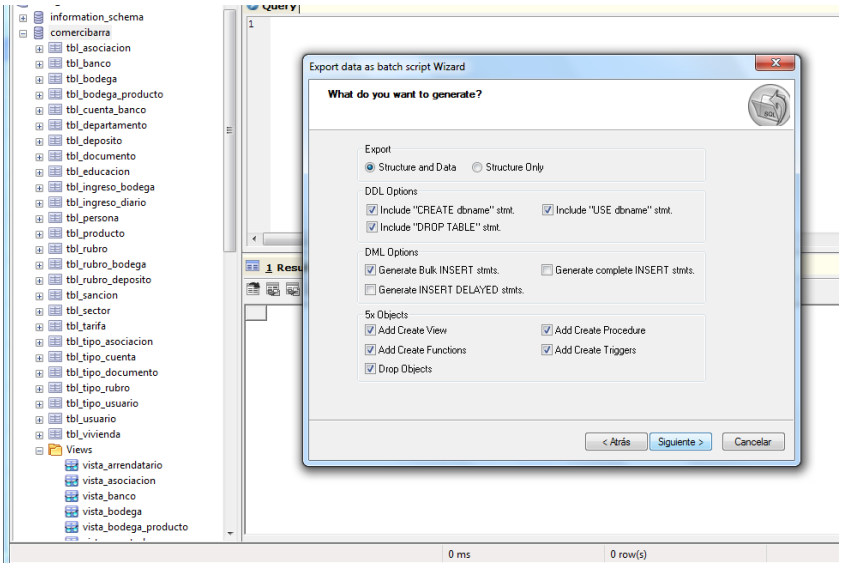

Figura. 6.2 Opciones previas para sacar el backup de la Base de Datos

Pulse continuar y listo, hemos sacado el respaldo de la base de datos del sitio.

6.2.2. Respaldo de contenidos.

Para hacerlo podemos hacerlo de dos maneras, la primera sería directamente desde el sitio de administración del proveedor del hosting y segunda es mediante

la utilización de un software adicional como por ejemplo un ftp el cual permite acceder a la información directa al contenido del administrador del hosting**,** claro está mediante el ingreso con sus respectivas contraseñas provistas por el proveedor. A continuación copie la carpeta del sitio "comercibarra", que es donde se encuentra toda la información de la Aplicación Web.

Toda la información antes mencionada grabar en un dispositivo de almacenamiento (CDs, Disco Duro etc.).

6.3. Informe de la Instalación

Antes de realizar la instalación de todos los paquetes de software necesario es preciso tener en cuenta la compatibilidad de cada uno de los mismos para no tener ningún inconveniente más adelante cuando el Aplicativo este ejecutándose; para ello a continuación se expone una guía de instalación y ciertas recomendaciones para evitar conflictos…para más detalle revisar el anexo adjunto. [WWW.012]

Ver anexo 5

6.4 Carta de Aceptación

Luego de haber realizado una serie de comprobaciones de posibles errores como son de enlace y conexiones con el servidor hosting se realizó el respectivo lanzamiento de la Aplicación Web en la sala del Reuniones de COMERCIBARRA, donde se aprobó el proyecto para más detalle revisar el anexo adjunto.

Ver Anexo 6