# PLAN DE CONTINGENCIA SISTEMA MK

Finalidad

Con este documento se busca definir las normas y procedimientos necesarios para enfrentar cualquier eventualidad que se produzca en el SISTEMA MK, de modo que se asegure la continuidad en su funcionamiento, además de la seguridad y confiabilidad del mismo.

La idea es evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un “desastre” ocurra y así facilitar la recuperación después del evento.

Objetivos

* Entregar a Hospital Clínico del Sur una guía que ayude a prevenir, mitigar y solucionar rápidamente cualquier eventualidad relacionada con el cese de funcionamiento del SISTEMA MK o inoperatividad de los equipos que lo mantienen (Servidor de Base de datos y Servidor Web).
* Garantizar el normal funcionamiento de Hospital Clínico del Sur.
* Minimizar la posible pérdida de datos financiera y operativa, ejecutando los procedimientos de respaldo apropiados.

Metodología

El plan se estructura en 3 fases:

* **Mitigación:** Procedimientos previos ante el posible evento o emergencia, haciéndolos menos graves, reduciendo las consecuencias o posibles pérdidas.
* **Emergencia:** Acciones que deben ejecutarse durante el evento o emergencia.
* **Recuperación:** Restablecer las condiciones y operación normal del SISTEMA MK.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **MITIGACION** | **EMERGENCIA** | **RECUPERACION** |
| **OBJETIVO** | Reducir consecuencias del daño | Limitar el daño | Continuar y Recuperar procesos vitales |
| **ACTUAR** | Antes del evento | Inmediata | A medio plazo |
| **CONTENIDO** | Procedimientos para evitar daños graves. | Alternativa a procesos normales | Estrategia para la recuperación de los recursos |

# Mitigación

Con el fin de reducir los riesgos de daños graves se evalúa primeramente todas las eventualidades que podrían ocurrir, elaborando una lista para una preparación oportuna:

* Siniestros
  + Incendio
  + Corto circuito
  + Terremoto
* Robos
  + Fraude
  + Robo de Equipo
  + Robo de Información
  + Robo de tiempo de trabajo
* Fallas de Hardware
  + Fallas de Placa Madre (MotherBoard)
  + Falla de Tarjeta de Red
  + Falla de Disco Duro
  + Falla de Fuente de Alimentación
* Fallas de Software
  + Falla de Sistema Operativo
  + Falla de Software de Base de Datos
  + Falla de Software Aplicación (ej : Microsoft Office)
* Errores Humanos
  + Borrado de Datos (Servidor BD)
  + Apagado de Equipos (Servidor BD y Servidor Web)
  + Perdida de Claves de Acceso (Servidor BD y Servidor Web)
* Accesos No Autorizados
  + Accesos Físicos no autorizados
  + Accesos Lógicos no autorizados (a la red, a la base de datos, etc.)
* Malware Informático
  + Infecciones de virus, spam, phishing, etc.
* Vandalismo Informático
  + Borrados de Información
  + Deterioro de Equipo
  + Hackers

|  |  |  |  |
| --- | --- | --- | --- |
| **DESCRIPCION** | **CAUSA CONTROLABLE** | **PROBABILIDAD OCURRENCIA** | **INTENSIDAD DEL DAÑO**  **(1 al 10)** |
| **Siniestros** | | | |
| Incendio | Si | Baja | 10 |
| Cortocircuito | Si | Baja | 10 |
| Terremoto | No | Baja | 10 |
| **Robos** | | | |
| Fraude | Si | Medio | 3 |
| Robo de Equipo | Si | Medio | 4 |
| Robo de Información | Si | Medio | 5 |
| Robo de tiempo de trabajo | Si | Alta | 5 |
| **Fallas de Hardware** | | | |
| Fallas de Placa Madre | No | Medio | 10 |
| Fallas de Tarjeta de Red | No | Medio | 8 |
| Falla de Disco Duro | No | Medio | 8 |
| Falla de Fuente de Alimentación | No | Medio | 8 |
| **Fallas de Software** | | | |
| Falla de Sistema Operativo | No | Medio | 8 |
| Falla de Software de Base de Datos | Si | Alta | 8 |
| Falla de Software de Aplicación | Si | Medio | 5 |
| **Errores Humanos** | | | |
| Borrado de Datos | Si | Medio | 8 |
| Apagado de Equipos | Si | Medio | 10 |
| Perdida de Claves de Acceso | Si | Medio | 5 |
| **Accesos no Autorizados** | | | |
| Accesos Físicos no autorizados | Si | Alta | 5 |
| Accesos Lógicos no autorizados | Si | Alta | 5 |
| **Malware Informático** | | | |
| Infección de Virus, spam, phishing | Si | Media | 8 |
| **Vandalismo Informático** | | | |
| Borrados de Información | Si | Medio | 7 |
| Deterioro de Equipo | Si | Medio | 7 |
| Hackers | Si | Medio | 7 |

Con lo anterior se detalla cual es la situación ideal para cada una de las eventualidades que podrían ocurrir.

* **Siniestros:** Se debe contar con extintores de incendios, los cuales permitan atacar el problema cuando ya se produjo pero no prevenirlo o dar la alarma para combatirlo en su inicio, por ello es necesario detectores de humo y sistemas de aspersión automática. Eliminar todo tipo de material inflamable dentro del área, ventilación adecuada. Tener una adecuada instalación del cableado eléctrico y datos, evitar el uso de artefactos eléctricos inadecuados altamente resistivos y capacitación al personal.
* **Robos:** Hay dos tipos de robos, uno tangible y otro intangible. En lo que respecta al robo de tangibles sólo se puede identificar a través de la seguridad interna del Hospital Clínico del Sur a cargo de la Gerencia respectiva. En cuanto al robo de intangibles, se considera el robo de tiempo de trabajo (horas- hombre y horas-máquina), el robo de información y también cualquier otro tipo de fraude relacionado. Contra el robo de tiempo de trabajo y los fraudes no se tiene protección, sólo se cuenta con normas como el Reglamento Interno de Hospital Clínico del Sur y la Ley del Trabajo, por lo cual seria necesario realizar su difusión a fin de inducir y sensibilizar a los usuarios, labor que estaría a cargo de la Gerencia respectiva. Actualmente la manera más frecuente de robar información es a través de Internet, fotos digitales, medios magnéticos de almacenamiento USB o en impresiones, este control deberá estar a cargo del funcionario responsable del área. Para el servidor principal de base de datos es conveniente tener un servidor de respaldo totalmente operativo para realizar el cambio lo más rápido posible.
* **Fallas de Hardware:** Todo hardware de reciente adquisición debería estar bajo garantía y en el caso especifico de fallas en el disco duro que podría ocasionar pérdida de información, se tiene en el servidor de BD configurado un sistema de backups periódicos de la base de datos del SISTEMA MK (el cual debe estar además en algún dispositivo óptico o disco externo en lo posible fuera de Hospital Clínico del Sur), y en ambos servidores se debería tener un backup periódico de todo el sistema e idealmente habilitar el sistema RAID. En cuanto a fallas de la fuente de alimentación, todos los servidores deben contar con un UPS (o control de voltaje en su defecto) y algunos con fuentes redundantes, para fallos mas graves como pérdida total de alimentación se podría contar con grupo electrógeno de alimentación para Hospital Clínico del Sur. Para el fallo de Equipos de Comunicación como los Access Point o Switch se debe tener uno de reserva que actuará inmediatamente en remplazo. Además siempre es necesario un mantenimiento preventivo, protección eléctrica óptima y reposición por tiempo de vida útil. Para el servidor principal de base de datos es conveniente tener un servidor de respaldo totalmente operativo para realizar el cambio lo más rápido posible.
* **Fallas de Software:** frente a este tipo de contingencia se debe contar con la reinstalación del software o la reconfiguración. Todo el software que se usa debe tener copias de respaldo. Los instaladores del sistema MK se encuentran en carpeta de soporte para su reinstalación en equipos clientes. Además se debe contar con formularios en papel para realizar el ingreso posterior de los datos. Para el servidor principal de base de datos es conveniente tener un servidor de respaldo totalmente operativo para realizar el cambio lo más rápido posible.
* **Errores Humanos:** Frente al borrado se cuenta con copias de respaldo de la base de datos del SISTEMA MK. Solo el administrador de la red puede recuperar una clave si existiera la necesidad de conocerla sin intervención del usuario.
* **Accesos no autorizados:** Se identifican dos casos, los accesos físicos y los accesos lógicos. En cuanto al acceso físico cada vez que la oficina queda sin personal informático se cierra con llave restringiendo la entrada del personal no autorizado a la oficina de Informática. En cuanto a los accesos lógicos, al igual que con los fraudes, se debe usar la protección de la red y de los sistemas de información fijado por las claves de acceso.
* **Virus Informáticos:** Los servidores y estaciones deben contar con licencia del antivirus respectivo. Asimismo contar con soporte y mantenimiento de los servidores de Correo Electrónico, Firewall-Proxy con lo cual asegurar la continuidad de las operaciones con el menor tiempo de paralización en caso de incidentes. Para el servidor principal de base de datos es conveniente tener un servidor de respaldo totalmente operativo para realizar el cambio lo más rápido posible.
* **Vandalismo Informático**: en lo que respecta la información se debe contar con los backups para la restauración de la información y en cuanto a equipos se debe tener la seguridad interna a cargo de la Gerencia respectiva.

# Emergencia

Presenta las acciones detalladas que deben ser llevadas a cabo durante la emergencia para mantener la continuidad de los procesos críticos en el momento de la materialización de los riesgos, para cada proceso crítico asociado a un riesgo, se define una acción o procedimiento a seguir.

Se detallan a continuación las principales acciones a tomar en la etapa de emergencia, destacando principalmente aquellas que afectan directamente el normal funcionamiento del SISTEMA MK.

Principalmente si alguna de las eventualidades descritas en los puntos anteriores se ejecutan se deben tomar las precauciones para realizar ingresos a mano sobre formularios de papel u hojas Excel para realizar los ingresos posteriores al restablecimiento del servidor principal de base de datos o el equipo de escritorio. Estos formularios recaen principalmente sobre los siguientes sistemas:

* Admisión
* Ambulatorio
* Agenda Médica
* Abastecimiento
* Contabilidad
* Facturación

Se debe tener algún servidor o equipo de escritorio de respaldo que se debe comenzar a preparar en la fase de recuperación de la eventualidad ocurrida.

En esta etapa es siempre conveniente tener contacto directo con Soporte MK para coordinar las acciones a tomar en la fase de recuperación.

# Recuperación

Para esta etapa se debe coordinar principalmente con Soporte MK las acciones a tomar, además es siempre conveniente tener en cuenta lo siguiente:

* Mantener las especificaciones para las configuraciones de hardware que deben ser instaladas en el Servidor y los diferentes equipos.
* Evaluar la instalación del software del sistema MK (al momento de la recuperación) con la asistencia del soporte MK ante cualquier eventualidad.
* Evaluar la instalación del Motor de Base de datos SQL y la carga de la base de datos de respaldo (al momento de la recuperación) con la asistencia del soporte MK.
* Implementar los procedimientos para generar y/o almacenar materiales que deben estar fuera del recinto de Hospital Clínico del Sur y son necesarios para la recuperación.
* Mantener un plano de la configuración de la red para ser implementada ante cualquier eventualidad.
* Evaluar los procedimientos de backup’s para establecer los distintos servicios (servidor, servidor web, equipos de escritorio, base de datos, correos, etc.).

La fase de recuperación para el servidor principal recae principalmente en preparar el servidor de respaldo si lo hubiera, instalando lo necesario para su funcionamiento, esto es:

* Windows Server 2003 32/64 bits en adelante, versiones standard o superior.
* SQL 2000 en adelante, versiones standard o superior.
* Internet Information Services (Para Servidor Web)
* Office 2007 o Superior
* Framework 4.0 - Crystal Reports (Se encuentran en Directorio Soporte\Prerrequisitos)
* Tener validados los usuarios de Windows en Servidor SQL.

Es importante tener instaladas las últimas actualizaciones (Service Pack), de los sistemas anteriormente mencionados.

Se deberán generar los siguientes directorios en el Servidor.

Directorio “Soporte” (c:\Soporte). Este debe tener permisos de lectura para los usuarios/grupos que trabajaran con el sistema. En este directorio se encuentran los siguientes datos: Manuales, Instaladores, Prerrequisitos Ejecutables, entre otros.

Directorio “RespaldosBD” (c:\RespaldosBD). En este directorio se encuentran los respaldos de la base del sistema.

Se recomienda mantener siempre un respaldo actualizado de ambos directorios en un lugar seguro, esto es, disco óptico o disco externo.

Posteriormente a la implementación de los prerrequisitos el proceso seria el siguiente:

* Previamente se coordina el horario de migración, dentro de este se deberá fijar una hora tope en el que el sistema deja de trabajar, y así los usuarios no deban ingresar al sistema. En ese horario se generan respaldos de las bases del SISTEMA MK para tener la última información ingresada.
* Eso significa que cualquier información ingresada al sistema posterior a la toma del backup, no será registrada.
* MasterKey restaura la base de datos en el nuevo servidor, instala los módulos del sistema y realiza pruebas de acceso al sistema en el servidor. Posteriormente y coordinando con personal de Hospital Clínico del Sur deberán realizar las pruebas a nivel de los clientes y confirmar si estos pueden trabajar con el sistema.
* Los usuarios de Windows deben ser validados en SQL, el número de estos variará según la naturaleza de la implementación, o sea Controladores de Dominio o Grupo de Trabajo, pudiendo validar desde un grupo hasta cada uno de los usuarios respectivamente.

Es necesario que todo lo que se menciona anteriormente se debe tener implementado, ya que sin esto, no se podrá continuar con la instalación del Sistema MK.

# Contacto Soporte

El contacto con la empresa MasterKey S.A. para soporte 24x7 es el siguiente:

Lunes a Viernes de 8:30 a 18:30 los siguientes teléfonos fijos:

* 32-2993200
* 32-2881980
* 32-2698255

Fuera de ese horario contactarse con los móviles:

* 74305211
* 74305213

Contacto vía correo electrónico:

* Rubén Golmo – [rgolmo@masterkey.cl](mailto:rgolmo@masterkey.cl)
* Gustavo Valladares – [gvalladares@masterkey.cl](mailto:gvalladares@masterkey.cl)
* Kevin Ramírez – [kramirez@masterkey.cl](mailto:kramirez@masterkey.cl)
* Rafael Moreno – [rmoreno@masterkey.cl](mailto:rmoreno@masterkey.cl)
* Álvaro Cortez – [acortez@masterkey.cl](mailto:acortez@masterkey.cl)
* Pablo Rojas – [projas@masterkey.cl](mailto:projas@masterkey.cl)
* Roger Nieto – [rnieto@masterkey.cl](mailto:rnieto@masterkey.cl)
* Rodrigo Ramírez – [rramirez@masterkey.cl](mailto:rramirez@masterkey.cl)
* Marco Gómez – [mgomez@masterkey.cl](mailto:mgomez@masterkey.cl)