MUNICIPALIDAD DE SAGRADA FAMILIA
INFORMÁTICA

PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE INFORMACION

NOVIEMBRE DEL 2008 – MAYO 2013

AUTOR : Ricardo Hormazàbal Sànchez.
CARGO : Informática Municipal

PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE INFORMACION

PRESENTACIÓN.

El Plan de Contingencia Informático implica un análisis de los posibles riesgos a los que pueden estar expuestos los equipos de cómputo y sistemas de información municipales. Corresponde a Informática municipal aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance de este plan guarda relación con la **infraestructura informática**, así como los **procedimientos relevantes** asociados con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del municipio. Los procedimientos relevantes de la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o humanos. La información como uno de los activos más importantes de la municipalidad, es el fundamento más importante de este Plan de Contingencia.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que el plan de contingencia Informático incluya el **Plan de Recuperación de Desastres** con el único objetivo de restaurar el servicio Informático en forma rápida, eficiente, con el menor costo y pérdidas posibles.

RESUMEN

La protección de la información ante la posible pérdida, destrucción, robo y otras amenazas de una empresa, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático. Dicho plan indica las acciones que deben tomarse inmediatamente tras el desastre. Un primer aspecto importante del plan es **la organización de la contingencia**, en el que se detallan los nombres de los responsables de la contingencia y sus responsabilidades. El segundo aspecto crítico de un Plan de Contingencia es la preparación de **un plan de respaldo (Backup)**, elemento primordial y necesario para la recuperación. El tercer aspecto es la preparación de un **plan de recuperación**. La municipalidad debe establecer su capacidad real para recuperar información crítica en un periodo de tiempo aceptable.

La base del plan de contingencia y posterior recuperación, es establecer prioridades claras sobre **qué tipo de procesos son los más esenciales**. Es necesario por tanto la identificación previa de cuales procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

El plan de contingencia informático, debe contemplar los planes de respaldo (backup), emergencia y recuperación los que deben comprobarse mediante simulaciones y retroalimentación del mismo. Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio. No debe limitarse a estas medidas organizativas. También debe expresar claramente:

- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- Qué protocolos de actuación deben seguir y cómo son.

La Dirección debe comprender los principales riesgos para la municipalidad y las posibles consecuencias de un desastre. Un Plan de contingencia adecuado identifica las necesidades de todos los departamentos e involucra a TODO el personal de todas las direcciones/departamentos municipales.

INDICE

CAPITULO III: PLAN DE RESPALDO, EMERGENCI A Y DE RECUPERACIÓN DEL DESASTRE.

CAPITULO I. ANALISIS DE LA SITUACIÓN ACTUAL DE LA INFORMÁTICA MUNICIPAL DE SAGRADA FAMILIA.

1.1. Introducción

El hardware y el software están expuestos a diversos factores de riesgo humano y físicos. Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y de la estrategia a seguir previamente definidas. ¿Qué componente ha fallado?, ¿Cuál es el dato o archivo con información que se ha perdido?, ¿en que día y hora se ha producido y cuán rápido se descubrió? Estos problemas menores y mayores sirven para retroalimentar los procedimientos y planes de seguridad de la información.

Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (los discos duros), por grandes desastres naturales (incendios, terremotos), hechos humanos (sabotajes, operación errónea) o por fallas técnicas (virus informático) que producen daño físico y lógico irreparable. Frente al mayor de los desastres sólo queda el tiempo de recuperación, lo que significa adicionalmente una fuerte inversión en recursos humanos y técnicos para reconstruir el sistema de red y los sistemas de información.

1.2. Objetivos e Importancia del Plan de Contingencia

Objetivos

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los sistemas de Información.

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un sistema de Información.

Importancia

- Garantiza la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.

- Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que de el se puedan derivar.

- Permite realizar un Análisis de Riesgos, respaldo de los datos y su posterior recuperación. En general, cualquier desastre es un evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

- Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

1.3. Sistema de Red municipal

Informática municipal está a cargo del :
Hardware, comunicaciones, sistemas de información, conectividad y servicios Informáticos que se brinda de forma interna y externa a las diferentes direcciones, departamentos. Se resume que la administración de Red esta dividido en
dos rubros: 1) Conectividad: encargada de la conexión alámbrica e inalámbrica de los equipos de comunicación y 2) Manejo de servidores: se encarga de alojar todos los servicios y sistemas de comunicación e información.

Los servicios de Red implementados en la Municipalidad son los siguientes:

- Servidor de Bases de datos del proyecto Sifim
- Servidor de datos de desarrollo comunitario.

1.4. Sistema de Información municipales.

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, documentación y bibliografía.

El listado de Sistema de Información municipales se detalla a continuación:

- Sistema de contabilidad gubernamental
- Sistema de Tesorería Municipal
- Sistema de Órdenes de Ingreso
- Sistema de conciliación bancaria.
- Sistema de planificación presupuestaria
- Sistema de datos comunes.
- Sistema de personal municipal
- Sistema de remuneración municipal
- Sistema de patentes comerciales.
- Sistema de permisos de circulación
- Sistema de licencias de conducir.
- Sistema de oficina de partes.

- Sistema de control de facturas.
- Sistema de causas civiles y criminales (J.P.L.)
- Sistema de adquisiciones.
- Sistema de inventario municipal.
- Sistema de bodegas (D.O.M.)
- Sistema de libro de bancos.
- Sistema de desarrollo comunitario.

CAPITULO II ANÁLISIS DE RIESGOS.

El plan de contingencias implica la realización de un análisis de todas las posibles causas a las que pueden estar expuestos los equipos conectados a la red de datos municipal así como la información contenida en cada medio de almacenamiento. Se realizará un **análisis de riesgo** y el **plan de operaciones** tanto para reducir la posibilidad de ocurrencia como para reconstruir el sistema de Información y/o sistema de red de computadoras en caso de desastres. Incluye la formación de equipos de trabajo durante las actividades de establecimiento del **plan de Acción**, tanto para la etapa preventiva, correctiva y de recuperación.

2.1. Análisis de Riesgos

Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal
b) Hardware
c) Software y utilitarios
d) Datos e información
e) Documentación
f) Suministro de energía eléctrica
g) Suministro de comunicaciones

Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información, proceso de información no deseado.

c) Divulgación de información fuera de la institución y que afecte su patrimonio estratégico, sea mediante robo o Infidencia.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la municipalidad son:

- Acceso no autorizado
- Detección de las claves de acceso a los sistema computacionales
- Desastres Naturales: a) Movimientos telúricos b) Inundaciones causadas por fallas en los suministros de agua c) Fallas en los equipos de soporte (causadas por la agresividad del ambiente, falla en la red de energía eléctrica, falla en los equipos de acondicionamiento atmosférico, fallas en la comunicación, fallas en el tendido físico de la red de la red local, fallas en la central telefónica)
- Fallas de Personal Clave o vital en el procesamiento de datos: por los siguientes inconvenientes: a) Enfermedad b) Accidentes c) Renuncias d) Abandono de sus puestos de trabajo e) Otros. Imponderables.
- Fallas de Hardware: a) Falla en los Servidores b) Falla en el hardware de Red (Switches, cableado de la Red, Router, Gateway, FireWall)
- Incendios

2.1.1. Características

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la organización
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un plan adecuado. Los criterios que se usarán para tipificar los posibles problemas son:

Tabla 1. Escala de Valores para Criterios de Posibles Problemas

Criterios	Escala			
Grado de negatividad	Leve	moderado	Grave	muy grave
Posible frecuencia del evento negativo	Nunca	Aleatorio	Periodico	continuo
Grado de impacto o consecuencias	Leve	moderado	grave	muy grave
Grado de certidumbre	Nunca	Aleatorio	proable	seguro

2.1.2. Clases de riego

2.1.2.1. Clase de Riesgo: Incendio o Fuego

Grado de Negatividad : Muy Severo
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
El área de Servidores cuenta con un extintor cargado pero No al día.	Recargar extintor
En Educación y Salud no existen extintores.	Instalar extintores
No se ejecuta un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	Implantar un Programa de Capitación para el manejo de extintores.

Una probabilidad máxima de contingencia de este tipo en la municipalidad, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de servidores tendría un impacto mínimo, por las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los respaldos de información. Un incendio es más que suficiente para destruir los dispositivos de almacenamiento, tal como CD, DVD, Blueray, discos duros externos, aunque estén en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor). Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocarán estratégicamente en lugares distantes, con una segunda copia de seguridad custodiada en un lugar externo a la Municipalidad, de preferencia en un **data center**.

2.1.2.2. Clase de Riesgo: Robo Común de Equipos y Archivos

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Moderado
Grado de Certidumbre : Aleatorio

Situación actual	Acción correctiva
Vigilancia permanente.	La salida de un equipo informático es registrada por el personal de Informática (número de serie). No obstante ha habido robo de notebooks.
El Personal de seguridad cumple con su obligación de cerrar puertas y ventanas al finalizar su jornada.	Se cumple
Remitir aviso a Informática para retirar equipo informático.	Se Cumple

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre algún Jefe de Departamento/ Dirección e Infomática municipal. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

Es relativamente fácil remover un disco duro del CPU, tarjeta y no darse cuenta de ello hasta días después. Estas situaciones no se han presentado, pero se recomienda siempre estar alerta.

2.1.2.3. Clase de Riesgo: Falla en los Equipos por problemas eléctricos.

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
La red de datos del proyecto Sifim posee una red eléctrica estabilizada y una UPS para el servidor de 30 minutos de duración	No es necesario corregir.
No existe un adecuado tendido eléctrico en desarrollo comunitario	Proponer un Estudio para instalar red eléctrica estabilizada
Existe un generador eléctrico; pero no tiene encendido automático y alimenta sólo a Finanzas y Alcaldía	Estudio de encendido automático y extender cobertura a toda la municipalidad
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo.	Existe Mantenimiento de los equipos de cómputo. Contar con proveedores, en caso de requerir reemplazo de piezas, y de ser posible tener repuestos a la mano
La duración de las baterías de la central telefónica es muy breve y un corte prolongado genera problemas de comunicación.	Contar con baterías en buen estado y de mayor duración y resetear la central telefónica en caso de problema mayor.

Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente por el uso de las U.P.S., pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día aunque se cuenta con generador eléctrico con los inconvenientes mencionados.

Para el adecuado funcionamiento de los computadoras personales, necesitan de una fuente de alimentación eléctrica limpia. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía mas frecuentes:

- Fallas o cortes de energía
- Transistores y pulsos
    - Bajo voltaje
    - Ruido electromagnético
    - Distorsión

- Variación de voltaje.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de alzas.
- Estabilizadores
- Sistemas de alimentación ininterrumpida (UPS)

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra

Se denomina así a la comunicación entre el circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura el aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón

vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

La Toma a Tierra tiene las siguientes funciones principales: a) protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las superficies metálicas, b) protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales., c) facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las inspecciones deben realizarse **semestralmente**, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los **meses de verano**. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Fusibles y diferenciales

Al cablear la computadora, la carcaza normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad se fugara a través del aislante y llegase a la carcaza, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (un fusible se debe sustituir tras fundirse, un diferencial se debe restaurar tras saltar).

Si una parte de un computador funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema se puede a conectar el equipo.

Extensiones eléctricas

Se deben usar los enchufes tipo “magic”, sin embargo a veces es imprescindible usar extensiones eléctricas (alargadores). El uso de éstas debe ser controlado con cuidado. No solo para que no queden a la vista, si no también porque suponen un peligro considerable

para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.
Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso,

- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase mas corriente de la que los cables están diseñados para soportar.

- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales

- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperes que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.

- Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener conexión a tierra.

2.1.2.4. Clase de Riesgo: Equivocaciones

Grado de Negatividad : Moderado
Frecuencia de Evento : Periódico
Grado de Impacto : Moderado
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos y normas
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor específica.
El no cumplimiento de los procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para fortalecer los procedimientos.
Informática municipal no recibe comunicación del personal de reemplazo por vacaciones o llegada de nuevos usuarios.	Se debe informar a Informática el reemplazo para su registro y accesos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores.
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet	Enviar via mail comunicando los nuevos cambios y políticas.

2.1.2.5. Clase de Riesgo: Acción de Virus Informático

Grado de Negatividad : Muy Severo
Frecuencia de Evento : Continuo
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
Se cuenta con un software antivirus NO corporativo con licencia por dos años. No hay contrato de renovación automática	El software debe ser corporativo. Se debe renovar oportunamente.
Todo Software (oficina, desarrollo, mantenimiento, drivers, etc.) es manejado por personal de Informática, quienes son los encargados de su instalación en las PC's con su respectivo antivirus.	Se cumple.
Se tiene un programa permanente de bloqueo de acciones como cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple.
Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de loguear un equipo a la red (dominio) se comprueba al existencia de virus en la PC.	Se cumple

En estos últimos años la acción del virus informático ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software (Kaspersky) el que es actualizado automáticamente con licencia por dos (2) años.

2.1.2.6. Clase de Riesgo: Fenómenos Naturales

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
El terremoto del 2010 no afectó a la sala de Informática, sí a equipos en oficinas de adobe los que , sin embargo, continuaron operativos. La salida de	Ampliar oficina de Informática, mejorar vías de

emergencia de la oficina de Informática es crítico por lo reducido de la oficina y estantes existentes. No se han presentado inundaciones, aluviones, etc.	escape.
Ingreso de agua lluvia en el techo (gatera)	Ubicación apropiada. Pero ante resultado de filtraciones realizar trabajos de mantenimiento preventivo.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos en la sala de Informática, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal.
Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital.

2.1.2.7. Clase de Riesgo: Accesos No Autorizados

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
Se controla el acceso al Sistema de Red mediante la definición de “Cuenta” o “Login” con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los “Atributos de confianza” para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones,	Se cumple

Se forman Grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos	Se cumple
A veces se entregan contraseñas a compañeros de trabajo.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que implica.

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de seis (6) caracteres. No se permiten claves en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos. Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas de información, si lo tuviere.

2.1.2.8. Clase de Riesgo: Robo de Datos

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
Las Oficinas tienen disponible grabadores de CD/DVD, puertos USB, pero no se lleva un control estricto la información que ingresa y/o sale del PC.	Usuarios deben controlar los accesos de sus equipos respectivos.
El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica	Existe Manual de normas que regulan el uso y acceso de Internet.

Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático del UNP el problema persistirá.	Resguardar la información en archivos. Destruir reportes con máquinas trituradoras.

El robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar “copia no autorizada” a nuestros archivos electrónicos en un medio magnético u óptico y retirarla fuera de la municipalidad.
- La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.
- La tercera modalidad es la remisión de información vía Internet a direcciones de correo que no corresponden a la gestión municipal.

2.1.2.9. Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad : Grave
Frecuencia de Evento : Aleatorio
Grado de Impacto : Grave
Grado de Certidumbre : Probable

Situación actual	Acción correctiva
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadasa causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje.	La protección contra el sabotaje requiere: una selección rigurosa del personal. Buena administración de los recursos humanos, buenos controles administrativos, buena seguridad física en la oficina de informática.

No se comunica el movimiento de personal al CIT, para restringir accesos del personal que es reubicado y/o cesado en la Muniipalidad	Comunicar movimiento de personal a Informática.

El peligro más temido por los centros de Informática es el sabotaje. Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más difíciles. Éste puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios.
Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existe un plan idóneo o una recomendación simple para resolver el problema dela seguridad. Realmente no es una situación estática o un problema “puntual”, sino que requiere un constante y continuo esfuerzo y dedicación.

2.2. Protecciones actuales

Se realizan las siguientes acciones:

- Se hacen copias diarias de los archivos que son vitales para la institución.
- Para prevenir el robo común se cierran las puertas de entrada.
- A la falla de los equipos, se realiza el mantenimiento de forma regular.
- Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
- A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se debe capacitar.

- A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias sólo da pautas al respecto.
- Al acceso no autorizado, se cierra la puerta de entrada
- Al robo de datos, se cierra la puerta principal y cajones de escritorios.
- Al fuego, en la actualidad se encuentran instalados extintores en sitios estratégicos.

2.2.1. Seguridad de información

La Seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas e incluso la vida privada de las personas. Ladrones, manipuladores, saboteadores reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque. La Seguridad de información tiene tres directivas básicas que actúan sobre la protección de los datos, a saber:

- La lectura
  Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
- La escritura
  Es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso.
- El empleo de esa información
  Es Secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos. Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

2.2.1. 1. Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

- Control de acceso a la oficina de Informática

El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

La forma propuesta de implantar el Control de Acceso a Informática, seria la siguiente:

- Para personas visitantes otorgar Credencial de Visitante.
- Para personal municipal, con autorización del encargado de lnformática.

- Acceso limitado a computadoras personales y/o terminales de la red.
- Control de acceso a la información confidencial.

Sin el debido control, cualquier usuario encontrara la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada.

2.2.1. 2. Destrucción de la información.

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos y bases de datos.

2.2.1. 3. Revelación o Deslealtad

La revelación o deslealtad es otra forma que utilizan trabajadores deshonestos para su propio beneficio. La información de carácter confidencial es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

- Control de uso de información en paquetes/ expedientes abiertos, cintas/CD, DVD y otros datos residuales.

- Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de ella a personas que pueden usar mal los datos residuales de estas.
- Mantener información impresa o magnética fuera del trayecto de la basura. El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadoras o trituradoras de papel).
- Preparar procedimientos de control para la distribución de información. Una manera de controlar la distribución y posible derivación de información, es mantener un rastro de copias múltiples indicando la confidencialidad o usando numeración como “pag 1 de 9”

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de la Oficinas y relativamente disponible a gran número de personas.

2.2.1. 4. Modificaciones

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

- Los programas de aplicación: adicionalmente a proteger sus programas de aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.

- La información en Bases de Datos: como medidas de Seguridad, para proteger los datos en el sistema, efectuar auditorias y pruebas de consistencia de datos en nuestros respaldos históricos. Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

- Nuestra mejor protección contra la perdida/modificación de datos consiste en hacer copias de seguridad, almacenando en

copias autorizadas de todos los archivos valiosos en un lugar seguro

- Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados

.

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

 ¿Que soporte de copias de seguridad se va utilizar?

 ¿Se van a usar dispositivos especializados para copia de seguridad?

 ¿Con que frecuencia se deben realizar las copias de seguridad?

 ¿Cuales son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

Informática municipal establecerá directivas y/o Reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación educativa.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

 Hacer de la copia de seguridad una política, no una opción.

 Hacer de la copia de seguridad resulte deseable.

 Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).

 Hacer de la copia de seguridad un proceso obligatorio.

CAPITULO III: PLAN DE RESPALDO, EMERGECIA Y RECUPERACIÓN DEL DESASTRE.

El costo de la recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía aseguradora.

El costo de recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 7 o un incendio controlable, estará dado por el valor no asegurado de equipos informáticos e información más el costo de oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal de Informática, personal de Seguridad.

Las actividades a realizar en un Plan de Recuperación de Desastres se clasifican en tres
etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

3.1. Actividades previas al desastre

Se considera las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para la institución.

3.1.1. Establecimientos del Plan de Acción

En esta fase de planeamiento se establece los procedimientos relativos a:

a. Sistemas e Información.
b. Equipos de Cómputo.
c. Obtención y almacenamiento de los Respaldos de Información (BACKUPS).
d. Políticas (Normas y Procedimientos de Backups).

a. Sistemas de Información

La Institución deberá tener un listado de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas .Los *Sistemas y Servicios críticos* para la Informática Municipal son los siguientes:

Lista de Sistemas

- Sistema de contabilidad gubernamental
- Sistema de Tesorería Municipal
- Sistema de Órdenes de Ingreso
- Sistema de conciliación bancaria.
- Sistema de planificación presupuestaria
- Sistema de datos comunes.
- Sistema de personal municipal
- Sistema de remuneración municipal
- Sistema de patentes comerciales.
- Sistema de permisos de circulación
- Sistema de licencias de conducir.
- Sistema de oficina de partes.
- Sistema de control de facturas.
- Sistema de causas civiles y criminales (J.P.L.)
- Sistema de adquisiciones.
- Sistema de inventario municipal.
- Sistema de bodegas (D.O.M.)
- Sistema de libro de bancos.
- Sistema de desarrollo comunitario.

Lista de servicios
Sistema de comunicaciones
Servicio de correo corporativo
Servicios Web: Publicación de páginas Web, noticias de la UNP,
 Internet, Intranet.
 VPN: servicios de acceso privado a la red de la Institución desde cualquier
lugar.
 Servicio de Monitoreo de la red: monitorea los equipos de comunicación
distribuidos en la red la UNP.
 Servicios de telefonía Principal: teléfonos IP
 Servicios de enseñanza de manera virtual.
 Servicio de Antivirus
 Servicio de Antivirus

b. Equipos de Cómputo

Se debe tener en cuenta el inventario de Hardware, impresoras, scanner, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

- Backup del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la Red.
- Backup del software aplicativo: backups de los programas fuente y los programas ejecutables en caso de desarrollos propios.
- Backups de los datos (Base de datos, passsword y todo archivo necesario para la correcta ejecución del software aplicativos de la institución).
- Backups del Hardware, se puede implementar bajo dos modalidades:

Modalidad Externa: mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una contingencia mientras se busca una solución definitiva al siniestro producido.

En este Caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, etc., que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.
Modalidad Interna: si se dispone de más de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia.
Es importante mencionar que en ambos casos se debe probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado
de los sistemas.

d. Políticas (Normas y Procedimientos)

Se debe establecer procedimientos, normas y determinación de responsabilidades en la obtención de los “Backups” o Copias de Seguridad. Se debe considerar:

- Periodicidad de cada tipo de backup: los backups de los sistemas informáticos se realizan de manera diferente:

⇒ Sistemas de la empresa CAS Chile del proyecto Sifim se realiza backup diario.

- Respaldo de información de movimiento entre los periodos que no se sacan backups: días no laborales, feriados, etc. en estos días es posible programar un backup automático.
- Uso obligatorio de un formulario de control de ejecución del programa de backups diarios, semanales y mensuales: es un control a implementar, de tal manera de llevar un registro diario de los resultados de las operaciones del backups realizados y su respectivo almacenamiento.
- Almacenamiento de los backups en condiciones ambientales optimas, dependiendo del medio magnético empleado.
- Reemplazo de los backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar. No se realiza reemplazos pero se realiza copias de las mismas, considerando que no se puede determinar exactamente el periodo de vida útil del dispositivo donde se ha realizado el backup.
- Almacenamiento de los backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local). Esta norma se cumple con la información histórica, es decir se tiene distribuidos los backups de la siguiente manera: una copia reside en las instalaciones de Informática Municipal y una segunda copia reside en la Caja fuerte de Rentas Municipales.

- Pruebas periódicas de los backups (Restore), verificando su funcionalidad, a través de los sistemas comparando contra resultados anteriormente confiables.

Esta actividad se realizara haciendo una comparación entre el contenido de la primera y segunda copia realizada o con el contenido de la información que se encuentra el Servidor de información histórica.

3.1.2. Formación de equipos operativos

En cada unidad operativa, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el Jefe Administrativo de dicha Área. Sus funciones serán las siguientes:

 Contactarse con los autores de las aplicaciones y personal de mantenimiento respectivo.

El equipo encargado en Informática Municipal está formado por las siguientes unidades:

- Unidad de Comunicaciones
- Unidad de Soporte Tecnológico.
- Unidad de Administración de Servidores.

 Proporcionar las facilidades (procedimientos, técnicas) para realizar copias de respaldo.

Esta actividad esta dirigida por el Equipo de Soporte y Mantenimiento.

 Supervisar el procedimiento de respaldo y restauración

 Establecer procedimientos de seguridad en los sitios de recuperación

 Organizar la prueba de hardware y software: el encargado y el usuario final dan su conformidad.

 Ejecutar trabajos de recuperación y comprobación de datos.

 Participar en las pruebas y simulacros de desastres: en esta actividad deben participar el encargado de la ejecución de actividades operativas, y los servidores administrativos del área, en el cumplimiento de actividades preventivas al desastre del Plan de Contingencias.

3.1.3. Formación de Equipos de Evaluación (Auditoria de cumplimiento de los procesos de seguridad)

Esta función debe ser realizada preferentemente por el personal de auditoria, de no ser posible, lo realizaría el personal del área de

informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:
 Revisar que las normas y procedimientos con respecto a backups, seguridad de equipos y data se cumpla.
 Supervisar la realización periódica de los backups, por parte de los equipos operativos, es decir, información generada en el área funcional, software general y hardware.
 Revisar la correlación entre la relación de los Sistemas e información necesarios para la buena marcha de la institución y los backups realizados.
 Informar de los cumplimientos e incumplimientos de las normas para las acciones de corrección necesarias.

3.2. Actividades durante el Desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:
a. Plan de Emergencias
b. Formación de Equipos
c. Entrenamiento

a. Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.
Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a *buscar ayuda inmediatamente* para evitar que la acción del siniestro causen más daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de carabineros y bomberos. Todo el personal debe conocer lo siguiente:

- Localización de vías de Escape: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape

- Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esa actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.
- Ubicación y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.
- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, ambulancias, Seguridad.

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 2 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

3.3. Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son
las siguientes:
a. Evaluación de Daños.
b. Priorización de Actividades del Plan de Acción o recuperación
c. Ejecución de Actividades.
d. Evaluación de Resultados.
e. Retroalimentación del Plan de Acción o recuperación.

a. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuánto tiempo.
En el caso de Informática Municipal se debe atender los procesos de contabilidad, tesorería, administrativo, documentarios; que son las actividades que no podrían dejar de funcionar, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades del Plan de Acción o recuperación.

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución.
Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse un problema, reportarlo de inmediato a la Jefatura a cargo del Plan de Contingencias.
Los trabajos de recuperación tendrán dos etapas:

- La primera la restauración del servicio usando los recursos de la institución o local de respaldo.
- La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no

perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectado por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, qué tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de Acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción o recuperación.

Con la evaluación de resultados, debemos de optimizar el Plan de Acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionan adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no contar con el Plan de Contingencias en la institución.

3.4. Acciones frente a los tipos de riesgo.

3.4.1. Clase de Riesgo: Incendio o Fuego.

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local.

Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento

b) Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.

c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento

d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.

e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

 Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.

 No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.

 Verificar las condiciones de extintores y capacitar para su manejo.

 Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se
hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.

 No almacenar sustancias y productos inflamables.

 No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.

 Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.

 Si se detecta cualquier anomalía en los equipos de seguridad (extintores, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Dirección de Obras.

 Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de
las causas que provocan incendios.

 Tener a la mano los números telefónicos de emergencia.

DURANTE

 Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

 En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el servidor central, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente de Informática municipal.

 Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si éste es
considerable no trates de extinguirlo con los propios medios, solicitar ayuda.

 Si el fuego está fuera de control, realizar evacuación del inmueble, siguiendo las
indicaciones del personal de bomberos.

 Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo boca y nariz con un pañuelo bien mojado y respirar a través de el,

 Si es posible mojar la ropa.

 Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

 Retirarse inmediatamente del área incendiada y ubicarse en la zona de seguridad externa que corresponda.

 No obstruir las labores del personal especializado, dejar que los profesionales se
encarguen de sofocar el incendio.

 El personal calificado realizara una verificación física del inmueble y definirá si está en condiciones de ser utilizado normalmente.

 Colaborar con las autoridades.

3.4.2. Clase de Riesgo: Robo común de equipos y archivos.

Analizar las siguientes situaciones:

 En qué tipo de vecindario se encuentra la Institución?

 Las computadoras se ven desde la calle?

 Hay personal de seguridad en la Institución y están ubicados en zonas
Estratégicas?

 Cuánto valor tienen actualmente las Bases de Datos?

 Cuánta pérdida podría causar en caso de que se hicieran públicas?
 Asegurarse que el personal es de confianza, competente y conoce los
procedimientos de seguridad.
 Revisar el trabajo no supervisado, las malas técnicas de contratación, evaluación y de despido de personal.

3.4.3. Clase de Riesgo: Vandalismo.

 Si el intento de vandalismo es mayor implica un grave riesgo dentro de la oficina de Informática ya que puede dañar los dispositivos perdiendo toda la información y en consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.
 A continuación se menciona una serie de medidas preventivas:
- Establecer vigilancia mediante cámaras de seguridad en el lugar, el cual
registre todos los movimientos de entrada del personal.
- Instalar identificadores mediante tarjetas de acceso.
- Determinar lugares especiales, fuera de Informática, para almacenar
los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (data center).

 Los principales conflictos que pudieran presentarse son:
- En cuanto a la red, si el sistema llegará a presentar una falla no habría
personal que atendiera la problemática y por consecuencia se detendrían
las operaciones a falta del monitoreo a los distintos sistemas.
- Respecto a los dispositivos de almacenamiento, si se mantienen los
respaldos únicamente dentro de la Municipalidad, sería
imposible reanudar las actividades que en un momento dado fueran críticas,
como la contabilidad gubernamental.

3.4.4. Clase de Riesgo: Equivocaciones.

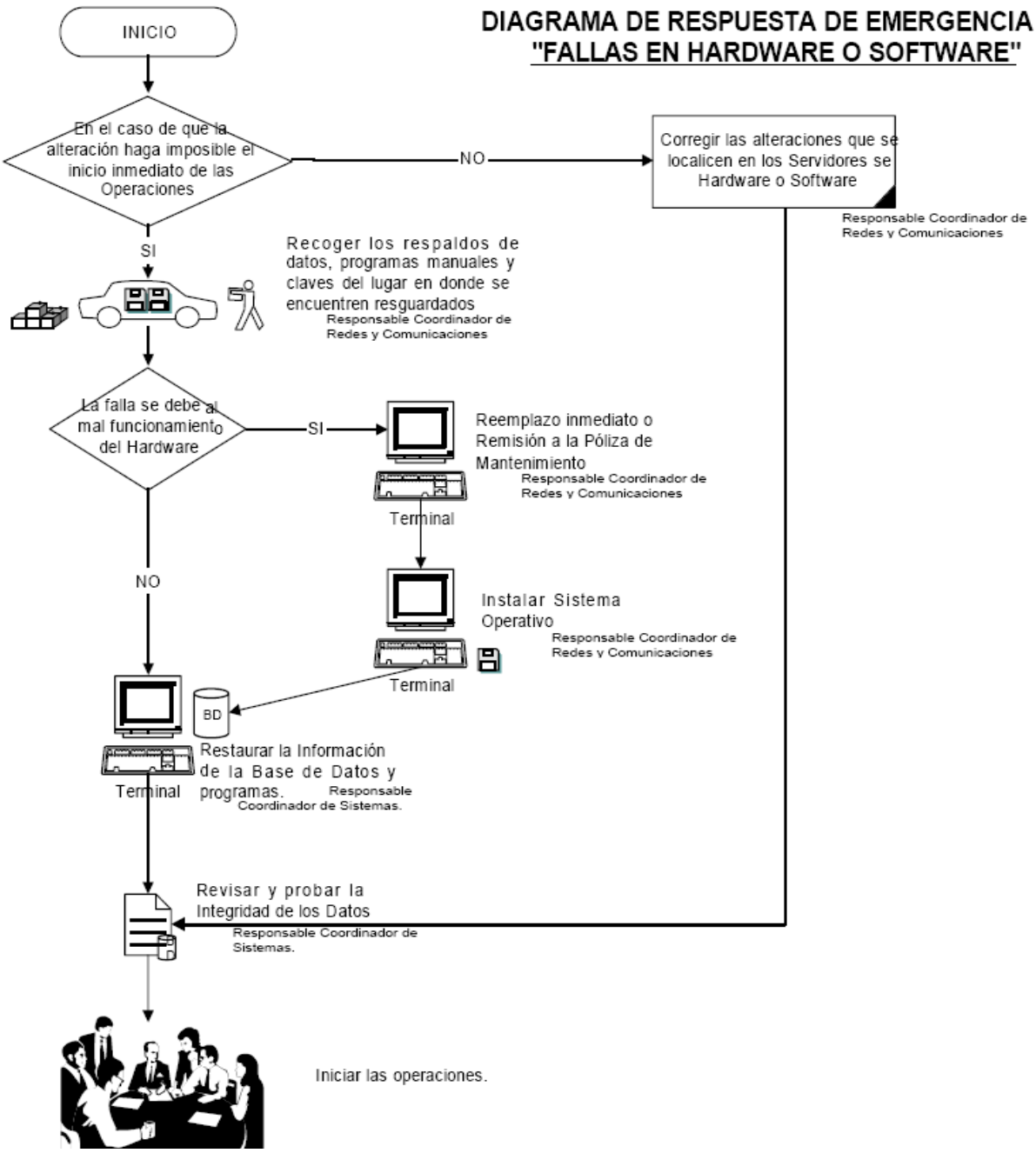
 Cuánto saben los empleados de computadoras o redes.
 Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los
sustituye y qué tanto saben del manejo de computadoras?

 Difusión de Manuales de Usuario y operación del correcto uso del software y el
hardware a todo el personal que labora de manera directa con los equipos
informáticos.

3.4.5. Clase de Riesgo: Fallas en los equipos por problemas eléctricos.

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos o a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo o de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la figura A2.

FIG. A2. DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "FALLAS EN HARDWARE O SOFTWARE"



Casos

- **Error Físico de Disco de un Servidor (Sin R.A.I.D.).**

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser
reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Verificación el buen estado de los sistemas.
8. Habilitar las entradas al sistema para los usuarios.

 Error Físico de Disco del servidor del proyecto Sifim (con R.A.I.D.).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:
1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de departamentos/direcciones afectados
2. Habilitar de inmediato servidor alternativo (HP) cargando el último respaldo de las bases de datos para permitir continuidad de servicios.
3. Ubicar el disco malogrado.
4. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
5. Bajar el sistema y apagar el equipo.
6. Retirar el disco malo y reponerlo con otro del mismo tipo, reconstruir r.a.i.d. correspondiente.
7. Ejecutar master de restauración del servidor HP Proliant DL 380 G6 (Pendrive de 16 Gb)
8. Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad. Reconstruir usuarios.
9. Verificación el buen estado de los sistemas.
10. Habilitar las entradas al sistema para los usuarios.

 Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco

En el caso de las memorias RAM, se dan los siguientes síntomas:
• El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.
• Ante procesos mayores se congela.
• Arroja errores con mapas de direcciones hexadecimales.
• Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la municipalidad, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el switch correspondiente, ello evitará que al encender el sistema, los usuarios ingresen
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el switchr, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

Falla en las estaciones de trabajo

Si la sección de informática municipal no solucionare inmediatamente el problema, se retirará la unidad y si es crítica su continuidad de trabajo será reemplazada por otra mientras se repara el equipo.

Desperfecto de impresoras.

Previa evaluación del encargado de informática la impresora será dada de baja, o bien, enviada a servicio técnico especializada. Si se requiere será sustituida por otra unidad.

Desperfecto de monitores.

Se deberán reemplazar momentáneamente por los monitores de emergencia con que se cuentan mientras se envian al servicio técnico especializado.

Desperefecto de teclados y mouse.

Previa evaluación del encargado de informática municipal serán dados de bajo y adquiridas nuevas unidades.

Desperfecto de scanners.

Se reempalzarán por equipos alternativos. No obstante y previa evaluación, se deberá comprar nuevas unidades.

Desperfecto de cables U.T.P. nivel 6 de interconexión de la red.

En tal caso se cuenta con “chicotes” cruzados (cable “cross over”) que se instalarían entre los switchs y routers y entre éste y la Gateway de la empresa proveedora de Internet. Si el problema estuviera en el cable de conexión de alguna estación de trabajo se deberá subir al entretecho y parchar el cable, o bien, reemplazarlo por otro nuevo. Ambos trabajos se realizarán por el encargado de Informática municipal.

Desperfecto de switchs.

Se deberá contar con dos unidades de switch de reemplazo en caso de estar quemados o con problemas de colisión prolongados y que serán instalados por el encargado de Informática.

Desperfecto del router.

Se deberá contar con otro router de reemplazo para subsanar problemas de quema, el cual debe ser instalado por administrador de la red municipal.

Desperfecto de la pasarela (Gateway) de la empresa proveedora de Internet/Telefonía.

Este dispositivo es de responsabilidad de la empresa proveedora de Internet, por lo tanto, en tal caso se deberá llamar a soporte técnico para que lo evalúen en terreno previo llamado del administrador de la red municipal.

Interrupción de las Comunicaciones con la planta de la empresa proveedora de Internet.

Este problema debe subsanarlo la empresa proveedora de Internet, por lo que se deberá llamar a soporte técnico para su solución previa evaluación del administrador de la red municipal.

 Error de la central telefónica Hipath 3550

Resetear:
1.- Apagar (off) elswitch de la batería.
2.- desenchufar cable de alimentación.
3.- Sacar conector de tarjeta principal.
4.- Enchufar cable de alimentación.
5.- Encender (on) el switch de la batería.
6.- Esperar que el visor dl teléfono digital conectado muestre la información correspondiente.
7.- Poner conector de la tarjeta principal.
8.- Cerrar carcasa.

3.4.6. Clase de Riesgo: Acción de Virus Informático.

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:
Para servidor:
• Se contará con antivirus para el sistema; aislar el virus para su futura investigación.
• El antivirus muestra el nombre del archivo infectado y quién lo usó.
• Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:
• Utilizar los discos de instalación que contenga sistema operativo igual o posterior a la versión instalada en el computador infectado.
• Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.

3.4.7. Clase de Riesgo: Accesos No Autorizados.

Enfatiza los temas de:
 Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. Informática municipal implementa la complejidad en sus contraseñas de tal forma que sean mas de siete caracteres y consistentes en números y letras.

 Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

 Privilegio. En los sistemas informáticos municiales, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado.
Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en “Grupos” con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

3.4.8. Clase de Riesgo: Fenómenos naturales.

a) Terremoto e Inundación

 Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm de altura.
 En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
 Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local,
 Cuando el daño ha sido menor se procede:
a) Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento
b) Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
c) Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento
d) Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.
e) Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

3.4.9. Clase de Riesgo: Robo de Datos.

Se previene a través de las siguientes acciones:

 Acceso no Autorizado: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas.
- Computadoras personales y/o terminales de la red.
- Información confidencial.

 Control de acceso al Área de Sistemas: El acceso al área de Informática estará restringido:

- Sólo ingresan al área el personal que trabaja en el área.
- El ingreso de personas extrañas solo podrá ser bajo una autorización.

 Acceso Limitado a los Terminales: Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Designación del usuario por terminal.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).

 Niveles de Acceso: Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

- Nivel de consulta de la información.- privilegio de lectura.
- Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

3.4.10. Clase de Riesgo: Manipulación y Sabotaje.

 La protección contra el sabotaje requiere:

1. Una selección rigurosa del personal.
2. Buena administración de los recursos humanos.
3. Buenos controles administrativos.
4. Buena seguridad física en los ambientes donde están los principales componentes del equipo.

5. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.
 A continuaciones algunas medidas que se deben tener en cuenta para evitar acciones hostiles:
1. Mantener una buena relación de trabajo con el departamento de policía local.
2. Mantener adecuados archivos de reserva (backups).
3. Planear para probar los respaldos (backups) de los servicios de procesamiento de datos.
4. Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
5. Usar rastros de auditorias o registros cronológicos (logs) de transacción como medida de seguridad.
 Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:
- Capturar los datos faltantes en las bases de datos de los sistemas. Responsable:

Áreas afectadas
- Revisar y probar la integridad de los datos. Responsable: Desarrollo de Sistemas.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados.

CONCLUSIONES

 El presente Plan de contingencias y Seguridad de la Municipalidad de Sagrada Familia tiene como objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información extremando las medidas de seguridad para protegerse y estar preparados a una contingencia de cualquier tipo.

 Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, evaluación de riesgos, Asignación de prioridades a las aplicaciones, establecimiento de los requerimientos de recuperación, elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.

 Un Plan de Contingencia es la herramienta que la institución debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

 Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un plan de Contingencia.

RECOMENDACIONES

 Programar las actividades propuestas en el presente Plan de Contingencias y Seguridad de Información.

 Divulgar el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal municipal.

 Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

 Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad municipal.