MUNICIPALIDAD DE ILLAPEL
ALCALDIA

LA ALCALDÍA DECRETA HOY LO QUE SIGUE

DECRETO EXENTO N° 1.690.
MAT.: Aprueba Plan de Contingencia Informático.

ILLAPEL, 25 de Octubre de 2013.

VISTOS Y TENIENDO PRESENTE: a) Lo dispuesto en el artículo 37, letra i) del Decreto Supremo N° 83, del año 2004; b) Las atribuciones que me otorga la Ley N° 18.695, Orgánica Constitucional de Municipalidades; c) Decreto Alcaldicio N° 90 de fecha 06 de diciembre de 2012, en que don Denis Cortés Vargas, asume el cargo de Alcalde de la Municipalidad de Illapel, por un periodo de 04 años.

DECRETO

APRUÉBESE, Pan de Contingencia Informático, para asegurar continuidad de operaciones en la Municipalidad de Illapel; cuyo texto se entiende formar parte del presente Decreto Exento.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

JOSÉ VALLEJOS BASUALTO
SECRETARIO MUNICIPAL (S)

DENIS CORTÉS VARGAS
ALCALDE

D. C .V./J. V. B. /V. V. A./poo.
DISTRIBUCIÓN:
- Contraloría Regional.
- Secretaría Municipal.
- Administración Municipal.
- Departamentos Municipales.

Plan de contingencia informático

I Municipalidad De Illapel

Informática 2013

INDICE

1. Plan de contingencia para asegurar continuidad de operaciones informáticas en la institución. I Municipalidad Illapel.

Se entiende por plan de contingencia a una serie de acciones de carácter preventivo, predictivo y reactivo ante situaciones inesperadas que afecten el normal funcionamiento de una institución.

Este plan contiene una serie de procedimientos informáticos alternativos que se deben adoptar si los equipos tecnológicos fallan y afectan el flujo normal de trabajo, por lo tanto, cuando alguna de las funciones cotidianas se ve perjudicada, ya sea por una eventualidad interna o externa, estos planes deben garantizar la continuidad operacional informática de cada área.

2. Funcionarios a cargo:

Personal de informática.

3. Posibles amenazas:

- Alzas o bajas de voltaje.
- Cortes de energía de poca o larga duración.
- Catástrofes naturales como temporales o terremotos.
- Siniestros producidos por acción humana.
- Mal uso de usuarios.
- Ataques informáticos.
- Actualizaciones que corten temporalmente los servicios.
- No pago de servicios.
- Virus informático.
- Mal estado de equipamiento.

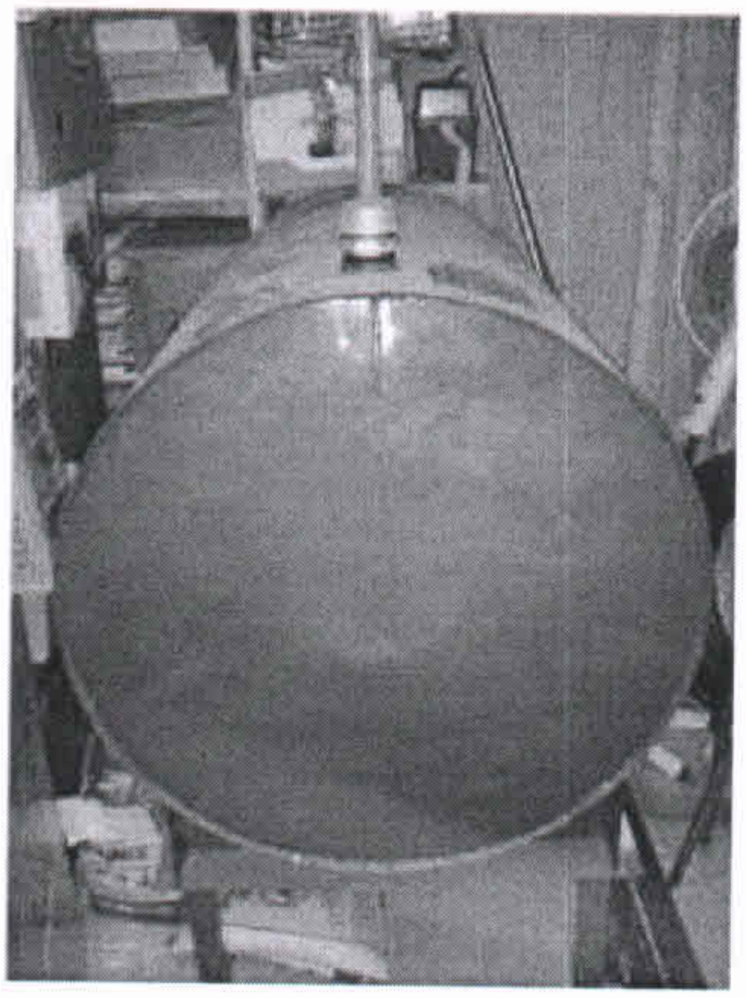
3.1 Impacto de las amenazas

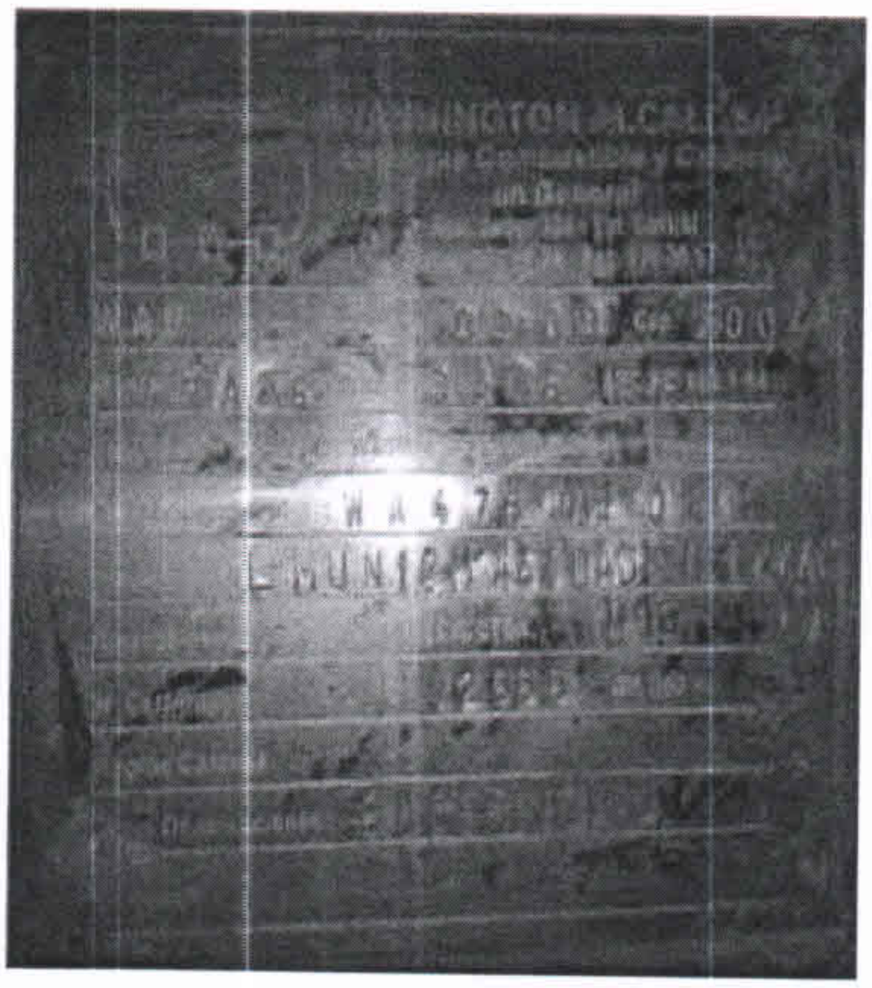
Las amenazas influyen directamente en los sistemas informáticos y sistemas de telecomunicación dentro de la municipalidad, pudiendo detener casi la totalidad de las operaciones realizadas en los distintos departamentos, siendo los mayores afectados: Transito, Finanzas, Juzgado de policía local, Informática, educación y salud. Por otro lado existe la necesidad de estar comunicados con la ciudadanía por medio de sistemas externos de gobierno o contacto telefónico, es por esto que ningún departamento quedaría libre de daños o pérdidas.

4. Plan de respaldo

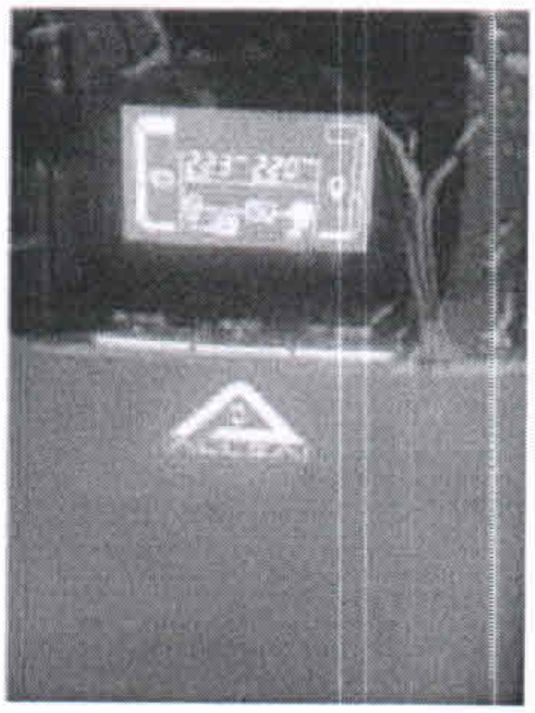
4.1 Energía: La Municipalidad de illapel cuenta con un generador ubicado en el subterráneo capaz de mantener alimentado circuitos de emergencia en el edificio por un periodo aproximado de 48 horas. Este generador tiene las siguientes características.

Generador: Washington Alcadep.
Tipo combustible: petróleo.
Capacidad: 500 litros.
Duración: aproximadamente 48 horas (no comprobado).





Además tanto el servidor principal que contiene los sistemas Sifim y giradores, el sistema de asistencia biométrica, centrales telefónicas, switch y equipos informáticos están protegidos por UPS marca "ALLSAI" capaz de alimentar central y switch por 2 horas continuas y UPS HP para servidor que alimenta por 4 horas.



4.2 Protección física: todo el equipamiento principal (servidor, central telefónica, switch) están ubicados en una sala especialmente acondicionada donde solo el equipo informático tiene acceso, evitando el daño causado por personas no autorizadas.
Los equipos están situados sobre racks metálicos antisísmicos capaces de protegerlos de golpes.
Dentro de la sala existe equipamiento de aire acondicionado el que se debe mantener entre 17°C y 20°C.
Todo el cableado es de categoría 6 y está protegido por escalerillas metálicas.

5. Protección de datos:

1-En el caso del servidor SIFIM:
Se respalda automáticamente todos los días a las 21:00 hrs, quedando una copia en el disco local, la que luego es copiada semanalmente a dos discos externos. Además de esto una empresa externa "intesis" es la encargada de mantener una copia actualizada de las bases de datos, dejando esta información en el data center de la moneda, Santiago. (Ver anexo procedimiento para el correcto funcionamiento de las aplicaciones y bases de datos del servidor SIFIM de la municipalidad)

2-Para el caso de los equipos de los usuarios:
Estos según la configuración ya definida deben ser respaldados todos los viernes a cierta hora según el departamento, este respaldo es previamente acordado con el usuario, guardando solo la información imprescindible según su trabajo. La ubicación final de estos respaldos es un servidor NAS ubicado en la sala de servidores.

Cada computador cuenta con protección antivirus, malware y con cuentas limitadas para que los usuarios no tengan privilegios de administrador y así evitar desconfiguraciones.
En casos excepcionales se habilita la cuenta de administrador. El motivo de esto es porque algunos sistemas o software logran un correcto funcionamiento con cuentas que tengan todos los permisos y no estén limitadas.

3. Para el caso de la red interna:
Esta se encuentra protegida por un firewall Forinet fortigate 50 que restringe la entrada y salida de conexiones, además de todo el cableado protegido por escalerillas metálicas en entretecho.

4. Acceso de usuarios:
Todo sistema interno y externo debe estar protegido con ingreso mediante contraseña para cada uno de sus usuarios.
Las contraseñas deben contener letras y números.

5. Para el caso de servidores internos:
Se crean backups semanalmente de las bases de datos, codigos fuentes, archivos multimedias y archivos generales.

Para más información ver "políticas de respaldo"

6. Plan de emergencia

En caso de problemas o cortes de energía eléctrica:
Los generadores y ups deben comenzar a trabajar inmediatamente sin interrumpir el funcionamiento normal de los equipos. Si alguno no continúa operando, el personal de informática es el encargado de chequear cada uno para identificar y corregir el problema. Por otro lado el departamento de operaciones es el encargado de revisar tableros, puntos eléctricos, generadores, etc. y restablecer servicios eléctricos.

En caso de falla en el servidor SIFIM:
La empresa Cas Chile es la encargada de dar soporte a situaciones como errores en base de datos para los sistemas Sifim y giradores, siendo esta falta de información o errores en los datos arrojados. Además de dar soporte en las aplicaciones clientes.

Si se presenta alguna falla que impida el trabajo en todos los sistemas, por ejemplo una falla en hardware o software que no tenga solución inmediata, se debe acudir a la empresa Intesis, que dentro de su plan de emergencia conecta los equipos clientes al servidor externo ubicado en el data center de la moneda, Santiago, donde el equipo informático solo debe cambiar la dirección ip dentro del archivo host re direccionando las aplicaciones de cada computador mientras se soluciona el problema en el servidor local.

En caso de problemas con los sitios alojados en servidor externo al municipio:

Se debe realizar la Limpieza total, parcial o reemplazo del sitio afectado a través de los respaldos hechos con anterioridad, utilizando el servicio FTP Filezilla (OPEN SOURCE), desde el servidor o por el FTP del servicio hosting.

- Informar a través de la cuenta (chat o email), a los técnicos de soporte del servicio hosting del status offline del sitio afectado, para volver a estar online en el menor tiempo posible.
- Se debe realizar el cambio de clave, a la vez esta debe ser modificada mensualmente. todo cambio en cuentas de acceso debe quedar registrado y debe ser de conocimiento de todos los usuarios habilitados.
- Las claves a modificar deben ser las siguientes:
    - sistema joomla u otro de gestión de contenido.
    - cliente ftp del sitio web.
    - servicio hosting.

En caso de problemas con servidores internos:
El personal de informática debe chequear y corregir problemas de red, sistema operativo, software de base de datos, software de gestión, código fuente de sistemas y todo harware y programa involucrado en su correcto funcionamiento.

Si los problemas se presentan en bases de datos y aplicaciones, se deben cargar nuevamente con los backup más actualizados.
Si los problemas son de harware, se debe reponer la pieza dañada, de lo contrario si el daño es mayor se repone el servidor por otro equipo con similares características o que sea capaz de brindar el servicio sin complicaciones.

Para el caso del sistema biométrico de asistencia:
Se debe contactar con la empresa punto seguro para que dé solución a los problemas presentados.

En caso de problemas con correos municipales:
Se debe realizar un chequeo inicial del problema, según esto, se realizan las correcciones siempre y cuando estén al alcance del equipo informático de la municipalidad.
Todo problema mayor como caídas en el servicio, errores al cargar la cuenta, no envío ni recepción de correos, debe ser informada a DreamHost a través de su contacto o chat online para una rápida solución. Además si es necesario se debe restaurar la cuenta del usuario con los backup almacenados según lo indiquen los técnicos del servicio.

En caso de problemas con el servicio de internet y telefonía:
La empresa proveedora de servicio ISP debe ser capaz de dar solución al problema según los tiempos de respuesta estipulados en los contratos.

En caso de problema con la información de los usuarios:
Cuando un usuario tenga pérdida de información ya sea por robo de equipo o pérdida de dato accidental o intencionalmente, se debe buscar el último respaldo guardado en el servidor Nas y reponer parte o la totalidad de la información perdida. De no contar con este respaldo, utilizando las copias de seguridad automática se puede volver a un punto anterior. Esto no garantiza que el usuario recupere la información y es por esta razón que constantemente se recomienda mantener una copia personal de los archivos más importantes e ir guardando los cambios a medida que se modifican dichos documentos.

Si el equipo presenta fallas se siguen los mismos pasos mencionados, otorgando al usuario un equipo temporal para que continúe el flujo de sus funciones.

7. Contactos

Contacto Cas Chile : Fono +56(2) 24966900
Mail: alvaro.setien@caschile.cl (jefe de proyecto)
Web: www.caschile.cl

Contacto Intesis : Fono +56 2 271 336 00 / +569 83693292
Mail: cchen@intesis.cl (Senior IT Engineer)
Web: www.intesis.cl

Contacto Punto Seguro : Fono: (562) 2220 2336 / (562) 2417 7345
Mail: contacto @puntoseguro.cl
Web: www.puntoseguro.cl

La empresa punto seguro es la encargada de dar soporte al sistema de biometría para el control de asistencia municipal. Si se presenta algún problema, ellos deben ser capaces de corregir o guiar al informático para llegar a la solución esperada.

Contacto DreamHost: web: www.dreamhost.com/contact y llenar formulario
-ingresando mediante cuenta de administrador a la sección Chat Live

8. Plan general de recuperación

1. Reparar fallas de hardware o software en servidor.
2. Reponer la totalidad de los datos guardados en servidor externo en servidor interno.
3. Reponer bases de datos (backup) y verificar su correcto funcionamiento.
3. Reparar fallas de hardware o software en equipos de usuarios
3. Configurar equipos para reconectar a servidor interno (redireccionar).
4. Reparar fallas en sistemas (clientes).
5. Reponer los datos en equipos de usuarios verificando su integridad.
6. Reparar y corregir problemas en generadores eléctricos y Ups.
7. Reponer cableado si este presenta fallas.
8. Cambio de equipamiento que resulte afectado sin posibilidad de repararlo.
9. Evaluar contactos y tiempos de respuesta de empresas responsables.
10. Revisar todo el plan de contingencia y modificarlo s es necesario.