MUNICIPALIDAD PROVINCIAL DEL CALLAO
SECRETARIA GENERAL
CERTIFICA:
Que esta copia concuerda con su original que se conserva en el Archivo de éste Municipio
Callao, 26 AGO. 2011

MUNICIPALIDAD PROVINCIAL DEL CALLAO
SECRETARIA GENERAL - GACMA
ALEXANDER DIAZ PINEDO
Jefe (e) Unidad de Coordinación y Apoyo

MUNICIPALIDAD PROVINCIAL DEL CALLAO
ALCALDÍA

Resolución de Alcaldía Nº 1061 -2011-MPC-AL

Callao, 26 AGO. 2011

EL ALCALDE DE LA MUNICIPALIDAD PROVINCIAL DEL CALLAO.

Visto: el Informe Nº 155-2011-MPC-GI, remitido por la Gerencia de Informática, por el cual solicita la aprobación del Plan de Contingencia de los Equipos Informáticos y de Comunicaciones de la Municipalidad Provincial del Callao; y,

CONSIDERANDO:

Que, de acuerdo a lo señalado en el Artículo II del Título Preliminar de la Ley Orgánica de Municipalidades - Ley N° 27972, las municipalidades son órganos de gobierno local que gozan de autonomía política, económica y administrativa en los asuntos de su competencia;

Municipalidad Provincial del Callao Vº Bº Gerencia Municipal

Que, mediante el documento de visto la Gerencia de Informática, remite para su aprobación el Plan de Contingencia de los Equipos Informáticos y de Comunicaciones de la Municipalidad Provincial del Callao, con el objetivo de definir y programar la implementación de medidas de seguridad que garanticen el funcionamiento continuo de los equipos informáticos y de comunicaciones de la Institución;

Que, dada la importancia del mismo, resulta necesario se expida la respectiva Resolución de Alcaldía, aprobando dicho plan;

Estando a las consideraciones expuestas, con el visto bueno de la Gerencia General de Planeamiento, Presupuesto y Racionalización, Gerencia General de Asesoría Jurídica y Conciliación y Gerencia Municipal, en ejercicio de las atribuciones conferidas al Alcalde por la Ley Orgánica de Municipalidades Nº 27972;

Municipalidad Provincial del Callao Gerencia de Informática Vº Bº

RESUELVE:

ARTÍCULO 1º Aprobar el **PLAN DE CONTINGENCIA DE LOS EQUIPOS DE INFORMATICA Y DE COMUNICACIONES DE LA MUNICIPALIDAD PROVINCIAL DEL CALLAO**, el mismo que consta de 13 folios y forma parte de la presente Resolución.

ARTÍCULO 2º Notifíquese a todas las dependencias el contenido de la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

Municipalidad Provincial del Callao Vº Bº G.G.A.J.C.

MUNICIPALIDAD PROVINCIAL DEL CALLAO
GEORGE COLLANTES FERNANDEZ
SECRETARIO GENERAL

MUNICIPALIDAD PROVINCIAL DEL CALLAO
JUAN SOTOMAYOR GARCIA
ALCALDE

MUNICIPALIDAD PROVINCIAL DEL CALLAO

PLAN DE CONTINGENCIA DE LOS EQUIPOS INFORMÁTICOS y DE COMUNICACIONES

PLAN DE CONTINGENCIA DE LOS EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES

I. ASPECTOS GENERALES

El Plan de Contingencia implica identificar y analizar los posibles riesgos a los cuales pueden estar expuestos los Equipos Informáticos (servidores, estaciones de trabajo, laptops, impresoras, dispositivos de almacenamiento y periféricos) y de Comunicaciones (router, switch, hubs, access point, antenas y cableado de datos), por lo que en este plan se hará un análisis de los riesgos para reducir su posibilidad de ocurrencia que permita establecer los procedimientos para atender de manera: oportuna, eficiente y eficaz; ante un desastre, consecuencia de un fenómeno natural, incidentes a nivel interno o externo en la Municipalidad.

II. OBJETIVOS

- Definir y programar la implementación de las medidas de seguridad que garanticen el funcionamiento continúo de los equipos informáticos y de comunicaciones en la Municipalidad Provincial del Callao.
- Establecer el plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad de los sistemas informáticos en el menor tiempo posible.
- Establecer las actividades que permitan evaluar los resultados y la retroalimentación del presente plan.

III. BASE LEGAL

- Reglamento de Organización y Funciones de la Municipalidad Provincial del Callao, aprobado por Ordenanza Municipal Nº 000067.
- Manual de Organización y Funciones de la Municipalidad Provincial del Callao.
- Normas y documentos sobre la elaboración de Planes de Contingencia, que presentó y aprobó el Instituto Nacional de Estadística e Informática – INEI, y que ha hecho suyos la Presidencia del Consejo de Ministros, en su rol de entidad encargada de normar el Sistema Nacional de Informática.
- Normas Técnicas de Control Interno, aprobadas por Resolución de Contraloría N° 320-2006-CG.
- Resolución Ministerial Nº 19-2011-PCM. Aprueban la formulación y evaluación del Plan Operativo Informático de las entidades de la Administración Pública y su Guía de Elaboración.

IV. FINALIDAD

Disponer de un plan que permita atender de manera ordenada y prevista las situaciones que pongan en riesgo la operatividad de los Equipos Informáticos y de Comunicaciones en la Municipalidad Provincial del Callao, estableciendo procedimientos que eviten interrupciones en su operación.

V. ALCANCE

El presente Plan de Contingencia es de observancia y estricto cumplimiento para todo el personal de **LA MUNICIPALIDAD PROVINCIAL DEL CALLAO**, sea cual fuere su régimen laboral.

Se aplica a todos los locales institucionales de la Municipalidad donde se encuentren instalados los **EQUIPOS INFORMÁTICOS y DE COMUNICACIONES**, que están bajo responsabilidad de la **GERENCIA DE INFORMÁTICA**.

VI. DE LA GERENCIA DE INFORMÀTICA

Es el órgano de la Municipalidad Provincial del Callao, que administra, opera y supervisa los equipos informáticos, los sistemas informáticos y de comunicaciones del Municipio.

VII. VIGENCIA

El presente Plan de Contingencia tendrá vigencia de doce (12) meses, contados a partir del día siguiente de su aprobación.

VIII. ANÁLISIS DE RIESGOS

Los equipos informáticos y de comunicaciones están expuestos a distintas clases de riesgos, que pueden afectar su normal funcionamiento. Los problemas potenciales se clasifican en los siguientes factores:

8.1 Naturales y/o Artificiales

Originados por causas externas al Municipio y cuyo grado de previsión es muy reducido. Se consideran dentro de este grupo a los **factores naturales** como: terremotos, maremotos, entre otros similares; **factores artificiales** como: incendios, inundaciones, robos y problemas de terrorismo.

Estos percances generan pérdidas o daños físicos en el local de la Municipalidad Provincial del Callao.

8.2 Servicios

Los riesgos identificados en este grupo pueden generar la interrupción del procesamiento de la información en línea, lo que afectaría seriamente la atención al público; por ejemplo:

- Caídas en los circuitos dedicados de comunicaciones.
- Corte de energía eléctrica.

8.3 Sistema Informático

Estos riesgos están asociados con el funcionamiento de los equipos, cuyo deterioro o mal uso puede implicar lo siguiente:

- Daños en los componentes de los equipos de informática, entiéndase hardware, (discos duros, adaptadores de red, placa, interfaces y memoria).
- Fallas en los dispositivos de comunicaciones (switches, hub, routers, antenas y access point).
- Desperfectos en los equipos de cómputo é impresoras de los usuarios de las distintas áreas del Municipio.
- Daños en los archivos del sistema operativo por causa de errores del hardware o software.
- Software corrupto o incompatible (copia sin licencia).
- Virus que infecten los archivos y dañen los equipos de cómputo.

8.4 Recursos Humanos

Está relacionado a la atención del personal de mantenimiento encargado de los equipos de informática y de comunicaciones por causa en la demora de atención por desperfectos; daños en los archivos, equipos y otros dispositivos que requieren del personal.

8.5 Otros Factores

Se incluyen en esta clasificación otros riesgos que no se encuentren comprendidos en las clasificaciones anteriores. Por ejemplo: Derrame de líquidos en los equipos.

IX. PLAN DE CONTINGENCIA

9.1 El Plan de Contingencia de Equipos de Cómputo y Comunicaciones considera los siguientes aspectos:

- Las actividades que deben realizar los grupos de trabajo o los responsables de cada área.
- El control, referido a las pruebas y las verificaciones periódicas, sobre la operatividad y la actualización del plan de contingencia.

9.2 Forman parte del plan de contingencia:

- Plan de reducción de riesgos o plan de seguridad.
- Plan de recuperación de desastres.

9.3 El plan de recuperación de desastres se clasifica en tres fases:

- Actividades previas al desastre.
- Actividades durante el desastre.
- Actividades después del desastre.

9.3.1 Actividades previas al desastre

a. Establecimiento del plan de acción, que comprende:

a.1.- Sistema de información: son los sistemas o aplicaciones administrados por el Municipio tales como: Sistemas de Gestión

Administrativa (Sistema Integrado de Gestión Administrativa – SIGE, Sistema de Trámite Documentario, Sistema de Control de Asistencia de Personal) y Sistemas de Gestión Municipal (Sistema de Rentas, Sistema de Licencia de Funcionamiento, Sistemas de Tesorería, Sistema Texto Único de Procedimientos Administrativos - TUPA), Sistemas Operativos y aplicaciones de Internet.

a.2.- Equipos de cómputo: Se dispone con el inventario de hardware y software, especificación técnica, ubicación física y el área a la que está asignada de acuerdo al código patrimonial del Municipio.

La Gerencia de Informática es la responsable de identificar las computadoras de acuerdo a su importancia, para lo cual se deberá hacer uso del inventario de los equipos de informática, el mismo que proporcionará la información para realizar los reemplazos del mismo.

a.3.- Obtención y almacenamiento de los Respaldos de Información (Backup), que incluye:

- Backup de los Sistema de Gestión Administrativa.
- Backup de los Sistema de Gestión Municipal.
- Backup del Sistema Operativo por servidor.
- Backup del Software Base (paquetes y/o lenguajes de programación con los cuales han sido desarrollados o interactúan los aplicativos institucionales). Backup del Software Aplicativo.
- Backup de la base de datos.

El procedimiento para los equipos, por sus características técnicas y capacidades, es susceptible de ser usado en equipos de emergencia.

a.4.- Políticas (normas y procedimientos de backup), que considera:

- Determinación de las responsabilidades para la obtención del backup; realizándose de la siguiente forma:

  - Sistema de Gestión Administrativa, Sistema de Gestión Municipal y Sistemas Críticos se realiza diariamente.
  - Sistemas Operativos se realiza Semanalmente.
  - Data en General mensualmente.

- Almacenamiento del backup en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo del backup, en forma periódica, antes que el medio magnético de soporte se deteriore (reciclaje o refresco).

b. Formación de equipos operativos, mediante la designación del responsable de los equipos de informática y de comunicaciones, en cada órgano, tendrán las siguientes funciones:

- Comunicarse con los propietarios de los equipos de informática, proporcionando el soporte técnico para la realización de las copias de respaldo de su información y las aplicaciones de sus equipos.

- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a los archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar los procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones y la creación de respaldos incrementales.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Realizar los procedimientos de control de de inventario y seguridad del almacenamiento
- Participar en las pruebas de simulacros de desastres.

c. Formación de equipos de evaluación, para la supervisión de los procedimientos de seguridad; cuyas funciones se detallan:

- Revisar la aplicación y cumplimiento de las normas y procedimientos con respecto al backup, seguridad de equipos y data.
- Supervisar la realización periódica de los backup, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de sistemas e información necesarios para la buena marcha del Municipio, y los backup realizados.
- Informar sobre el cumplimiento e incumplimiento de las normas para la toma de acciones y corrección respectivas.

9.3.2 Actividades durante el desastre

a) **Plan de emergencias:** Señalización de los extintores.

b) **Formación de equipos:** El personal de la Gerencia de Informática es el responsable del salvamento de equipos informáticos, de acuerdo a la prioridad del equipo.

c) **Entrenamiento:** Establecer un programa de prácticas periódicas para el personal, contra los diferentes tipos de siniestros, de acuerdo a los roles asignado en los planes de evacuación de personal o equipos.

La Gerencia de Abastecimiento deberá coordinar en las fechas de recarga de los extintores para gestionar y realizar charlas informativas, capacitaciones y entrenamientos con los organismos vinculados a siniestros (por ejemplo: Defensa Civil).

El personal debe tomar conciencia de que los siniestros (incendios, inundaciones, terremotos, tsunamis, apagones, etc.) pueden ocurrir en cualquier momento, y deben asumir con seriedad y responsabilidad las capacitaciones y los entrenamientos.

Los Funcionarios del Municipio están en la obligación de participar en todas las actividades antes mencionadas.

9.3.3 Actividades después del desastre

a) **Evaluación de los daños:** Concluido el siniestro, se deberá evaluar la magnitud del daño producido.

- ¿Qué sistemas y equipos se afectaron?
- ¿Qué equipos se encuentran en estado no operativo?
- ¿Cuáles se pueden recuperar y en qué tiempo?

b) **Priorizar las actividades del plan de acción:** Si el plan de acción es general y contempla una pérdida total; la evaluación de los daños y su comparación contra el plan, proporcionará la lista de las actividades a realizar en función de la prioridad. Es importante evaluar la dedicación del personal a las actividades que puedan no haberse afectado, a fin de asignarlos, en forma temporal, a las actividades que han sido afectadas, como apoyo al personal y soporte técnico.

c) **Ejecución de actividades:** Conformación de equipos de trabajo para realizar las actividades. Cada uno de los equipos deberá contar con un coordinador responsable, que deberá reportar diariamente el avance de los trabajos de recuperación y en caso de producirse algún problema, reportarlo, de inmediato, a la Unidad Orgánica a cargo del Plan de Contingencia.

El trabajo de recuperación consta de dos etapas:

- Primero: Restauración del servicio usando los recursos del Municipio;
- Segundo: Contar con los recursos necesarios en las cantidades y lugares apropiados, debiendo ser esta etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad del Municipio.

d) **Evaluación de resultados:** Concluida la labor de recuperación de los sistemas informáticos, equipos informáticos y de comunicaciones, afectados por el siniestro, se debe evaluar cada una de las actividades realizadas, considerándose entre otros aspectos:

- ¿Cómo evaluaría los resultados de las labores realizadas?
- ¿Qué tiempo demandó el trabajo de restauración?
- ¿Qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción?
- ¿Cómo se comportaron los sistemas, equipos informáticos y de comunicaciones?

De la Evaluación de resultados y del siniestro, deben obtenerse dos tipos de recomendaciones:

- Retroalimentación del plan de Contingencias
- Recomendaciones para minimizar la pérdida que ocasionó el siniestro.

e) **Retroalimentación del Plan:** Con la evaluación de los resultados, se debe optimizar el plan original, mejorando las actividades que tuvieron

algún tipo de dificultad, reforzando los elementos que funcionaron adecuadamente.

Evaluar ¿cuales hubieran sido los costos al no contar con un Plan de Contingencia?

9.4 El riesgo es la probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y de comunicaciones. El análisis supone obtener una evaluación económica del impacto de dichos sucesos negativos. El valor calculado se utiliza para contrastar el costo de la protección de la información con el costo de una nueva producción.

Se consideran los siguientes **factores** de riesgo:

- Factor de riesgo muy bajo.
- Factor de riesgo bajo.
- Factor de riesgo medio.
- Factor de riesgo alto.
- Factor de riesgo muy alto.

Se realizará un resumen de los riesgos ordenados por el factor de riesgo de cada uno de ellos contemplados en la presente Directiva.

9.5 El análisis de riesgos debe responder a las siguientes preguntas para determinar su grado de confiabilidad:

- ¿Cuál es el impacto para el Municipio?
- ¿Con qué frecuencia pueden ocurrir los desastes?
- ¿Cuáles serían las consecuencias para el Municipio?

9.6 La evaluación de riesgos debe responder a las siguientes preguntas con la mayor confiabilidad:

- ¿Qué se va a proteger?
- ¿Cuál es el valor para el Municipio o la persona?
- ¿Cuál es la probabilidad de un siniestro?

9.7 Los órganos del Municipio, sin excepción, están obligados a brindar todo el apoyo necesario a la Gerencia de Informática.

9.8 La Alcaldía, Gerentes, Jefes de Oficina, según sea el caso, designarán a los responsables de cada área, para que brinden el apoyo al personal de la Gerencia de Informática ante qué riesgos se enfrenta el Municipio:

- **Fuego,** que puede destruir los equipos y archivos.

  - La institución cuenta con protección contra incendios.
  - Se cuenta con sistemas de aspersión automática.
  - Extintores en cada área.
  - Detectores de Humo.
  - Los empleados están preparados para enfrentar un posible incendio.

- **Robo común,** llevándose los equipos y los archivos.

9.10 La Alcaldía, Gerentes, Jefes de Oficina, según sea el caso, dispondrán que el personal realice con carácter obligatorio las siguientes acciones de protección de los equipos de informática.

- **Generales:** Una copia mensual de los archivos que son vitales para la Institución.
- **Robo común:** Cerrar las puertas de entrada y ventanas de cada Oficina en coordinación con el personal de seguridad del Municipio.
- **Vandalismo:** Cerrar las puertas de ingreso en coordinación con el personal de seguridad del Municipio.
- **Fallas de los equipos:** Realizar el mantenimiento de forma constante. Debe preverse el préstamo de equipos, según el tipo de usuario, para los casos de reparación.
- **Daño por virus:** Todo el software y archivos que llega debe ser analizado en un sistema, utilizando software antivirus actualizado y licenciado. Los programas de dominio público y de uso compartido, sólo se usarán si proceden de una fuente fiable.
- **Terremoto:** Aplicar la protección contra incendio.
- **Inundaciones:** Mantener cerradas las llaves o grifos de los servicios higiénicos. No mantener los equipos de cómputo en el piso, apagar las llaves de alimentación eléctrica al concluir la jornada laboral.
- **Acceso no autorizado:** Cerrar la puerta de entrada. La vigilancia debe rondar por los pasillos de las instalaciones de la Municipalidad Provincial del Callao.
- **Robo de datos:** Mantener cerrada la puerta principal y oficina. Todas las computadoras de los usuarios deben estar bloqueadas con claves de acceso.
- **Fuego:** Colocar extintores en sitios estratégicos. La Gerencia de Abastecimiento debe coordinar y gestionar:

  - Charlas informativas
  - Entrenamiento
  - Capacitaciones

  Para el uso adecuado de los equipos especializado contra incendios.

X. DISPOSICIONES ESPECIFICAS

10.1 La Gerencia de Informática, es la responsable de formular, programar, realizar, coordinar, ejecutar, evaluar y controlar el Plan de Contingencia de los equipos informáticos y de comunicaciones.

10.2 La Gerencia de Administración y Finanzas, a través de la Gerencia de Abastecimiento, es la responsable del entrenamiento en el uso de extintores, para lo cual deberá programar las fechas en que se realizará: charlas informativas, capacitaciones y entrenamientos.

10.3 La Gerencia de Administración y Finanzas, a través de la Gerencia de Abastecimiento, es la responsable de proporcionar a la Gerencia de Informática el inventario de equipos informáticos y de comunicaciones, debidamente actualizados.

10.4 La Alcaldía, Gerentes, Jefes de Oficina, según sea el caso y bajo responsabilidad, proporcionarán a la Gerencia de Personal los datos del responsable que formará parte del equipo del Plan de Contingencia del Municipio, dentro de los (05) días útiles de aprobado el presente Plan. El nombre del responsable no debe coincidir con el nombre de personal alguno de la Gerencia de Informática.

10.5 La Gerencia de Personal, en coordinación con la Gerencia de Informática, elaborará y ejecutará, dentro de los treinta (30) días calendarios posteriores a la aprobación del Presente Plan, la encuesta o cuestionario (contemplados en el numeral **(9.8)** que se entregado a cada Unidad Orgánica. El personal institucional está en la obligación, bajo responsabilidad, en desarrollar objetivamente la encuesta o cuestionario que la Gerencia de Informática le presentará. El desarrollo de esta será en un solo acto.

10.6 Previo al desarrollo de la encuesta o cuestionario, La Gerencia de Informática en coordinación con la Gerencia de Personal, brindará charlas al personal.

10.7 La Alcaldía, Gerentes, Jefes de Oficina, según sea el caso, brindarán a su personal las facilidades para el cumplimiento de los objetivos.

XI. DISPOSICIONES COMPLEMENTARIAS

11.1 El Plan de Contingencia de equipos informáticos y de comunicaciones tiene la clasificación de prioridad muy alta.

11.2 La Gerencia de Informática, en coordinación con la Gerencia de Personal, son las áreas responsables de velar por el estricto cumplimiento de lo dispuesto en el presente Plan.

11.3 El Personal del Municipio, independientemente de su nivel y cargo, forma parte como un todo del Plan de Contingencias.

11.4 La Gerencia de Personal, en coordinación con la Gerencia de Informática, remitirá vía correo electrónico, a cada trabajador del Municipio, el presente Plan.

11.5 El personal deberá comprometer a lo establecido en el presente Plan, bajo responsabilidad.

11.6 La Gerencia de Informática, bajo responsabilidad, informará al término de cada mes, al Gerente Municipal, sobre la ejecución del Plan de Contingencias, formulando las recomendaciones a que hubiere lugar.