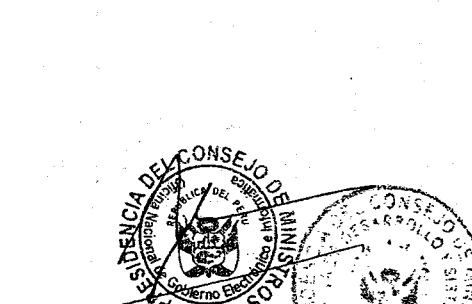
Directiva 006-2004-PCM/SG
Plan de Contingencias de los Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros 2004



HOJA DE INFORMACION GENERAL

CONTROL DOCUMENTAL:

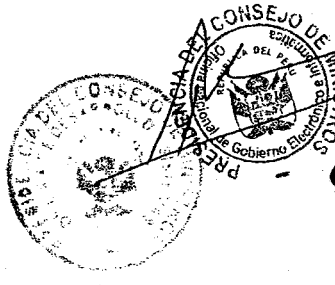
PROCEDIMIENTO:	Plan de Contingencias de los Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros 2004.
PROYECTO:	Plan de Contingencias de los Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros 2004.
ENTIDAD:	Oficina de Desarrollo y Sistemas de la Presidencia del Consejo de Ministros
VERSIÓN:	1.0
FECHA EDICIÓN:	02/06/2004
DOCUMENTOS RELACIONADOS:	
NOMBRE DE ARCHIVO:	P01-PCM-PLAN_CONTIN-001
	Directiva 006-2004-PCM/SG
RESUMEN:	Documento para la implementación de un Plan de Contingencias de los Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros 2004.

ESTADO FORMAL:

Preparado por:	Revisado por:	Aprobado por:
Nombre: Oficina de Desarrollo y Sistemas con el apoyo ONGEI Cargo: PCM Entidad: PCM Fecha: Junio 2004	Nombre: Rafael Parra Erkel Cargo: Jefe (e) Oficina de Desarrollo y Sistemas Jefe de la Oficina Nacional de Gobierno Electrónico e Informática Entidad: PCM Fecha: Junio 2004	Nombre: Jaime Reyes Miranda Cargo: Secretario General Entidad: PCM Fecha: Junio 2004

CONTROL DE VERSIONES

FUENTE DE CAMBIO	FECHA DE SOLICITUD DEL CAMBIO	VERSIÓN	PARTES QUE CAMBIAN	DESCRIPCIÓN DEL CAMBIO	FECHA DE CAMBIO
P01-PCM-PLAN_CONTIN-001.doc		1.00	N/A		



INDICE

INTRODUCCIÓN 2

1. OBJETIVOS 2

2. FINALIDAD 2

3. BASE LEGAL 3

4. ALCANCE 3

5. DE LA OFICINA DE DESARROLLO Y SISTEMAS 3

6. VIGENCIA 3

7. DETERMINACIÓN DE RIESGOS 3

7.1. Factores Naturales y/o Artificiales 3

7.2. Factores de Servicios 4

7.3. Factores de Sistemas 4

7.4. Factores de Recursos Humanos 4

7.5. Factores Diversos 4

8. MEDIDAS DE CONTINGENCIAS 5

8.1. Factores Naturales y/o Artificiales 5

8.2. Factores de Servicios 6

8.3. Factores de Sistemas 7

8.4. Factores de Recursos Humanos 10

"Directiva 006-2004-PCM/SG
Plan de
Contingencias de los
Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros"

INTRODUCCIÓN

Los sistemas informáticos existentes y los que se implementarán en la Oficina de Desarrollo y Sistemas de la Presidencia del Consejo de Ministros, significan para la Institución un importante avance en materia de modernización de los servicios ofrecidos al público usuario y a las dependencias internas de la Institución.

Es importante prever las medidas de seguridad que garanticen la continuidad del funcionamiento de estos sistemas.

En el "Plan de Contingencias" se identifican los riesgos a los que están expuestos los sistemas y se precisan las medidas de contención para minimizarlos, así como los requerimientos inmediatos para atenderlos cuando se produzcan.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también existe la posibilidad que el daño sea total, por lo que se debe prever un "Plan de Contingencias" completo.

1. OBJETIVOS

- Definir y programar la implementación de las medidas de seguridad que garanticen el funcionamiento continuo de los sistemas informáticos de la Presidencia del Consejo de Ministros.

- Restaurar el sistema en forma eficiente y con el menor costo y pérdidas posibles, en caso se produzca un incidente. Para estos imprevistos se incluyen las "Medidas de Contención".

2. FINALIDAD

a. Disponer de un plan que permita atender de manera ordenada y prevista situaciones que pongan en riesgo la operatividad de los Sistemas Informáticos y de Redes en la Presidencia del Consejo de Ministros,

Estableciendo procedimientos que eviten interrupciones en su operación.

3. BASE LEGAL

a. Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros (dado por D.S. N° 067-2003-PCM).
b. Manual de Organización y Funciones de la Presidencia del Consejo de Ministros.

4. ALCANCE

Esta Directiva será administrada por la Oficina de Desarrollo y Sistemas.

5. DE LA OFICINA DE DESARROLLO Y SISTEMAS

Se entiende a la Oficina de Desarrollo y Sistemas, como el órgano de la Presidencia del Consejo de Ministros que administra, opera y supervisa los sistemas informáticos y de redes de la institución, o al órgano que haga sus veces.

6. VIGENCIA

La presente Directiva entrará en vigencia a partir de la fecha de su aprobación por la Secretaría General de la Presidencia del Consejo de Ministros.

7. DETERMINACIÓN DE RIESGOS

Los sistemas mecanizados están expuestos a distintas clases de riesgos, que pueden afectar su normal funcionamiento, por lo que los problemas potenciales se han clasificado en grupos que se detallan a continuación:

7.1. Factores Naturales y/o Artificiales

Son originados por causas externas a la Institución y cuyo grado de previsión es muy reducido. Se consideran dentro de este grupo a los factores naturales como terremotos, maremotos, entre otros similares; artificiales como incendios, inundaciones, robos y problemas de terrorismo. Estos percances pueden generar pérdidas o daños físicos en el local de la PCM (equipos,

mobiliario, inclusive recursos humanos).
La probabilidad de los riesgos de origen natural es baja, mientras que los riesgos artificiales son de probabilidad mediana.

7.2. Factores de 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.

7.3. Factores de Sistemas

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

- Daños en componentes de hardware (discos duros, controladores de red, etc.). Fallas en dispositivos de comunicaciones (hubs, switches, routers).
- Desperfectos en las impresoras de las áreas usuarias.
- Falla en los terminales de ingresos de datos.
- Daños graves en los archivos del sistema por errores de hardware o software.
- Software corrupto o incompatible (copia sin licencia).
- Virus que dañen los archivos y hasta los equipos de cómputo.

7.4. Factores de Recursos Humanos

Están relacionados con la ausencia o presencia insuficiente de las personas que trabajan en el mantenimiento de las aplicaciones. Podrían causar demoras en atención de desperfectos; daños a archivos, equipos y otros dispositivos que requieren personal entrenado para su operación.
Estos riesgos pueden estar motivados por:

- Administradores no capacitados.
- Acceso de personas no autorizadas a sala de máquinas del centro de cómputo.

7.5. Factores Diversos

Se incluyen en esta clasificación otros riesgos que no se encuentren comprendidos en las clasificaciones anteriores. Por ejemplo:

- Derrame de líquidos en los equipos.

8. MEDIDAS DE CONTINGENCIAS

A continuación se detallan las medidas que deberán ser aplicadas para minimizar los riesgos de interrupción de los sistemas mecanizados. Adicionalmente, se explican los impactos de los riesgos, así como su probabilidad de ocurrencia, de acuerdo a las cinco categorías siguientes:

Muy Alta
Alta
Mediana
Baja
Muy baja

Se detallan los riesgos clasificados en las categorías antes especificadas:

8.1. Factores Naturales y/o Artificiales

Riesgo 1.1	Desastres naturales (terremotos, maremotos, etc.) y/o artificiales (incendio, inundación, terrorismo, robo, vandalismo etc.).
Probabilidad de Ocurrencia	Mediana
Efecto	• Posible deterioro/inutilización de los locales de la PCM • En casos muy graves, inutilización total de servidores de aplicación y equipos de comunicación. • Incapacidad temporal para utilizar sistemas mecanizados, servidores y equipos.
Medidas de Contención	• Entrenamiento del personal para asumir funciones alternas en caso de desastre. • Sistemas de detección y extinción de fuego (alarma de humo y extinguidores). • Mobiliario especial (racks) para los equipos críticos (servidores, equipos de comunicaciones). • Mantener contacto con proveedores y/o instituciones que provean equipos de características similares a los de la PCM, con capacidad de alquiler o préstamo en casos de quedar inutilizada totalmente la capacidad operativa de la PCM.

	• Retiro o reemplazo de todo tipo de objetos que en caso de incendio puedan ayudar a la expansión del fuego. • Revisión continúa del estado de la cablería de energía eléctrica. • Prohibición total de fumar en el área sensible. • Contar con vigilancia privada las 24 horas al día.

8.2. Factores de Servicios

Riesgo 2.1	Corte prolongado de la energía eléctrica.
Probabilidad de Ocurrencia	Mediana.
Efecto	• Paralización total de las actividades de la PCM. • Servicio restringido, se mantendría la operatividad con equipamiento mínimo. • Sólo podrán ingresar a los sistemas las estaciones de trabajo de provincias y locales periféricos.
Medidas de Contención	• Poner en funcionamiento una fuente de energía alternativa para la alimentación de equipos de la sala de operaciones. • Contar con un grupo electrógeno capaz de suministrar energía a todos los equipos involucrados. • Otorgar mantenimiento preventivo mensual de todo el equipo relacionado. • Distribuir la energía eléctrica que provee el grupo electrógeno por áreas, de acuerdo a lo crítico de su actividad.

Riesgo 2.2	Caídas de circuitos dedicados.
Probabilidad de Ocurrencia	Mediana
Efecto	• Si se da en el circuito principal de Lima, se produciría una paralización de los servicios a los locales remotos en Lima. • Si se da en el circuito del local remoto, se paraliza la producción local. • Corte en servicio de correo electrónico.

	• Imposibilidad de acceso a Internet
Medidas de Contención	• Realizar los procedimientos establecidos para verificar si el corte es producido por la empresa de telecomunicaciones o fallas en los equipos de comunicaciones. Coordinar con la empresa de telecomunicaciones la reposición del servicio o enmendar la falla del equipo de comunicaciones. • De acuerdo al tipo de equipo, contar como mínimo con un equipo de backup para su reemplazo, en caso de que sea necesario. • Contar con un UPS exclusivo para la sala de servidores.

8.3. Factores de Sistemas

Riesgo 3.1	Falla en componentes de la red de comunicación interna de datos.
Probabilidad de Ocurrencia	Mediana.
Efecto	• Fallas en switches principales paralizarían la red totalmente, hasta su reemplazo. • Fallas de hubs darían como resultado la paralización temporal en la operatividad de todas las estaciones de trabajo, terminales de ingreso de datos e impresoras a las cuales éstos sirve. • Fallas en las controladoras de redes del terminal, impresoras y estaciones de trabajo paralizarían el trabajo de la estación de la controladora de red afectada, hasta su reemplazo (hardware). • Deterioros de líneas de data podrían producir cortes prolongados de servicio al terminal, estación de trabajo, impresora de red o a todo un segmento, hasta su reemplazo.
Medidas de Contención	• Contar con mantenimiento preventivo para equipos de comunicaciones. Se deberá estar en capacidad de reemplazar temporalmente un dispositivo afectado hasta su reparación. • Mantener un stock mínimo de controladores de red y dispositivos de comunicaciones que garanticen el reemplazo inmediato de los equipos afectados. • Mantenimiento periódico del circuito de toma a

	tierra, puesto que los equipos de comunicaciones son sensibles a las variaciones de este circuito, lo cual puede afectar el rendimiento y performance. • Contar con un UPS exclusivo para estos equipos en la Sala de Operaciones.

Riesgo 3.2	Desperfectos en estaciones de trabajo, terminales de ingreso de datos y/o impresoras de las áreas usuarias
Probabilidad de Ocurrencia	Mediana
Efecto	• Imposibilidad de emisión de resultados en forma oportuna.
Medidas de Contención	• Se deberá contar con mantenimiento preventivo y correctivo para los equipos de cómputo (por la misma institución u outsourcing). Se deberá estar en capacidad de reemplazar temporalmente el equipo averiado hasta su reparación. • Las áreas usuarias deberán respetar estrictamente el calendario de mantenimiento preventivo, lo cual servirá para evaluar el estado de los dispositivos. • Durante el mantenimiento, se recomienda la permanencia del personal de la Oficina a cargo, para el asesoramiento respectivo. • Todo equipo o dispositivo ubicado en los ambientes del Despacho Ministerial deberán considerarse como repuestos críticos.

Riesgo 3.3	Fallas en la Granja de Servidores
Probabilidad de Ocurrencia	Muy baja.
Efecto	Paralización de atención a usuarios internos y externos, que utilicen las aplicaciones de la granja de servidores afectados.
Medidas de Contención	• Contar con mantenimiento de hardware y software tanto preventivo como correctivo (preferentemente outsourcing). • El proveedor del servicio de mantenimiento deberá estar en la capacidad de tener un tiempo

	de respuesta máximo de 45 minutos, producida la llamada de reporte de falla. • El proveedor deberá tener un tiempo máximo de reparación de 5 horas, en caso de excederse deberá reemplazar el equipo afectado por otro, con las condiciones mínimas para mantener la operatividad. • Los servidores contarán con UPS con una autonomía de 2 horas, lo que protegerá de fallas producidas por anormalidades en la provisión de energía eléctrica. • Contar con una política de backup para recuperar la información, de ser el caso.

Riesgo 3.4	Daños en los archivos de los sistemas mecanizados producido por fallas de Hardware.
Probabilidad de Ocurrencia	Mediana
Efecto	• La pérdida total o parcial de información ocasionaría problemas en la atención en línea y en la emisión de resultados • Paralización temporal a la atención de usuarios internos y externos de la PCM
Medidas de Contención	• Implementar una política de respaldo de información, teniendo en consideración el volumen de ésta, frecuencia de actualización, frecuencia de consulta, usuarios. • Realizar mantenimiento periódico a los dispositivos para las copias de seguridad, reemplazando las unidades defectuosas. • Almacenar los cartuchos de backup en un lugar que reúna las condiciones mínimas para su conservación. • Contar con almacenamiento externo para copias de seguridad.

Riesgo 3.5	Daños en los archivos por virus informáticos
Probabilidad de Ocurrencia	Alta
Efecto	• Paralización de la Granja de Servidores y estaciones de trabajo al atacar el virus al Sistema

	Operativo. • Destrucción y alteración de Archivos causando paralización temporal de actividades.
Medidas de Contención	• Restringir el libre uso de diskettes, uno de los principales medios de contaminación. • Contar con Software Antivirus instalando en cada servidor de aplicación y estación de trabajo. • Contar con una política de actualización continua de Antivirus. • Tener como norma la revisión con Software Antivirus de todos los archivos provenientes desde el exterior de la PCM, vía diskette, correo electrónico, Internet, etc.

8.4. Factores de Recursos Humanos

Riesgo 4.1	Ausencia de personal
Probabilidad de Ocurrencia	Mediana
Efecto	• En el caso que el personal encargado del adecuado funcionamiento del sistema no pudiera presentarse a laborar, se podría ver afectada la operatividad del mismo y no se daría una adecuada atención a los usuarios. • El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos y otros dispositivos que requieren entrenamiento para su operación.
Medidas de Contención	• Implementación de manuales de operaciones y procedimientos en los que se señalen claramente todas las labores diarias que se llevan a cabo por cada proceso operativo del sistema. • Aplicación de políticas de rotación para que cada persona esté familiarizada con las distintas labores que se llevan a cabo en cada área. • Contar con el número adecuado de personal encargado del funcionamiento del sistema (de tal manera que si una persona no se presenta, las labores no se verían afectadas en alto grado). • El personal a contratarse, así como el personal

	practicante, deberá en lo posible tener disponibilidad para presentarse al centro de trabajo fuera del horario establecido como laborable, en caso sea necesario.

Riesgo 4.2	Acceso de personas no autorizadas a los sistemas implementados.
Probabilidad de Ocurrencia	Mediana
Efecto	La manipulación del sistema por personas no autorizadas puede generar graves problemas, desde causar desperfectos en el funcionamiento hasta incluir modificaciones al mismo.
Medidas de Contención	• Cuando un empleado renuncie o salga de vacaciones, su clave de acceso deberá ser desactivada del sistema para evitar que en su ausencia otra persona pueda acceder al mismo y manipular los dispositivos. • Toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el Jefe de Desarrollo y Sistemas de la PCM. • El uso de passwords personales para la operación de los sistemas será responsabilidad y de uso exclusivo del dueño del password, puesto que cada acceso será grabado en una bitácora. • Política mensual de expiración de password a usuario. • Se recomienda que todo password tenga una longitud mínima de seis caracteres alfanuméricos. • El acceso a la sala de servidores de la PCM debe estar restringido sólo al personal autorizado por la Jefatura de Desarrollo y Sistemas.

PRESIDENCIA DEL CONSEJO DE MINISTROS
RAFAEL PARRA ERKEL
JEFE (e)
OFICINA DE DESARROLLO Y SISTEMAS

PRESIDENCIA DEL CONSEJO DE MINISTROS
RAFAEL PARRA ERKEL
JEFE
Oficina Nacional de Gobierno Electrónico e Informática