Resolución de Secretaría General

VISTO: 22 JUN. 2016

N° 018-2016-PCM/SG

El Memorando N° 0615-2016-PCM/OS de la Oficina de Sistemas; el Memorando N° 853-2016-PCM/OGA de la Oficina General de Administración; el informe N°046-2016-PCM/OGPP/GABS de la Oficina General de Planeamiento y Presupuesto; y el Informe N°011-2016-PCM/OGAJ-AMSS de la Oficina General de Asesoría Jurídica, y demás antecedentes; y,

CONSIDERANDO:

Que, de conformidad con lo establecido por el artículo 28° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo N° 063-2007-PCM, y modificatorias, la Oficina de Sistemas es la unidad orgánica, que depende jerárquicamente de la Oficina General de Administración, encargada de realizar las actividades relacionadas con el desarrollo, implementación, operación, mantenimiento y seguimiento de los sistemas informáticos y de brindar soporte técnico a los usuarios;

Que, mediante Resolución del Secretario General N° 005-2004, de fecha 23 de junio de 2004, se aprobó la "Directiva N° 006-2004-PCM/SG "Plan de contingencias de los sistemas informáticos y de redes de la Presidencia del Consejo de Ministros";

Que, mediante Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB, se aprueba la Norma Técnica Peruana NTP –ISO/IEC 27001:2014, 2da. Edición, que establece para todas las entidades integrantes del Sistema Nacional de Informática, la política de seguridad de la información con el objeto de dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos de la institución y la normatividad vigente;

Que, mediante Resolución Ministerial N° 053-2015-PCM/SG, se aprobó la Directiva N° 001-2015-PCM "Normas para la formulación, modificación y aprobación de directivas en la Presidencia del Consejo de Ministros", que tiene como objetivo normar y establecer los lineamientos para la formulación, modificación y aprobación de directivas que se expidan en la Presidencia del Consejo de Ministros;

Que, de acuerdo al numeral 5.3 de la Directiva N° 001-2015-PCM/SG, los titulares de los órganos, comisiones, programas y proyectos especiales de la Presidencia del Consejo de Ministros, son responsables de evaluar las directivas bajo su ámbito, cuya

vigencia sea mayor a los dos años, con el fin de proceder a su actualización y /o iniciar los trámites de aprobación de nuevas directivas que la reemplacen, de ser el caso;

Que, conforme a lo dispuesto en el numeral 7.3.2 de la Directiva N° 001-2015-PCM/SG, las directivas quedan sin efecto por declaración expresa, cuando las disposiciones de la que emanan pierden vigencia o cuando su materia es integrante o regulada por otra directiva;

Que, el numeral 21.4 del artículo 21 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, establece como una de las funciones de la Oficina General de Planeamiento y Presupuesto, el elaborar, actualizar y difundir los documentos normativos y de gestión del sistema de racionalización, en concordancia con la normatividad vigente;

Que, en dicho sentido, atendiendo a las sustanciales modificaciones que contiene la propuesta de Directiva "Contingencias Informáticas de la Presidencia del Consejo de Ministros"; corresponde aprobar una nueva Directiva y dejar sin efecto la "Directiva N° 006-2004-PCM/SG "Plan de contingencias de los sistemas informáticos y de redes de la Presidencia del Consejo de Ministros", que fue aprobada mediante Resolución del Secretario General N° 005-2004, de fecha 23 de junio de 2004;

Que, el proyecto de Directiva "Contingencias Informáticas de la Presidencia del Consejo de Ministros", tiene por objeto establecer los procedimientos y acciones de contingencia, necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos en la Presidencia del Consejo de Ministros, ante situaciones que pongan en riesgo su operatividad;

Que, asimismo, el proyecto de Directiva "Contingencias Informáticas de la Presidencia del Consejo de Ministros" se encuentra acorde a los lineamientos establecidos en la Directiva N° 001-2015-PCM, "Normas para la formulación, modificación y aprobación de directivas en la Presidencia del Consejo de Ministros", aprobada por Resolución Ministerial N°053-2015-PCM;

Que, de acuerdo al numeral 7.3.2.de la Directiva General N° 001-2015-PCM/SG, mediante los informes N° 046-2016-PCM/OGPP/GABS y N°011-2016-PCM/OGAJ-AMSS; las Oficinas Generales de Planeamiento y Presupuesto y de Asesoría Jurídica; respectivamente, han emitido opinión favorable al proyecto de Directiva;

Que, mediante el numeral 1.1 del artículo 1° de la Resolución Ministerial N° 298-2015-PCM, se delega al Secretario General de la Presidencia del Consejo de Ministros la facultad de aprobar directivas y /o manuales, así como todo documento normativo que regule los actos de administración interna, elaboración de documentos de gestión, trámites internos, lineamientos técnicos-normativos y metodológicos, orientados a optimizar los procedimientos administrativos de carácter interno a cargo de los órganos de apoyo de la Presidencia del Consejo de Ministros;

Que, de conformidad con lo señalado en el numeral 11.7 del artículo 11 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, y sus modificatorias; y, a la

Resolución de Secretaría General

delegación efectuada en el numeral 1.1 del artículo 1 de la Resolución Ministerial N° 298-2015-PCM;

Con los vistos de la Oficina General de Administración, de la Oficina General de Planeamiento y Presupuesto, Oficina de Sistemas; y de la Oficina General de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 003 -2016-PCM/SG, "Contingencias Informáticas de la Presidencia del Consejo de Ministros", cuyo texto forma parte integrante de la presente Resolución de Secretaria General.

Artículo 2.- Dejar sin efecto la Directiva N° 006-2004-PCM/SG "Plan de contingencias de los sistemas informáticos y de redes de la Presidencia del Consejo de Ministros", aprobada por Resolución del Secretario General N° 005-2004.

Artículo 3.- Disponer la publicación de la presente Resolución de Secretaría General y de la Directiva aprobada en el artículo 1, en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe).

Regístrese y comuníquese.

ABOG. MANUEL MESONES CASTELO
Secretario General
Presidencia del Consejo de Ministros

Directiva 003-2016-PCM/SG

Contingencias Informáticas de la Presidencia del Consejo de Ministros

2016

HOJA DE INFORMACIÓN GENERAL

CONTROL DOCUMENTAL:

PROYECTO:	Directiva "Contingencias Informáticas de la Presidencia del Consejo de Ministros"
ENTIDAD:	Presidencia del Consejo de Ministros
VERSIÓN:	2.0
FECHA EDICIÓN:	Junio 2016
DOCUMENTOS RELACIONADOS:	Directiva N° 006-2004-PCM/SG "Plan de Contingencias de los Sistemas Informáticos y de Redes de la Presidencia del Consejo de Ministros 2004"

DERECHOS DE USO:

La presente documentación es de uso interno de la Presidencia del Consejo de Ministros. Contiene información confidencial en los anexos

ESTADO FORMAL:

Preparado por:	Revisado por:	Aprobado por:
Nombre: Julia Milagros Olea Sal y Rosas	Nombre: María Angélica Castillo Ríos	Nombre: Manuel Gustavo Mesones Castelo
Oficina : Oficina de Sistemas	Oficina : Oficina de Sistemas	Cargo: Secretario General
Cargo : Oficial de Seguridad de la Información	Cargo : Jefe de la Oficina de Sistemas	Entidad: PCM
Entidad: PCM	Entidad: PCM	Fecha: Jun 2016
Fecha: Set 2015	Fecha: Set 2015	

Control de Versiones

Versión	Fecha de aprobación	Elaboración	Revisión	Aprobación	Breve descripción
1.0	2004	Oficina de Desarrollo y Sistemas con apoyo de ONGEI	Nombre: Rafael Parra Erkel Cargo: Jefe (e) Oficina de Desarrollo y Sistemas Jefe de la Oficina Nacional de Gobierno Electrónico e Informática Entidad: PCM	Resolución de Secretaría General N° 005-2004-PCM Directiva N° 006-2004-PCM/SG	Documento para la implementación de un plan de contingencias de los sistemas informáticos y de redes de la PCM

NOTAS

- La presente versión sustituye completamente a todas las precedentes de manera que éste sea el único documento válido.
- El propietario de los documentos de Seguridad de la Información es el personal que haga las veces de Oficial de Seguridad de la Información.

CONTENIDO

"CONTINGENCIAS INFORMÁTICAS DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS"

Directiva -2016-PCM/SG

I. OBJETIVO

Establecer los procedimientos y acciones de contingencia, necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos en la Presidencia del Consejo de Ministros, ante situaciones que pongan en riesgo su operatividad.

II. FINALIDAD

Definir y programar las medidas de seguridad que garanticen el funcionamiento continuo de los sistemas y servicios informáticos de la Presidencia del Consejo de Ministros – PCM, restaurándolos de forma eficaz, eficiente y con el menor impacto negativo posible, en caso se produzca un incidente que pudiera alterar su operación.

III. BASE LEGAL

- Ley N° 29733, Ley de Protección de Datos Personales
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley N° 29733, Ley de Datos Personales
- Decreto Supremo Nº 063-2007-PCM, Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros y sus modificatorias
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática
- Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales no arancelarias N° 129-2014/CNB-INDECOPI, que aprueba como Norma Técnica Peruana la "NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos. 2ª Edición. Reemplaza a la NTP-ISO/IEC 27001:2008"
- Resolución Ministerial N° 053-2015-PCM, que prueba la Directiva N° 001-2015-PCM "Normas para la formulación, modificación y aprobación de directivas en la Presidencia del Consejo de Ministros"
- Resolución Ministerial N° 004-2015-PCM, que aprueba la Directiva N° 004-2015-PCM "Directiva para el Desarrollo de Sistemas Informáticos en la Presidencia del Consejo de Ministros".

- Resolución de Contraloría N° 320-2006-CG, "Aprueban Normas de Control Interno".

IV. ALCANCE

La presente Directiva alcanza a los sistemas y servicios informáticos que gestiona la Oficina de Sistemas de la Presidencia del Consejo de Ministros.

V. RESPONSABILIDAD

5.1 La Oficina de Sistemas es responsable de:

a) Cumplir los procedimientos de respuesta ante cada tipo de desastre
b) Actualizar la presente Directiva.

5.2 La Oficina General de Administración es responsable de

a) Conducir el Comité Gerencial ante la ocurrencia de contingencias, en coordinación con la Oficina de Sistemas
b) Atender los requerimientos de la Oficina de Sistemas para la planificación de los medios de prevención, así como durante la ejecución y recuperación ante desastres.

VI. DISPOSICIONES GENERALES

Del Grupo de Trabajo para la gestión del riesgo de desastres

La organización ante contingencias en los sistemas y servicios informáticos de la PCM se detalla a continuación:

6.1 **Comité Gerencial:**

6.1.1 El Comité Gerencial está integrado por:

- Director (a) de la Oficina General de Administración, quien lo preside
- Jefe (a) de la Oficina de Sistemas, quien será el (la) "Responsable de Coordinaciones"
- Otros que el Director de la Oficina General de Administración considere pertinente incluir.

6.1.2 Ante la materialización de un riesgo, este grupo organizado de personas ejecutará todas las acciones necesarias para superar dicho evento negativo.

6.1.3 Antes de que se produzca algún incidente, este comité planificará los medios de prevención, ejecución, recuperación y actualización de las acciones de contingencia de los sistemas y servicios informáticos.

6.2 **Comité Operativo:**

6.2.1 El Comité Operativo está integrado por:
- Coordinador de Redes y Comunicaciones, quien lo preside
- Coordinador de Soporte
- Coordinador de Desarrollo
- Coordinador de Trámite Documentario
- Oficial de Seguridad de la Información.

6.2.2 El Comité Operativo es el grupo de responsables organizados que, en el ámbito de sus funciones, ejecutarán operativamente todas las tareas que permitan recuperar o mantener la operatividad de los servicios y aplicaciones en la Presidencia del Consejo de Ministros.

De la determinación del escenario de riesgo

6.3 **Identificación de peligros**

Los sistemas y servicios informáticos están expuestos a distintas clases de riesgos que pueden afectar su normal funcionamiento, razón por la cual los problemas potenciales se han clasificado en grupos de acuerdo a los factores que determinan su origen, los que se detallan a continuación:

6.3.1 Factores naturales y artificiales

Son originados por causas externas a la institución y cuyo grado de previsión es muy reducido. Estos percances pueden generar pérdidas o daños físicos en el local de la PCM (equipos, mobiliario, inclusive a las personas). Se consideran dentro de este grupo los siguientes:

Riesgo 1.1	Desastres naturales (terremotos, maremotos, entre otros)
Probabilidad de ocurrencia	Baja
Grado de impacto	Alto
Efecto	• Posible deterioro o inutilización parcial de la infraestructura física de los locales de la PCM • En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones) • Incapacidad temporal para utilizar servicios de tecnologías de la información.

Riesgo 1.2	Desastres artificiales
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
Efecto	• Posible deterioro de los equipos informáticos de la PCM • En casos muy graves, la inutilización total de los equipos de uso crítico • Incapacidad temporal para utilizar los servicios de tecnologías de la información.

6.3.2 Factores de servicios

Los riesgos identificados en este grupo pueden generar la interrupción de los sistemas y servicios informáticos, afectando las actividades administrativas y de atención al público. Se considera dentro de este grupo el siguiente factor:

Riesgo 2.1	Interrupción prolongada del suministro de energía eléctrica
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
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.

6.3.3 Factores de sistemas

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

Riesgo 3.1	Fallas en los dispositivos de comunicaciones
Probabilidad de ocurrencia	Media
Grado de impacto	Alto
Efecto	• Paralización total de las comunicaciones de toda la red de la PCM o un segmento de esta.

Riesgo 3.2	Fallas en las computadoras de escritorio o en las computadoras portátiles
Probabilidad de ocurrencia	Media
Grado de impacto	Medio

Efecto	• Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.

Riesgo 3.3	Fallas en los servidores
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
Efecto	• Paralización en la atención de usuarios internos que utilicen las aplicaciones de los servidores afectados.

Riesgo 3.4	Daños o pérdida de la información en las bases de datos
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
Efecto	• La pérdida total o parcial de la información ocasionaría problemas en la atención en línea y en la emisión de resultados • Paralización temporal a la atención de los usuarios internos y externos de la PCM.

Riesgo 3.5	Acceso de personas no autorizadas a los sistemas informáticos de la PCM de manera remota o a través de vulnerabilidades
Probabilidad de ocurrencia	Media
Grado de impacto	Alto
Efecto	• Alteración o pérdida de información de los sistemas informáticos • Difusión de información confidencial en medios públicos • Ataque de denegación de servicio que, sin vulnerar la confidencialidad de la información interna, haga inaccesible la página web institucional, el correo electrónico o la navegación por internet por parte del personal.

Riesgo 3.6	Infección de virus informáticos en las computadoras
Probabilidad de ocurrencia	Alta
Grado de impacto	Alto

Efecto	• Lentitud en el funcionamiento de los equipos informáticos • Modificaciones en los archivos o pérdida de información • Mensajes de error • Disminución del espacio en la memoria y el disco duro.

6.3.4 Factores de recursos humanos

Están relacionados con la ausencia o presencia insuficiente del personal que trabaja en el mantenimiento de las aplicaciones informáticas. Podrían causar demoras en la atención de desperfectos, daños a los archivos, equipos y otros dispositivos que requieren personal entrenado y calificado para su operación.

Estos riesgos pueden estar motivados por el siguiente factor:

Riesgo 4.1	Ausencia de personal de la Oficina de Sistemas
Probabilidad de ocurrencia	Mediana
Grado de Impacto	Alto
Efecto	• Se podría ver afectada la operatividad de los servicios informáticos y la adecuada atención a los usuarios • El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.

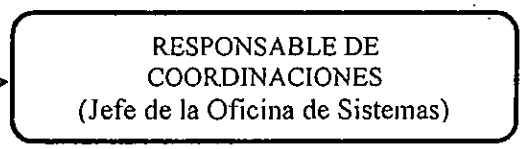
VII. DISPOSICIONES ESPECÍFICAS

7.1 Procedimiento de alerta

a) Se produce el incidente o se materializa una contingencia, llámese emergencia.
b) Cualquier servidor de la PCM, independientemente de la naturaleza de su contrato, identifica el suceso.
c) Es responsabilidad del servidor de la PCM que identificó la emergencia, reportar el evento al "Responsable de Coordinaciones" utilizando cualquier medio de los que encuentre disponibles (teléfono, correo electrónico o en persona).

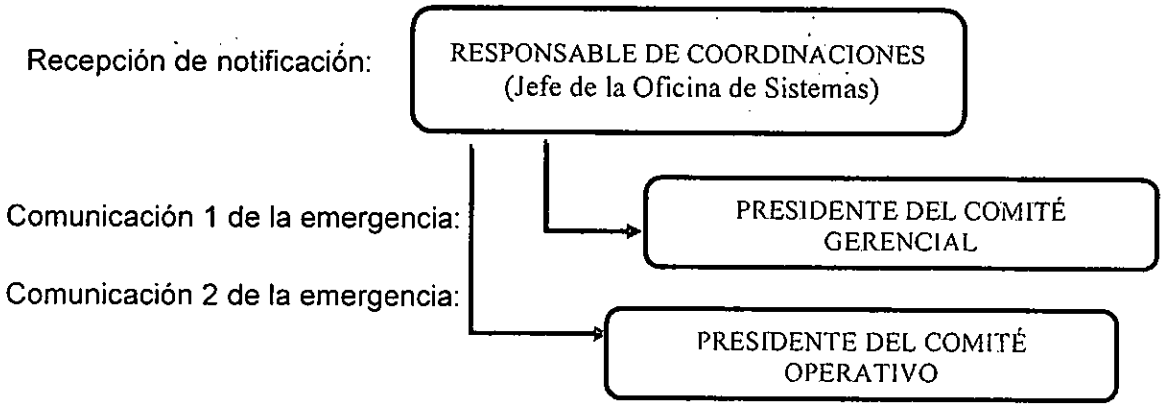
Identificación de la emergencia:

Notificación de la emergencia:



7.2 Procedimiento de coordinación

a) El "Responsable de Coordinaciones" recibe la información acerca de la emergencia.
b) El "Responsable de Coordinaciones" notificará inmediatamente lo sucedido al "Presidente del Comité Operativo" y al "Presidente del Comité Gerencial".
c) El "Responsable de Coordinaciones" coordinará con el "Presidente del Comité Gerencial" la necesidad para la activación de las acciones de contingencia.



7.3 Procedimiento de respuesta

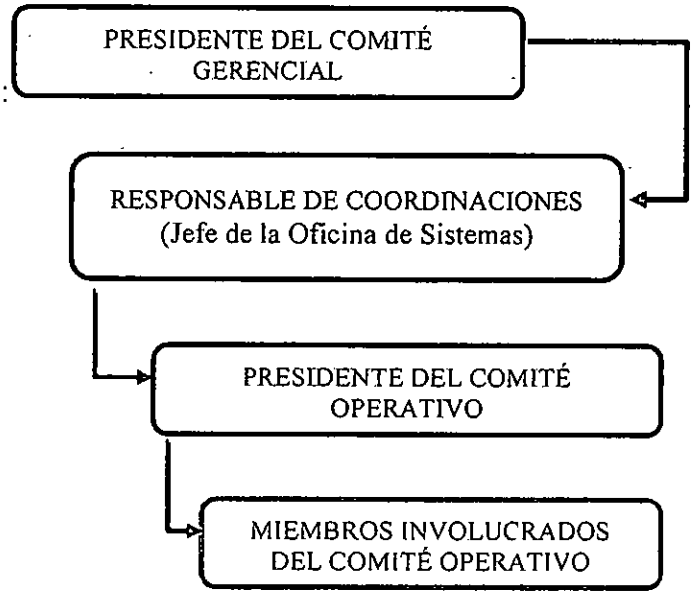
a) El "Presidente del Comité Gerencial" dará aprobación para la ejecución de las acciones de contingencia – A.C.
b) El "Responsable de Coordinaciones" ordenará inmediatamente al "Presidente del Comité Operativo" la activación de las acciones de contingencia
c) El "Presidente del Comité Operativo" identificará el tipo de emergencia a atender (ámbito funcional).
d) El "Presidente del Comité Operativo" coordinará con los miembros del comité involucrados en la ejecución de las acciones de contingencia, de acuerdo al tipo de emergencia.
e) Se ejecutan las acciones de contingencia para la continuidad de las operaciones. De ser necesario se coordinará con empresas, proveedores de servicios, autoridades locales y nacionales y otras instituciones.

Aprobación de ejecución de A.C.:

Ordena ejecución de A.C.:

Coordinación para ejecutar A.C.

Ejecución de A.C.:



7.4 Procedimiento para la continuidad de servicios

A continuación se detallan las medidas preventivas, de ejecución y recuperación, que deberán ser aplicadas para minimizar los riesgos de interrupción de los sistemas informáticos; de acuerdo con el grado de impacto de los riesgos, así como con su probabilidad de ocurrencia y posibles efectos, clasificados de acuerdo a las cinco categorías siguientes:

Probabilidad de ocurrencia
Muy alto
Alto
Medio
Bajo
Muy bajo

7.4.1 Factores naturales y artificiales

Riesgo 1	Desastres naturales (terremotos, maremotos, entre otros)
Probabilidad de ocurrencia	Baja
Grado de impacto	Alto
Efecto	• Posible deterioro o inutilización parcial de la infraestructura física de los locales de la PCM

	• En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones) • Incapacidad temporal para utilizar servicios de tecnologías de la información.
Acción de prevención	• Establecer zonas de seguridad en las cuales se proteja al personal, así como los equipos de uso crítico • Brindar entrenamiento constante al personal para que pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre • Contar con un grupo electrógeno, en cada sede de la PCM, que pueda activarse para apoyar a las fuentes de energía alternativa (UPS) en la misión de mantener la operatividad de los sistemas informáticos • Contar con mobiliario especial (racks) para los equipos informáticos • Fijar los equipos informáticos mediante mecanismos de anclaje a sus respectivas bases, con la finalidad de que ante un movimiento fuerte no sufran caídas • Realizar copias de seguridad de los aplicativos y bases de datos más importantes, de acuerdo a la política de respaldo establecida por la Oficina de Sistemas, para asegurar la continuidad de las operaciones.
Acción de ejecución	• Verificar el estado de la infraestructura del Data Center • Verificar las conexiones y el adecuado funcionamiento de los equipos de uso crítico. • De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos de uso crítico, falta de energía eléctrica, falla de servidores o de ocurrir un incendio posterior al desastre natural, se deberá tomar en consideración los pasos establecidos en este plan de contingencia como medida de contención para cada uno de los casos.
Acción de recuperación	• Luego de pasado el desastre natural, evaluar los daños ocasionados a la infraestructura tecnológica y física del centro de datos y a los equipos informáticos asignados al personal de PCM • Realizar un inventario general de los sistemas informáticos afectados, indicando el estado de operatividad de los mismos • Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración • Realizar tareas de recuperación de acuerdo a lo establecido por la Oficina de Sistemas.

Riesgo 1-2	Desastres artificiales
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto

Efecto	• Posible deterioro de los equipos informáticos de la PCM • En casos muy graves, la inutilización total de los equipos de uso crítico • Incapacidad temporal para utilizar los servicios de tecnologías de la información.
Acción de prevención	• Instalar y mantener operativos los sistemas de detección y extinción de fuego (alarmas de humo y extinguidores de gas) en el Centro de datos • Instalar Cámaras en el Centro de Datos, para vigilancia y monitoreo de los ingresos a la Sala de Servidores y así evitar sabotajes por ingresos no autorizados que ocasionen un desastre mayor. • Efectuar revisiones anuales del estado de conservación del cableado de energía eléctrica, • Contar con personal o servicio de vigilancia las 24 horas del día, con el fin de garantizar la seguridad en cada sede de la PCM de los equipos informáticos que procesan y almacenan toda la información de la institución • Realizar anualmente entrenamiento del personal de la Oficina de Sistemas para que pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre • Brindar mantenimiento y recarga a los extintores de incendios.
Acción de ejecución	• Si el fuego es controlable, intentar apagarlo haciendo uso de los extintores apropiados para cada tipo de incendio • Retirar todos los objetos inflamables que se encuentren cerca del fuego • De ser posible, desconectar y retirar los equipos informáticos a un ambiente libre de fuego • De no extinguirse el fuego, evacuar las instalaciones • De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos informáticos, falta de energía eléctrica o falla de servidores, tomar en consideración los pasos establecidos en este plan de contingencia, como medida de contención para cada uno de los casos.
Acción de recuperación.	• Luego de extinguido el incendio, evaluar los daños ocasionados a los sistemas y equipos informáticos • Realizar un inventario general de los sistemas y equipos informáticos afectados, indicando el estado de operatividad de los mismos • Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración • Efectuar tareas de recuperación, de acuerdo a lo establecido por la Oficina de Sistemas.

7.4.2 Factores de servicios

Riesgo 2.1	Interrupción prolongada del suministro de energía eléctrica
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
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
Acción de prevención	• Efectuar el mantenimiento preventivo de todo el equipamiento informático, de acuerdo al Plan de Mantenimiento establecido por la Oficina de Sistemas • Adquirir un grupo electrógeno por cada sede de PCM y capacitar al personal, designado por la Oficina General de Administración y la Oficina de Sistemas, en su funcionamiento • Realizar pruebas semestrales a los UPS y adquirir nuevos de ser necesario.
Acción de ejecución	• Poner en funcionamiento el (los) UPS para la alimentación de equipos de uso crítico • Comunicarse con el personal responsable del control de suministro de energía eléctrica, designado por la OGA en cada sede, para coordinar con la Oficina de Sistemas el restablecimiento del mismo • En caso de que la falta de energía eléctrica sea mayor a quince minutos, se deberán apagar los servidores hasta que el servicio sea restablecido.
Acción de recuperación	• Verificar si la falta de suministro de energía eléctrica se debe a algún desperfecto ocurrido dentro de la institución, en cuyo caso avisar al personal responsable, designado por la OGA, para que proceda con la reparación del desperfecto; de tratarse de una falla atribuible al proveedor de energía eléctrica, comunicarse con ellos para indicar el problema y solicitar la reposición inmediata del servicio • Esperar a que el suministro de energía eléctrica se restablezca y luego efectuar el encendido de los equipos informáticos del Centro de Datos y del personal.

7.4.3 Factores de sistemas

Riesgo 3.1	Fallas en dispositivos de comunicaciones
Probabilidad de ocurrencia	Media
Grado de impacto	Alto
Efecto	• Paralización total de las comunicaciones de toda la red de la PCM o un segmento de esta.
Acción de prevención	• Realizar el mantenimiento preventivo de los equipos de comunicaciones, de acuerdo a lo establecido por la Oficina de Sistemas • Mantener un stock de reposición de controladores de red y dispositivos de comunicaciones que garanticen su reemplazo inmediato en el caso que sufran fallas • Capacitación al personal responsable de los equipos de comunicaciones, de la Oficina de Sistemas, sobre la configuración de los equipos informáticos.
Acción de ejecución	• Verificar las conexiones de los hubs, switches y routers, entre otros equipos de comunicaciones • Reiniciar el equipo de comunicaciones que esté fallando • Verificar la configuración del equipo de comunicaciones que esté fallando • Si no se obtiene un funcionamiento óptimo, cambiar el equipo de comunicaciones por el equipo de comunicaciones de respaldo y proceder a efectuar la configuración necesaria.
Acción de recuperación.	• Verificar las posibles fallas en el equipo de comunicaciones; en el caso de detectarse alguna, coordinar con el proveedor su reparación o adquirir otro equipo de comunicaciones para su reemplazo • Poner operativo el equipo de comunicaciones de respaldo • Estabilizar la red de datos de la sede central (Palacio de Gobierno) y restablecer los enlaces con las demás sedes.

Riesgo 3.2	Fallas en las computadoras de escritorio o las computadoras portátiles
Probabilidad de ocurrencia	Media
Grado de impacto	Medio
Efecto	• Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.

Acción de prevención	• Realizar el mantenimiento preventivo de las computadoras de escritorio y computadoras portátiles de la PCM de acuerdo al Plan de Mantenimiento establecido por la Oficina de Sistemas • Tener un antivirus instalado y actualizado en todas las computadoras de escritorio y computadoras portátiles de la PCM • Concientizar a los usuarios sobre las buenas prácticas en el uso de las computadoras de escritorio y computadoras portátiles para minimizar la ocurrencia de posibles fallas en estos equipos, en las capacitaciones realizadas por la Oficina de Sistemas.
Acción de ejecución	• Verificar el origen de la falla y estimar el tiempo que tomará la reparación; si es menor a una hora, efectuar la reparación en el lugar del usuario, de lo contrario se procede a retirar el equipo para su reparación en el área de Soporte Técnico de la Oficina de Sistemas, entregándosele temporalmente al usuario una computadora portátil como equipo de reemplazo hasta que dicho equipo sea reparado y devuelto.
Acción de recuperación.	• Analizar las causas de la falla de la computadora de escritorio o computadora portátil para ser reparada y restaurada a su estado operativo, y luego devuelta al usuario asignado. Si no se consigue reparar el equipo, asignar otro con las mismas características al usuario afectado • Restaurar la información del usuario del correo institucional y aquella respaldada por el usuario.

Riesgo 3.3	Fallas en los servidores
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
Efecto	• Paralización en la atención de usuarios internos que utilicen las aplicaciones de los servidores afectados.
Acción de prevención	• Realizar el mantenimiento de hardware y software tanto preventivo como correctivo de acuerdo al Plan de Mantenimiento establecido por la Oficina de Sistemas • Los servidores deben contar con un UPS que asegure su operatividad por un tiempo prolongado ante la falta de suministro de energía eléctrica, de mínimo 1 hora • Tener un inventario, actualizado anualmente, de todos los programas y archivos de los servidores • Contar con copias de seguridad actualizadas de los servidores.
Acción de ejecución	• Diagnosticar los inconvenientes presentados en los equipos servidores o virtualizados

	• Realizar la captura de datos para determinar las fallas presentadas en los servidores físicos o virtualizados.
Acción de recuperación.	• Realizar la restauración desde las copias de seguridad • Realizar la restauración o "*snapshot*" de los equipos virtualizados • Realizar las pruebas de restauración de datos en los servidores físicos y virtualizados.

Riesgo 3.4	Daños o pérdida de la información en las bases de datos
Probabilidad de ocurrencia	Media
Grado de impacto	Muy alto
Efecto	• La pérdida total o parcial de la información ocasionaría problemas en la atención en línea y en la emisión de resultados • Paralización temporal a la atención de los usuarios internos y externos de la PCM.
Acción de prevención	• Restringir los accesos no autorizados a las bases de datos • Tener registros de actividad (logs) que registren los cambios realizados a las bases de datos con la finalidad de que sean auditables • Tener un inventario de las bases de datos y su ubicación en los servidores anualmente • Actualizar la política de respaldo y restauración de información de las bases de datos.
Acción de ejecución	• Verificar la integridad de los datos realizando una auditoría de la información registrada en los logs.
Acción de recuperación.	• Efectuar la restauración de las copias de seguridad de las bases de datos • Realizar las pruebas de integridad de la información restaurada y los permisos correspondientes • Restaurar los accesos y permisos de acceso de los usuarios.

Riesgo 3.5	Acceso de personas no autorizadas a los sistemas informáticos de la PCM de manera remota o a través de vulnerabilidades
Probabilidad de ocurrencia	Media
Grado de impacto	Alto
Efecto	• Alteración o pérdida de información en los sistemas informáticos • Difusión de información confidencial en medios públicos • Ataque de denegación de servicio que, sin vulnerar la

	confidencialidad de la información interna, hagan inaccesible la página web institucional, el correo electrónico o la navegación por internet por parte del personal.
	• Efectuar charlas de capacitación y concientización sobre seguridad de la información para los usuarios, de acuerdo al Plan de Capacitaciones de la Oficina de Sistemas • Desactivar de los sistemas informáticos los accesos de los servidores públicos que renuncien o hagan uso de su periodo vacacional, para evitar que en su ausencia, otra persona acceda con sus credenciales y pueda manipular la información de los sistemas informáticos
Acción de prevención	• Toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el Jefe (a) de Sistemas de la PCM con el debido sustento del Coordinador del área de Desarrollo y ser enviado al OCI para su conocimiento. • El acceso a la sala de servidores de la PCM debe estar restringido sólo al personal autorizado por la Jefatura de la Oficina de Sistemas • Contar con una matriz de control de acceso de los usuarios a los diferentes recursos de la red (archivos, bases de datos, impresoras, entre otros) especificando las autorizaciones respectivas sobre cada objeto • Limitar el número de intentos para el ingreso correcto de las credenciales de acceso a los sistemas, recursos y servicios informáticos, de acuerdo a la política establecida por la Oficina de Sistemas • Forzar a los usuarios a cambiar periódicamente su palabra clave, de acuerdo a la política establecida por la Oficina de Sistemas.
Acción de ejecución	• Bloquear el acceso de todos los usuarios al sistema informático inmediatamente sea detectada la intrusión. • Cambiar la clave de acceso de los sistemas informáticos afectados • Realizar una copia de seguridad de los sistemas informáticos afectados para realizar un análisis posterior • Aislar el sistema informático hasta que las vulnerabilidades sean encontradas y subsanadas.
Acción de recuperación.	• Realizar un análisis exhaustivo para detectar las vulnerabilidades que pudieron ser utilizadas para la intrusión • Analizar los daños que pudo haber ocasionado la intrusión • De ser necesario, restaurar una copia de seguridad de los sistemas informáticos y subsanar las vulnerabilidades encontradas.

Riesgo 3.6	Infección de virus informáticos en las computadoras
Probabilidad de ocurrencia	Alta
Grado de impacto	Alto
Efecto	• Lentitud en el funcionamiento de los equipos informáticos • Modificaciones de archivos o pérdida de la información • Mensajes de error • Disminución del espacio en la memoria y el disco duro.
Acción de prevención	• Brindar charlas de capacitación y concientización para los usuarios sobre el uso adecuado del internet y los dispositivos informáticos, de acuerdo al Plan de Capacitaciones de la Oficina de Sistemas • Contar con software antivirus instalado, actualizado y activo en todas las computadoras de la entidad • Realizar actividades de mantenimiento preventivo a las computadoras, de acuerdo al Plan de Mantenimiento establecido por la Oficina de Sistemas • Bloquear la opción de instalación de programas informáticos para los usuarios cuyas funciones sean ajenas a las de la Oficina de Sistemas.
Acción de ejecución	• Realizar un análisis de infección de virus informáticos en las computadoras con un antivirus actualizado y un antimalware • De detectarse la persistencia del virus, ejecutar procedimientos de limpieza antivirus y de ser necesario realizar las acciones del plan de ejecución para las "Fallas en las computadoras de escritorio o en las computadoras portátiles".
Acción de Recuperación.	• Analizar los daños que pudo haber ocasionado la infección, de ser necesario aplicar el plan de contingencia para "Daños o pérdida de la información en las bases de datos" • Realizar las acciones del plan de recuperación para las "Fallas en las computadoras de escritorio o en las computadoras portátiles".

7.4.4 Factores de recursos humanos

Riesgo 4.1:	Ausencia de personal de la Oficina de Sistemas
Probabilidad de ocurrencia	Mediana
Grado de impacto	Alto
Efecto	• Se podría ver afectada la operatividad de los servicios informáticos y la adecuada atención a los usuarios • El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.
Acción de prevención	• Implementar manuales de operaciones y procedimientos en los que se señale las labores que se llevan a cabo por cada proceso crítico de los sistemas informáticos • Tener un política de rotación del personal dentro de las áreas de la Oficina de Sistemas para que todos conozcan todas las labores de su área • Tener una lista de los sistemas informáticos críticos, con el nombre y número de teléfono del encargado de cada sistema y el de su reemplazo en caso de emergencia. Esta lista será actualizada cada vez que cambie el personal de la Oficina de Sistemas o rote de funciones • Almacenar las credenciales de acceso (usuarios y claves) con permiso de administrador, de los equipos del Centro de Datos en sobres lacrados, los cuales deberán estar bajo la custodia del Jefe(a) de la Oficina de Sistemas.
Acción de ejecución	• El personal de reemplazo asume las funciones del personal titular en caso de emergencia • Brindar al personal de reemplazo todos los accesos necesarios para que cumpla con las labores encargadas • Brindar al personal de reemplazo los usuarios y claves con permiso de administrador, de ser necesario.

Acción de recuperación.	• Retirar los accesos brindados al personal de reemplazo una vez recuperados los servicios • Realizar el cambio de las claves y generar nuevos sobres lacrados de credenciales de acceso a los equipos del Centro de Datos, en el caso que los anteriores sobres hayan sido abiertos.

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 Déjese sin efecto la Directiva N° 006-2004-PCM/SG "Plan de Contingencias de los sistemas informáticos y de redes de la Presidencia del Consejo de Ministros", aprobada por Resolución de Secretaría General N° 005-2004-PCM.

IX. ANEXOS

NOTA:
La información contenida en los anexos es CONFIDENCIAL, de uso exclusivo de la Oficina de Sistemas de la PCM para dar respuesta inmediata ante cualquier incidente de Seguridad de la Información que pueda suscitarse, por lo tanto no puede ser publicada, distribuida ni accedida por personas no autorizadas y ajenas a las designadas por la Oficina de Sistemas de la PCM, por ser información vital que compromete a toda la institución.

Lo señalado, está alineado a la NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos. 2ª Edición; que a la letra señala:

"...7.53. Información documentada
La información documentada requerida por el Sistema de Gestión de Seguridad de la información y por esta NTP se debe controlar para asegurar:
...
b) que esté protegida adecuadamente (por ejemplo de confidencialidad, uso impropio, o pérdida de integridad)
..."

Controles:

"A.8.2.1 Clasificación de la Información: La información debe ser clasificada en términos de los requisitos legales, valor criticidad y sensibilidad respecto a una divulgación o modificación no autorizada"

"A.8.3.3 Transferencia de medios físicos: Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte."