Resolución de Secretaría General

Nº 04 -2016-CENEPRED/SG

Lima, 17 JUN 2016

VISTOS:

El Informe N° 027-2016-CENEPRED/OA/I de fecha 14 de junio de 2016, el Memorándum N° 495-2016-CENEPRED/OPP de fecha 14 de junio de 2016 y el Memorándum N° 673-2016-CENEPRED/OA de fecha 14 de junio de 2016; y,

CONSIDERANDO:

Que, el artículo 12° de la Ley N° 29664 Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres, establece que el Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (CENEPRED) es un organismo público ejecutor con calidad de pliego presupuestal adscrito a la Presidencia del Consejo de Ministros;

Que, mediante Decreto Supremo N° 104-2012-PCM de fecha 18 de octubre de 2012, se aprobó el Reglamento de Organización y Funciones del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (CENEPRED), el mismo que entró en vigencia al día siguiente de su publicación; estableciendo en su artículo 6° la Estructura Orgánica del CENEPRED;

Que, la Ley N° 28716 "Ley de Control interno de la Entidades del Estado, tiene por finalidad que las entidades del Estado incorporen obligatoriamente sistemas de control interno en sus procesos, actividades, recursos, operaciones y actos institucionales;

Que, las diversas unidades orgánicas del CENEPRED, en su constante compromiso de mejoramiento, vienen revisando su normativa a efectos de solicitar la aprobación de nuevos documentos de gestión, con la finalidad de mejorar y optimizar las labores de cada una de ellas;

Que, el artículo 20° del Reglamento de Organización y Funciones del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (CENEPRED) señala que la Oficina de Administración es el órgano de apoyo encargado de realizar la gestión de recursos humanos, económicos-financieros, logísticos, servicios generales, así como la ejecución presupuestal y la gestión patrimonial de la institución. Teniendo además a su cargo la provisión

de servicios de soporte de tecnologías de información y comunicaciones, administración documentaria y archivo central de la institución;

Que, en el literal g) del artículo 21° Funciones de la Oficina de Administración establece que tiene la competencia para administrarlos recursos para el soporte informático de comunicaciones y desarrollo de soluciones informáticas para el cumplimiento de las funciones de la entidad;

Que, la Oficina de Administración–Área de Informática, mediante el Informe de vistos, remite el proyecto de Directiva denominado "Plan de Contingencia Informático del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres-CENEPRED", para su aprobación;

Que, con Memorándum de vistos la Oficina de Planeamiento y Presupuesto manifiesta su conformidad, con el proyecto de Directiva denominado "Plan de Contingencia Informático del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres-CENEPRED", debiéndose continuar con el trámite de aprobación;

Que, el literal c) del artículo 11° del Reglamento de Organización y Funciones del CENEPRED aprobado por Decreto Supremo N° 104-2012-PCM, prevé que la Secretaria General de la Entidad, podrá expedir Resoluciones en materia de su competencia o aquellas que se le hayan delegado;

Con la visación de la Oficina de Administración, la Oficina de Planeamiento y Presupuesto y la Oficina de Asesoría Jurídica; y,

De conformidad con lo dispuesto en el literal c) del artículo 11° del Reglamento de Organización y Funciones del CENEPRED aprobado por Decreto Supremo N° 104-2012-PCM; y en uso de las facultades conferidas mediante la Resolución Jefatural N° 135-2015-CENEPRED/J;

SE RESUELVE:

Artículo 1°.- Aprobar la Directiva N° 01-2016-CENEPRED/SG/OA "Plan de Contingencia Informático del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres-CENEPRED", propuesta por la Oficina de Administración-área de Informática.

Artículo 2°.- Encargar a la Oficina de Administración la difusión del documento normativo aprobado.

Artículo 3°.- Disponer la notificación de la presente Resolución de Secretaría General a las unidades orgánicas del CENEPRED, para las acciones correspondientes.

Regístrese, comuníquese y cúmplase.

CÉSAR A. VILLARREAL PÉREZ
Secretario General
Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres

	DIRECTIVA N° 01-2016-CENEPRED/SG/OA	
	PLAN DE CONTINGENCIA INFORMÁTICO DEL CENTRO NACIONAL DE ESTIMACION, PREVENCION Y REDUCCION DEL RIESGO DE DESASTRES - CENEPRED.	
	Formulada por: **Oficina de** Administración	Revisado por: **Oficina de Asesoría Jurídica**

I. OBJETIVO

El objetivo del Plan de Contingencia Informático es tomar las medidas preventivas necesarias para minimizar la probabilidad de que dichos riesgos se materialicen y, por otra parte, si esto ocurriera, posibilitar que la Institución tenga una respuesta acorde, sin que ello suponga un grave impacto para su continuidad operativa.

II. FINALIDAD

El Plan de Contingencia Informático tiene como finalidad definir las normas y procedimientos necesarios para afrontar las eventualidades que se produzca en los Sistemas de Información y Comunicación de la Institución, con lo que se asegura la continuidad, seguridad y confiabilidad de los sistemas mencionados.

III. BASE LEGAL

1. Ley N° 29664 Ley que crea el Sistema de Gestión de Riesgos de Desastres
2. Decreto Supremo Nº 104-2012-PCM, que aprueba el Reglamento de Organización y Funciones del CENEPRED.
3. Resolución de Contraloría N° 320-2006-CG, Normas de Control Interno.
4. Ley N° 28716 "Ley de Control Interno de la Entidades del Estado".
5. Resolución Jefatural N° 386-2002-INEI, del 31 de diciembre de 2002, que aprueba la Directiva N° 016-2002-INEI/DTNP, "Normas Técnicas para el Almacenamiento y Respaldo de la Información Procesada por las Entidades de la Administración Pública".
6. Resolución Jefatural N° 347-2001-INEI del 07 de noviembre de 2001 que aprueba la Directiva N° 018-2001-INEI/DTNP, "Normas y Procedimientos Técnicos para Garantizar la Seguridad de la Información Publicada por las Entidades de la Administración Pública".
7. Resolución Jefatural N° 090-95-INEI, del 30 de marzo de 1995 "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

IV. ALCANCE

El presente documento es de observancia por la Oficina de Administración del CENEPRED, y el Especialista de Informática y todos los servidores de la institución que tengan ineludiblemente carácter vinculante con el Plan de Contingencia Informático.

V. RESPONSABILIDAD

5.1 El responsable de la elaboración del Plan de Contingencia Informático es la Oficina de Administración a través del Especialista de Informática.

5.2 El mantenimiento y ejecución del Plan de Contingencia Informático tiene los siguientes responsables:

- El Jefe de la Oficina de Administración es responsable de la ejecución del Plan.
- El Especialista en Informática como Coordinador del Plan.
- El Técnico en Informática como apoyo para la Coordinación.
- El Técnico de Recursos Humanos como apoyo para la puesta en operaciones de los servicios.

- Profesionales de la Subdirección de Gestión de la Información de la Dirección de Gestión de Procesos – SGI-DGP, como apoyo para la puesta en operaciones de los servicios críticos.
- El personal de seguridad para apoyo con los movimientos de equipos que se puedan requerir.

VI. MARCO CONCEPTUAL

6.1 DEFINICIONES

6.1.1 Situación de Contingencia

Se entiende como Situación de Contingencia, a aquella situación en que suspende o inhabilita la operatividad de los procesos que se desarrollan en la Institución o parte de ellos, en este Plan, se contempla los posibles casos que se pueden dar. Esta situación, que, por sus características o consecuencias, impida la normal actividad de los servicios informáticos, durante un plazo estimado como no aceptable para los objetivos del servicio, y que afecten uno o más procesos de los Sistemas Críticos.

6.1.2 Plan de Contingencia

Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.

6.1.3 Procesos Críticos

Los procesos críticos son considerados indispensables para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución o para la ciudadanía en general.

6.1.4 Procesos No Críticos

Son los procesos que no son requeridos en caso de una situación de contingencia mayor.

6.1.5 Tiempo de Recuperación

Es aquel tiempo que demora en desarrollarse un trabajo de recuperación de un servicio determinado.

VII. EQUIPOS DE TRABAJO

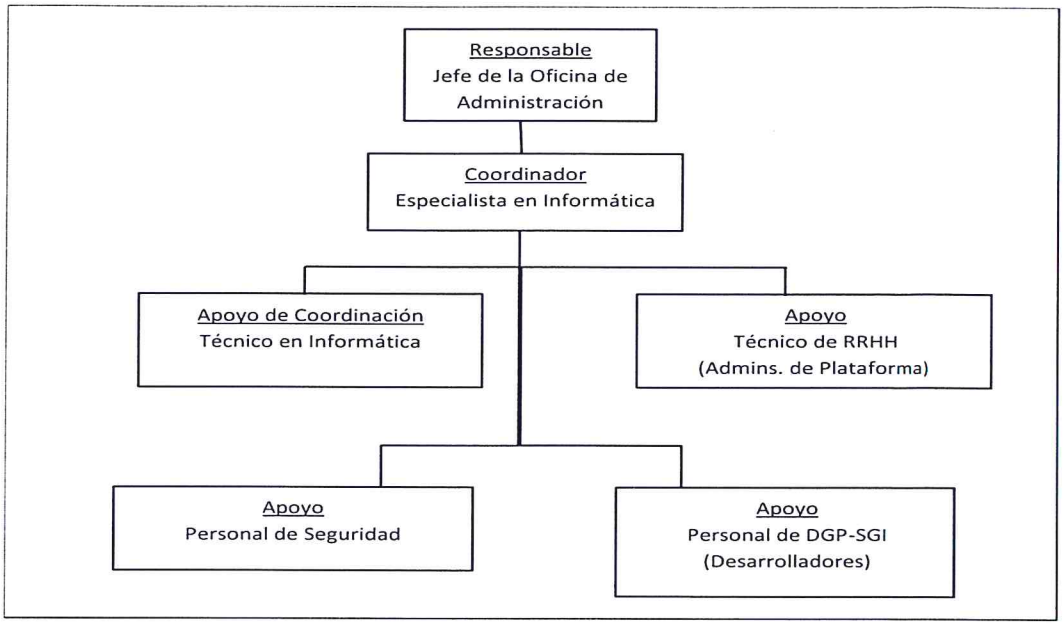
7.1 EQUIPO PLAN DE CONTINGENCIA

Esta sección identifica a las personas involucradas en el esfuerzo de recuperación del evento de contingencia y sus responsabilidades asociadas.

Teniendo en cuenta que, todas las personas identificadas en el Equipo del Plan de Contingencia, deben conocer las responsabilidades a asumir, se minimiza las posibilidades de inoperatividad de los equipos debido a la ausencia de sus integrantes o desconocimiento de sus responsabilidades.

Se determinan 2 equipos de trabajo para las actividades del Plan de Contingencia.

7.1.2 Equipo de Ejecución del Plan:



A continuación, se detallan las diferentes responsabilidades asignadas al Equipo de Ejecución del Plan de Contingencia:

a) Coordinación de Recuperación de Tecnologías de Información – CRTI
Se refiere a la coordinación, dirección respecto a acciones o estrategias a seguir en la configuración de un escenario específico de contingencia. Además de tomar la decisión de activación del Plan de Contingencia.

Los responsables de la Coordinación de Recuperación de Tecnologías de Información son:

- Jefe de Administración
- Especialista en Informática

b) Coordinación de Recuperación de Operaciones - CPO
Se refiere al aseguramiento de la documentación relacionada a operaciones, registros vitales, que serán almacenados en un ambiente seguro, además de mantener actualizado y en un lugar seguro la configuración del sistema alterno.

Los responsables de la Coordinación de Recuperación de Operaciones son:
- Especialista en Informática
- Técnico en Informática

c) Coordinación de Recuperación de Redes - CRD
Se refiere a la evaluación del daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores. Además de mantener actualizado el diagrama actual de conexiones de dispositivos, y el inventario de equipos de respaldo.

Los responsables de la Coordinación de Recuperación de Redes son:
- Técnico en Informática
- Personal de Seguridad (Apoyo)

d) Coordinación de Recuperación de Base de Datos - CBD
Se refiere a la recuperación de los servicios de Base de Datos, realizando la validación de integridad, y debidamente probada, a ser puesta a disponibilidad de los usuarios. Además de velar por el funcionamiento adecuado de los servicios de datos de la institución.

Los responsables de la Coordinación de Recuperación de Base de Datos son:
- Especialista en Informática
- Profesionales de SGI-DGP (Apoyo)
- Técnico en Informática

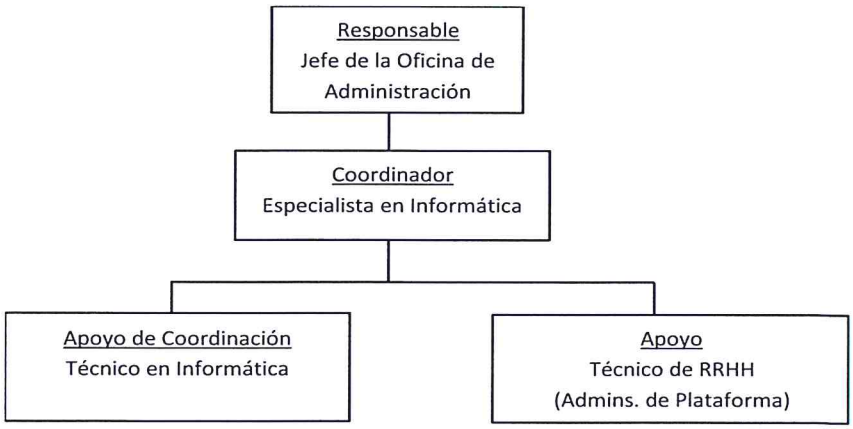
e) Coordinación de Recuperación de Seguridad Informática - CSI
Se refiere a la supervisión del cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante el evento de recuperación.

Los responsables de la Coordinación de Recuperación de Seguridad Informática son:
- Especialista en Informática
- Personal de Administración (Apoyo)

f) Coordinación de Recuperación de Aplicaciones - CSA
Se refiere al aseguramiento del correcto funcionamiento de los diferentes sistemas aplicativos una vez restablecidas las operaciones tecnológicas en la Institución.

Los responsables de la Coordinación de Recuperación de Aplicaciones son:
- Técnico en Informática
- Profesionales de SGI-DGP (Apoyo)

7.1.2 Equipo de Administración del Plan:



Las siguientes son las tareas para administrar las acciones contempladas a realizar por el Equipo de Administración del Plan de Contingencia

a) Coordinación de Administración del Plan de Contingencia
Que consiste en supervisar y dar apoyo al desarrollo de las distintas tareas respectivas a la Administración del Plan de Contingencia

Los responsables de la Coordinación de Administración del Plan son:
- Jefe de Administración
- Especialista en Informática

b) Distribución del Plan de Contingencia
Que consiste en garantizar la difusión del Plan entre los miembros del equipo y garantizar la distribución continua del plan.

Los responsables de la Distribución del Plan son:
- Jefe de Administración
- Personal de Administración (Apoyo)

c) Pruebas del Plan de Contingencia
Que consiste en supervisión y apoyo durante la ejecución de las pruebas y garantizar la ejecución de las mismas. Además del registro de los resultados de las pruebas y participar activamente en las pruebas a los sistemas de aplicación críticos.

Los responsables de las Pruebas del Plan de Contingencia son:
- Especialista en Informática
- Técnico en Informática

d) Mantenimiento del Plan de Contingencia
Que consiste en la consideración de los procedimientos de mantenimiento al Plan definido, debidamente formalizado y documentado. Además del análisis del impacto que tendrá cualquier cambio en el ambiente informático sobre el Plan de Contingencia y proceder a su actualización.

Los responsables del Mantenimiento del Plan de Contingencia son:
- Jefe de Administración
- Especialista en Informática

e) Entrenamiento en el Plan de Contingencia
Consiste en la definición y el cumplimiento oportuno de entrenamiento y capacitación en los procedimientos del Plan de Contingencia al Equipo encargado de la Ejecución del Plan.

Los responsables del Entrenamiento en el Plan de Contingencia son:
- Jefe de Administración
- Especialista en Informática

VIII. PLANIFICACIÓN

8.1 DETERMINACIÓN DE ESQUEMA DE TRABAJO

8.1.1 Identificación de Actividades y Servicios Críticos Informáticos:

Las funciones críticas de la Institución, se encuentran implementadas dentro de la infraestructura informática. Es por ello que la Institución deberá tomar medidas para tener a disponibilidad dicha infraestructura.

La determinación de las actividades y servicios críticos informáticos, se realiza en base a la determinación de los procesos críticos de la Institución. El servicio denominado Sistema de Información para la Gestión del Riesgo de Desastres – SIGRID es el proceso crítico más relevante, en mérito que gestiona la información compilada de diversas instituciones dentro del SINAGERD, es una fuente de información para las diversas instituciones involucradas en la Respuesta, Rehabilitación y Reconstrucción durante el evento de desastre.
El SIGRID, al ser un servicio crítico su recuperación deberá ser prioritaria y poner en operatividad los servicios relacionados que permitan su funcionamiento.

8.1.2 Operatividad de servicios no críticos

La habilitación de servicios no críticos se dará a través de servicios en la nube.

- Servicios de Dominio
- Enlaces de Red Internos
- Correo Institucional
- Portal Institucional
- Acceso a Internet
- Trámite Documentario
- SIAF
- SIIDE
- RITSE
- SIMSE

8.2 PROCEDIMIENTO DE RESTAURACIÓN DE SERVICIOS ALOJADOS EN SERVIDORES VIRTUALES

Periódicamente, se realizan copias de respaldo de los diferentes servicios alojados en los equipos servidores, dichas copias de respaldo se almacenan en discos duros externos que guardan copias históricas de máximo un mes de antigüedad. Dichas copias de respaldo son realizadas con el aplicativo "Copias de Respaldo de Windows Server". Es por ello que se debe conocer el procedimiento de restauración de dicho respaldo.

El procedimiento de restauración para máquinas virtuales se realiza de la siguiente manera:

- Habiéndose iniciado sesión dentro de la maquina host, se abre la ventana de "Administrador del Servidor -> Herramientas -> Copias de Seguridad de Windows Server".
- Dentro de la ventana de Copias de Seguridad de Windows Server, hacer clic derecho encima del ítem "Copia de Seguridad Local" y seleccionar "Recuperar..." y siguiente.
- Se muestra el Asistente de Recuperación, en la introducción se selecciona la ubicación donde se almacena la copia de seguridad (local o ubicación externa) y siguiente.

- Luego se muestra la ventana en donde se selecciona el tipo de ubicación donde se almacena la copia de seguridad, en este caso se selecciona "Unidad Local" y siguiente.
- En la siguiente ventana se listarán las unidades donde se encuentran copias de seguridad válidas, se selecciona la que contiene las copias de seguridad de la maquina a recuperar y siguiente.
- En la ventana, aparece el listado de hosts que tienen datos a recuperar. Se selecciona el host que deseamos recuperar y siguiente.
- Luego aparece un listado de fechas históricas de las que se tiene copia de respaldo, se selecciona la más apropiada y siguiente.
- En la siguiente ventana, se muestra las opciones de recuperación que se muestran para la fecha seleccionada, en nuestro caso se desean recuperar máquinas virtuales, por lo que se selecciona la opción "Hyper-V", y se oprime siguiente.
- Se muestran las máquinas virtuales que tienen registro de copia para la fecha seleccionada, se selecciona la máquina virtual a recuperar, y siguiente.
- Finalmente se especifica dónde se va a realizar la restauración (host original, o nuevo), y luego de la confirmación, se inicia el proceso de restauración.

La duración del proceso dependerá de la cantidad de información almacenada en la máquina virtual.

8.3 CONSIDERACIONES AL PLAN

8.3.1 Continuidad de Operaciones

La continuidad de operaciones, para el caso de los servicios informáticos, se debe considerar los siguientes componentes:

- Conectividad a internet
- Computadora con navegador

8.3.2 Operatividad Manual

Debido a la necesidad de operatividad vía plataforma informática, no es posible hacer uso de los servicios vía manual. Sin embargo, es posible consumirlos contando con un computador personal y una conexión activa de internet, sin necesidad de una ubicación específica o especializada.

8.3.3 Trabajo a Distancia y Lugar de Trabajo Alterno

En caso de requerir trabajo a distancia, se requiere implementar un equipamiento especializado para permitir conexiones de Red Privada Virtual, para asegurar la conexión y la seguridad de la información intercambiada.

8.3.4 Infraestructura Alterna

La determinación de la infraestructura alterna, se hará en base a la determinación de los servicios críticos informáticos realizados en la Institución.
Infraestructura alterna para la implementación de los servicios del SIGRID.

La infraestructura alterna deberá contar con las siguientes características:
- Estar ubicado en una zona geográfica distante a la ubicación del servicio originario.
- Contar con conectividad a internet permanente de al menos 10Mbps de subida.
- Flujo de energía respalda (mediante UPS u otro dispositivo de continuidad de energía).
- Personal técnico, con conocimiento de administración de redes y servidores.

8.4 ESCENARIOS DE CONTINGENCIAS

La evaluación de escenarios de contingencias se basa en la operatividad del centro de datos de la institución, esto es debido a que la funcionalidad de los servicios ha sido centralizada.

Los escenarios que han sido identificados son los siguientes:

Escenario 1: Falla de fluido/UPS del centro de cómputo de producción, sin afectación física y operativa de los equipos informáticos.

Escenario 2: Falla de los archivos del sistema operativo, tanto en el Servidor de aplicaciones o en el Servidor de Base de Datos, sin afectación física de los equipos informáticos.

Escenario 3: Falla de los archivos de datos, ya sea en base de datos (datafile) o, software de aplicación, sin afectación física de los equipos informáticos.

Escenario 4: Fallo físico (hardware), están comprendidos: Servidor de Base de Datos, Servidor de Aplicaciones y/o Sistema de Almacenamiento.

Escenario 5: Inoperatividad del centro de cómputo de producción, con afectación física y operativa de todos los equipos informáticos.

Con ello se tiene la matriz de tiempos de recuperación de los servicios mencionados según el escenario:

Tiempos de Recuperación
(según escenarios)

Servicios / Operac.	Escenario 1 (a partir de recuperación)	Escenario 2	Escenario 3	Escenario 4 (equipo alterno operativo)	Escenario 5
SIGRID	15 mins	2 horas	30 mins	2 horas	1.5 días
Servicios de Dominio	15 mins	1 hora (24 horas para servicio de archivos)	1 hora	1.5 horas	N/A
Enlaces de Red Internos	5 mins	N/A	N/A	15 mins	N/A
Correo Institucional	15 mins	2 horas max (SLA Optical)	2 horas max (SLA Optical)	2 horas max (SLA Optical)	2 horas max (SLA Optical)
Portal Institucional	15 mins	2 horas	30 mins	1 hora	N/A
Acceso a Internet	5 mins	2 horas max (SLA Optical)	2 horas max (SLA Optical)	2 horas max (SLA Optical)	2 horas max (SLA Optical)
Trámite Documentario	15 mins	2 horas	30 mins	1 hora	N/A
SIAF	15 mins	1 hora	1 hora	1 hora	N/A
SIIDE	15 mins	2 horas	30 mins	1 hora	N/A
RITSE	15 mins	2 horas	30 mins	1 hora	N/A
SIMSE	15 mins	2 horas	30 mins	1 hora	N/A

8.5 IDENTIFICACIÓN DE RIESGOS

Identificación de Riesgos

Los riesgos son sucesos inciertos que pueden llegar a presentarse en un futuro, dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, se consideran todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia:

a) Equipos centrales
   - Servidores

b) Comunicaciones
   - Equipos de comunicaciones
   - Enlaces de cobre y fibra óptica
   - Cableado de red de datos.

c) Software
   - Software de Base de Datos (Oracle, SQL Server, PostgreSQL)
   - Aplicativos utilizados por el CENEPRED.
   - Servidor de Aplicaciones (Apache, Apache Tomcat).
   - Antivirus para protección de servidores y estaciones de trabajo.

d) Información sobre Sistemas Informáticos
   - Base de datos utilizados por los Aplicativos.
   - Respaldo de información generada con Software Base y de Ofimática.
   - Respaldo de información generada por Aplicaciones.
   - Respaldos de Base de Datos.
   - Respaldos de información y configuración de los Servidores.

e) Equipos diversos
   - UPS
   - Aire Acondicionado (Sala de Servidores)

f) Operativos
   - Logística operativa (suministros Informáticos).

g) Servicios Públicos
   - Suministro de Energía Eléctrica.
   - Servicio de Telefonía Fija analógico/digital e Internet.

h) Recursos Humanos
   - Disponibilidad de personal de dirección.
   - Disponibilidad de personal operativo.

8.6 ÁMBITOS DE ACCIÓN

Es importante definir los procedimientos y planes de acción antes, durante y después de la ocurrencia de la falla o siniestro dentro de la Institución, a fin de recuperar la total o mayor

parte de la información, archivos y equipos informáticos, evitando así la pérdida de tiempo y dinero.

Se realizarán acciones de planificación en tres ámbitos: prevención, mitigación y recuperación.

Se debe planificar la realización tanto, de actividades previas al desastre, como las actividades durante la declaración del desastre, así como las actividades posteriores al desastre. Para ello, se deberá tener en cuenta lo siguiente:

Procedimientos previos al Desastre, con la definición del Equipo del Plan de Contingencia, teniendo un Diagnóstico Situacional, además de la definición de los procesos para el mantenimiento y administración del Plan de Contingencia, la Identificación de Riesgos y la definición de las Medidas de Precaución.

8.6.1 Acciones Preventivas

Como medida de prevención de contingencias, se deben tomar medidas para mantener la operatividad de los equipos informáticos, además de la infraestructura de comunicaciones. Para ello se deben tener en cuenta las acciones a realizar según los procedimientos para efectuar mantenimiento a los equipos informáticos.

Se realizarán mantenimientos periódicos a la infraestructura tecnológica informática, a fin de detectar debilidades, e implementar medidas correctivas, según sea el caso.

La evaluación periódica del estado de los equipos que componen tanto la plataforma informática, como la infraestructura de redes de la institución, así como los equipos que la soportan y el soporte de energía con el que se cuenta para los distintos tipos de contingencias que pudieran ocurrir, es de responsabilidad de la Oficina de Administración a través del Especialista en Informática.

Se deberá establecer la periodicidad de los mantenimientos de acuerdo al tipo y tiempo de uso del equipo informático.

8.6.2 Pasos Previos al Desastre

Se refiere al planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información y equipos informáticos, que nos aseguren el proceso de recuperación de ser necesario.

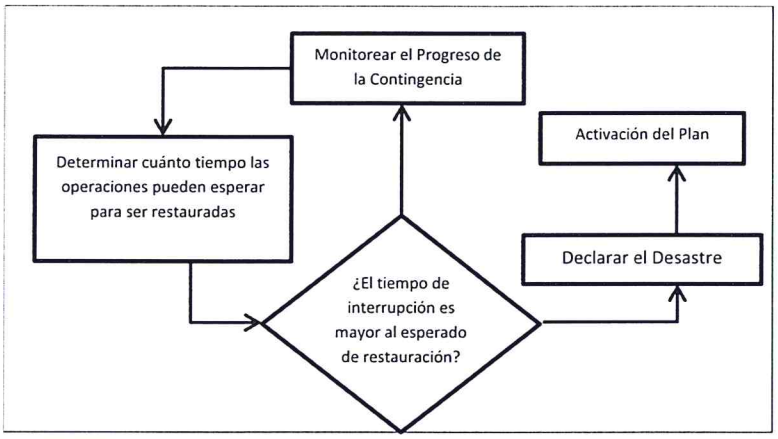
Para los procedimientos previos al desastre, se deben realizar acciones de prevención y gestión de las acciones a realizar durante la mitigación y recuperación. Es por ello que se requiere que la organización de los recursos humanos destinados a los procedimientos mencionados, realice coordinaciones en las diferentes áreas operativas.

Aquí se definen los Equipos del Plan de Contingencia, los procesos para el mantenimiento y administración del Plan de Contingencia y, las Medidas de Precaución. Adicionalmente, es aquí donde se hacen las actividades de mantenimiento y preparación de equipos, para disminuir el riesgo de una contingencia por uso o desgaste.

Se deberán seguir siguientes los criterios:

a) Criterios para activación del Plan

El siguiente diagrama muestra los criterios que deberán ser usados para activar el Plan de Contingencia:



b) Procedimiento para la activación del Plan

Este procedimiento tiene como objetivo la activación del Plan de Contingencias. De acuerdo a los criterios establecidos para la declaración del Desastre, se comunica a la Oficina de Administración, luego se comunica a Secretaría General. Con ambos se coordina la Declaración del Desastre y se activa el Plan de Contingencia.

Se deberán establecer las siguientes definiciones dentro del planeamiento:

- Definición del equipo de trabajo, y sus diferentes responsabilidades y tareas
- Equipo del Plan de Contingencia
- Equipo de Administración del Plan de Contingencia Informático.
- Definición de los servicios y actividades críticas y no críticas
- Criterios para la declaración del desastre
- Definición de Indicadores para la evaluación de los daños
- Definición de cronograma de actividades para capacitaciones, simulacros, y actualizaciones periódicas del Plan de Contingencia Informático.

8.6.3 Durante el Desastre

Durante el desastre, se debe seguir los protocolos definidos para la activación del plan, siguiendo el procedimiento para la declaración del desastre y los criterios para su activación.

Se procederá a la activación del Equipo de Trabajo definido, se establecerá el escenario dado para la contingencia actual, con lo cual se determinarán las acciones a tomar.

8.6.4 Procedimientos Posteriores al Desastre

Finalmente, luego de la contingencia, se deben realizar actividades los procedimientos posteriores al desastre, como son la Evaluación de Daños, Evaluación de Resultados, Retroalimentación del Plan de Contingencia.

IX. EJECUCIÓN DEL PLAN

9.1 ACTIVACIÓN DEL PLAN

Para realizar la activación del Plan se deben seguir los siguientes pasos:

- Determinar los servicios que han sido afectados por la contingencia, los cuales pueden ser:
  - Servicios de Dominio
  - Enlaces de Red Internos
  - Correo Institucional
  - Portal Institucional
  - Acceso a Internet
  - Trámite Documentario
  - SIAF
  - SIGRID
  - SIIDE
  - RITSE
  - SIMSE
- Determinar las operaciones afectadas por la contingencia, las cuales pueden ser:
  - Operaciones de línea
    - Operaciones en Inspecciones Técnicas de Seguridad en Edificaciones
    - Operaciones en Asistencia Técnica y Fortalecimiento de Capacidades
    - Operaciones en Monitoreo y Seguimiento
  - Operaciones Administrativas
    - Operaciones Contables-Financieras
    - Operaciones Logísticas
    - Operaciones de Soporte y Mantenimiento
    - Operaciones de Planeamiento y Presupuesto
- Determinación del *Escenario de Contingencia* específico
- Determinación de tiempos de recuperación mediante la *matriz de tiempos*
- Evaluación de *Criterios de Activación del Plan de Contingencia.*

9.2 EJECUCIÓN DEL PLAN

9.2.1. Recuperación de Contingencia Según Escenarios

9.2.1.1. Procedimiento de recuperación para el Escenario 1:

a) Servicio no crítico:
   - Se confirma no operatividad de los servicios de respaldo de energía.

- Se inicia la operación del grupo electrógeno para el centro de datos.
- Se verifica la calidad de la línea de energía del grupo electrógeno.
- Se levanta la línea de energía de los gabinetes de los servidores y switches.
- Se inician los equipos de conectividad de red (conversor de fibra, firewall y finalmente switches) y se verifica operatividad.
- Se inicia el servidor HP02, luego se inicia la máquina virtual de Dominio, se verifican sus servicios (red, internet, etc.).
- Se inicia el host donde se aloja el servicio no crítico, luego se inicia la máquina virtual del servicio no crítico, y se verifica su operatividad.

b) Servicio Crítico:
- Se confirma no operatividad de los servicios de respaldo de energía.
- Se inicia la operación del grupo electrógeno para el centro de datos.
- Se verifica la calidad de la línea de energía del grupo electrógeno.
- Se levanta la línea de energía de los gabinetes de los servidores y switches.
- Se inician los equipos de conectividad de red (conversor de fibra, firewall y finalmente switches) y se verifica operatividad.
- Se inicia el servidor HP02, luego se inicia la máquina virtual de Dominio, se verifican sus servicios (red, internet, etc.).
- Se inicia el host donde se aloja el servicio no crítico, luego se inicia la máquina virtual del servicio no crítico, y se verifica su operatividad.

c) Coordinaciones involucradas:
- Coordinación de Recuperación de Tecnologías de Información
- Coordinación de Recuperación de Operaciones
- Coordinación de Recuperación de Redes
- Coordinación de Recuperación de Aplicaciones

9.2.1.2. Procedimiento de recuperación para el Escenario 2:

a) Servicio no crítico:
- Se da de baja al registro de la máquina virtual comprometida.
- Se realiza el *procedimiento de restauración de la máquina virtual* desde las copias de respaldo del sistema.
- Una vez terminado el proceso de restauración, se inicia la máquina virtual afectada y se verifica la configuración de red, además se verifica la conectividad de la máquina restaurada.
- Finalmente, se verifica la operatividad de los servicios afectados.

b) Servicio Crítico:
- Se da de baja al registro de la máquina virtual comprometida.
- Se realiza el *procedimiento de restauración de la máquina virtual* desde las copias de respaldo del sistema.
- Una vez terminado el proceso de restauración, se inicia la máquina virtual afectada y se verifica la configuración de red, además se verifica la conectividad de la máquina restaurada.

- Finalmente, se verifica la operatividad de los servicios afectados.

c) Coordinaciones involucradas:
- Coordinación de Recuperación de Operaciones
- Coordinación de Recuperación de Base de Datos
- Coordinación de Recuperación de Redes

9.2.1.3. Procedimiento de recuperación para el Escenario 3:

a) Servicio no crítico:
- Se verifica si la contingencia involucra datos y/o aplicativo.
- En caso de que esté involucrado el aplicativo, se realiza la instalación del aplicativo comprometido, desde la copia de respaldo del mismo.
- Luego se restaura la base de datos del aplicativo comprometido, desde la copia de respaldo de la misma.
- Se verifica la configuración del aplicativo, luego se verifica la operatividad del mismo.

b) Servicio Crítico:
- Se verifica si la contingencia involucra datos y/o aplicativo.
- En caso de que esté involucrado el aplicativo, se realiza la instalación del aplicativo comprometido, desde la copia de respaldo del mismo.
- Luego se restaura la base de datos del aplicativo comprometido, desde la copia de respaldo de la misma.
- Se verifica la configuración del aplicativo, luego se verifica la operatividad del mismo.

c) Coordinaciones involucradas:
- Coordinación de Recuperación de Operaciones
- Coordinación de Recuperación de Aplicaciones
- Coordinación de Recuperación de Base de Datos

9.2.1.4. Procedimiento de recuperación para el Escenario 4:

a) Servicio no crítico:
- Se verifica la operatividad del equipo host alterno. En caso de encontrarse operativo, se realiza el *procedimiento de restauración del servicio*.
- Se realiza las configuraciones de red respectivas.
- Una vez terminado el proceso de restauración, se inicia la máquina virtual afectada y se verifica la configuración de red, además se verifica la conectividad de la máquina restaurada.
- Finalmente, se verifica la operatividad de los servicios afectados.

b) Servicio Crítico:
- Se verifica la operatividad del equipo host alterno. En caso de encontrarse operativo, se realiza el *procedimiento de restauración del servicio*.

- Se realiza las configuraciones de red respectivas.
- Una vez terminado el proceso de restauración, se inicia la máquina virtual afectada y se verifica la configuración de red, además se verifica la conectividad de la máquina restaurada.
- Finalmente, se verifica la operatividad de los servicios afectados.

c) Coordinaciones involucradas:
- Coordinación de Recuperación de Operaciones
- Coordinación de Recuperación de Aplicaciones
- Coordinación de Recuperación de Base de Datos

9.2.1.5. Procedimiento de recuperación para el Escenario 5:

a) Servicio no crítico:
- Debido a que no es un servicio crítico, dicho servicio se restablecerá cuando se restablezcan las operaciones del centro de datos

b) Servicio Crítico:
- Se activa el procedimiento de restauración del servicio en la ubicación alterna.
- Se verifican los servicios localmente en la ubicación alterna.
- Se realizan las coordinaciones para la asignación de una dirección IP pública en caso de ser necesario, y se verifica la operatividad del servicio.

c) Coordinaciones involucradas:
- Coordinación de Recuperación de Tecnologías de Información
- Coordinación de Recuperación de Operaciones
- Coordinación de Recuperación de Aplicaciones
- Coordinación de Recuperación de Base de Datos

9.3 EVALUACIÓN DEL IMPACTO Y RETROALIMENTACIÓN

El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos informáticos en:

- Impacto Alto: Se considera que una actividad crítica tiene impacto alto sobre las operaciones de la entidad cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.

- Impacto Medio: Se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones de la entidad por un tiempo mínimo de tolerancia.

- Impacto Bajo: Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la entidad.

Esta evaluación será de responsabilidad del Jefe de la Oficina de Administración y del Especialista en Informática.

X. GLOSARIO DE TERMINOS

- **Contingencia:** Se entiende como contingencia, a la posibilidad o riesgo de que suceda un evento de forma imprevista.
- **Peligro:** Circunstancia o situación que aumenta la inminencia de daños.
- **Riesgo:** Estar expuesto a un peligro
- **Emergencia:** Suceso que sobreviene de una forma imprevista.
- **Servicio:** Realizar una labor o proceso requerido por un cliente del mismo.
- **Operación:** Realización de una tarea o proceso.
- **Switch de Red:** Conmutador o interruptor de una señal digital dentro de una red de computadoras.
- **Firewall:** Es un dispositivo que se emplea para proteger una red. Lo que hace es bloquear los accesos no autorizados, limitando el tráfico de acuerdo a diversos criterios.
- **Dominio:** El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar.
- **Host:** Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella, las cuales alojan a computadoras virtuales llamadas "máquinas virtuales".
- **Máquina Virtual/Servidor Virtual:** Es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.
- **Copia de Respaldo/Copia de Seguridad:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Aplicativo:** Es una secuencia de instrucciones, escritas para realizar una tarea específica en una computadora.
- **Disco Duro:** Es el dispositivo de almacenamiento de datos que emplea un sistema de grabación magnética para almacenar archivos digitales.
- **Restauración/Recuperación:** Es la acción de leer y grabar en la ubicación original u otra alternativa los datos previamente respaldados.
- **Unidad de Almacenamiento:** Es un conjunto de componentes utilizados para leer o grabar datos en el soporte de almacenamiento de datos, en forma temporal o permanente.
- **Red Privada Virtual:** Es la interconexión de red entre equipos informáticos realizada de manera virtual, sin mediar conexión física alguna.