PLAN DE CONTINGENCIA INFORMÁTICO

2024

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

ÍNDICE

1.- INTRODUCCIÓN 3

2.- OBJETIVOS 4

2.1. Objetivo General 4

2.2. Objetivos Específicos 4

3.- ALCANCE 5

4.- BASE LEGAL 5

5.- MARCO TEÓRICO 5

5.1. Plan de Contingencia Informático 5

5.2. Plan de Prevención 6

5.3. Plan de Ejecución 6

5.4. Plan de Recuperación 6

5.5. Plan de Pruebas 6

6.- DEFINICIONES 6

7.- METODOLOGÍA 10

7.1. Fase 1: Planificación 10

7.1.1. Organización 10

7.1.2. Funciones 10

7.2. Fase 2: Identificación y priorización de riesgos 11

7.2.1. Análisis del Riesgo 11

7.2.2. Probabilidad del Riesgo 12

7.2.3. Impacto del Riesgo 12

7.2.4. Evaluación del Riesgo 12

7.2.5. Definición de Eventos Controlables y no Controlables 12

7.2.6. Definición de Matriz de Riesgo 13

7.3. Fase 3: Definición de eventos susceptibles de contingencia 17

7.4. Fase 4: Elaboración del Plan de Contingencia 19

7.5. Fase 5: Plan de Pruebas del Plan de Contingencia 19

7.5.1. Objetivos 19

7.5.2. Alcance 20

7.5.3. Definición 20

7.5.4. Lugar de la prueba 21

7.5.5. Cronograma de pruebas 21

7.5.6. Resultado de la prueba 21

7.6. Fase 6: Implementación del Plan de Contingencia 21

7.7. Fase 7: Monitoreo 21

8.- DESARROLLO DE LAS FASES Y ACTIVIDADES 22

8.1. Desarrollo de las Fases 22

8.2. Desarrollo de las Actividades 28

1.- INTRODUCCIÓN

El presente documento contiene el Plan de Contingencia Informático periodo 2024 de Plan COPESCO Nacional, de acceso a la Información en materia de Riesgos de Tecnología de Información y Comunicaciones (TIC).

Se establece el objetivo, alcance y metodología desarrollada. Incluye, además, las definiciones utilizadas, las políticas de seguridad, el análisis de la situación, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos de TIC.

El plan de contingencia de la información vital de Plan COPESCO Nacional ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático. Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos.

Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. La coordinación de TICS tiene el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a eso es importante contar con un Plan de Contingencia adecuado de forma que ayude al Plan COPESCO Nacional a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la Institución.

Los responsables del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a los líderes de los procesos, las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

Para realizar el Plan de Contingencia Informático de Plan COPESCO Nacional se tiene en cuenta la información como uno de los activos más importantes de la entidad, además que la infraestructura informática está conformada por el hardware, software y elementos

complementarios que soportan la información o datos críticos para la función de la entidad. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. Es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

2.- OBJETIVOS

2.1. Objetivo General

Garantizar la continuidad operativa en los procedimientos informáticos de Plan COPESCO Nacional, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la entidad.

2.2. Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos de Plan COPESCO Nacional que pueda suspender completa o parcialmente la prestación de alguno de los servicios prestados.
- Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas específicas determinadas a proteger la información contra los daños y perjuicios producidos por cortes de fluido eléctrico, fenómenos naturales, ingeniería social o vandalismo.
- Continuar brindando servicios de Tecnologías de Información a la Comunidad Interna y Externa de Plan COPESCO Nacional que se hayan visto afectadas por una situación adversa.

3.- ALCANCE

El Plan de Contingencia Informático alcanza a todos los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, servicios, equipos e instalaciones tecnológicas, personal y otros administrados por el Área de Informática de Plan COPESCO Nacional.

4.- BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 28716, Ley de Control Interno de las entidades del Estado.
- Resolución Ministerial N° 265-2015-MINCETUR, que aprueba el Manual de Operaciones de Plan COPESCO Nacional.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

5.- MARCO TEÓRICO

5.1. Plan de Contingencia Informático

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se haya visto afectado negativamente por causa de algún incidente interno o externo a la organización.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- Antes, como un plan de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El término “incidente” en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático.

5.2. Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

5.3. Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

5.4. Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

5.5. Plan de Pruebas

Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

6.- DEFINICIONES

a. **Amenaza:** Posible peligro que una situación, un objeto o una circunstancia especifica puede conllevar para la vida, de uno mismo o de terceros o de un sistema de información. Es un peligro que está latente, que todavía no se ha desencadenado pero que sirve como aviso para prevenir o para presentar la posibilidad de que sí lo haga. Posibilidad de ocurrencia de un suceso.

b. **Ataque:** Acción o evento que intente intervenir con el funcionamiento adecuado de un sistema informático, conectividad de una red de computadoras o intento de obtener un modo no autorizado la información confiada de una computadora.

c. **Ataque de Denegación de Servicio:** Acción o evento que intente intervenir con el funcionamiento adecuado de un sistema informático, conectividad de una red de computadoras o intento de obtener un modo no autorizado la información confiada de una computadora.

d. **Centro de Datos:** Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dentro de este concepto también se consideran los ambientes de comunicaciones de la Entidad.

e. **Confidencialidad:** Asegurar que el acceso a la información, sólo lo tengan las personas autorizadas.

f. **Contingencia:** Es la alteración de la continuidad del negocio, que informa en forma relevante el normal desarrollo de un servicio considerando crítico, teniendo su origen en la falla de uno o varios componentes o la interrupción de una tarea sin estar necesariamente prevista.

g. **Desastres Naturales:** Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa e indirecta. Dentro de los desastres naturales se entienden otros incidentes que se producen sin intervención humana como: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, etc. Se excluyen desastres específicos tales como incendios e inundaciones.

h. **Disponibilidad:** Se refiere a que la información se encuentre accesible en el momento que se requiera.

i. **Fallas de Hardware:** Las fallas de Hardware pueden ser críticas si se trata de averías que dejan sin funcionamiento a servidores o a dispositivos de telecomunicaciones de la empresa. La mejor manera para prevenir este tipo de contingencias es una labor continua y periódica de supervisión de los equipos Hardware, así como un control de garantía de estos.

j. **Fallas en software de Aplicación:** Existe una variedad amplia de errores de software. Desde errores cometidos en la programación de las aplicaciones hasta fallas del sistema operativo instalado en una máquina.

k. **Fallas o interrupción en los suministros de los Sistemas de Telecomunicaciones:** Las fallas o interrupciones en los sistemas de telecomunicaciones pueden afectar el funcionamiento correcto de las actividades del negocio y comprometer los servicios prestados por la red de datos de Plan COPESCO Nacional.

l. **Incendio:** Aunque la posibilidad de que se produzca un incendio grave es muy remota, las pérdidas que se producirían como consecuencias de este serían muy cuantiosas, por lo tanto, es siempre conveniente estar preparado ante una situación de grandes magnitudes ocasionando grandes consecuencias.

m. **Incidente:** Es cualquier evento que interrumpa el funcionamiento normal de un servicio afectando ya sea a uno, a un grupo o a todos los usuarios de un servicio, un incidente puede ser un inadecuado funcionamiento de los servicios de TI; estos pueden producir una reducción en la calidad de los servicios de TI.

n. **Integridad:** Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

o. **Interrupción del Suministro de Energía:** La interrupción o cortes de Energía eléctrica originan una parada temporal de los servicios de organización durante el tiempo que dura este. Pueden ocasionar además la perdida de datos y fallas graves de continuidad del negocio. Sin embargo, las pérdidas estimadas que podrían ocasionarse en la relación a la probabilidad de que el riesgo se materialice y las medidas preventivas no son muy altas.

p. **Intrusión (hackeo):** Acceso no autorizado a una estación de trabajo, servidor o red de datos del cual puede comprometer la comunidad de los servicios de la institución de la seguridad informática.

q. **Plan de contingencia:** Es un instrumento de gestión para una buena administración de las Tecnologías de la Información y Comunicaciones en el dominio de soporte y desempeño.

r. **Plan de Continuidad del Negocio:** Establece un esquema que ayuda a una organización a recuperarse después de un desastre. Es decir, es un mapa que detalla

cómo una organización puede continuar operando mientras dura la recuperación del desastre.

s. **Privacidad:** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundida o transmitida a otros.

t. **Sabotaje:** El sabotaje, normalmente es ocasionado por empleados de la misma empresa como actos de venganza o reivindicación, pueden ocasionar daños muy graves a los activos de los sistemas de información.

u. **Seguridad de la Información:** Se refiere a un conjunto de medidas preventivas y reactivas tomadas por las organizaciones con la finalidad de resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad.

v. **Siniestro:** Se entiende por Siniestro a las emergencias originadas por la naturaleza (sismos, inundaciones, erupciones volcánicas, deslizamientos, entre otros), y aquellas producidas por causas no controlables tales como choques eléctricos, explosiones, derrames, etc.

w. **Violaciones a la Seguridad de acceso a la infraestructura:** Este tipo de amenazas suponen una serie de daños potenciales muy graves para la organización, si bien es cierto de la probabilidad de que lleguen a producirse es muy remota. Las medidas de seguridad actual, llevada a cabo en su mayoría por la empresa de seguridad contratada, así como una política de restricciones de acceso a lugares críticos de la institución, deben asegurar una protección eficiente, aunque sencilla contra este tipo de ataques.

x. **Virus:** La forma más sencilla de contraer un virus en los sistemas informáticos es mediante periféricos infectados que son conectados a los equipos o estaciones de trabajo. La probabilidad de recibir un ataque es menor, ya que los firewalls instalados, las reglas de entrada/salida de los equipos de comunicaciones y configuración de las redes de datos.

7.- METODOLOGÍA

El desarrollo del Plan de Contingencia seguirá la siguiente metodología basada en siete (7) fases:

- Fase 1: Planificación
- Fase 2: Identificación y priorización de riesgos
- Fase 3: Definición de eventos susceptibles de contingencia
- Fase 4: Elaboración del Plan de Contingencia
- Fase 5: Plan de Pruebas del Plan de Contingencia
- Fase 6: Implementación del Plan de Contingencia
- Fase 7: Monitoreo

7.1. Fase 1: Planificación

7.1.1. Organización

El Área de Informática depende directamente de la Unidad de Administración, y tiene dentro de sus funciones supervisar la gestión de activos de Tecnologías de la Información, coordinar, ejecutar y supervisar las actividades relacionadas a los servicios de seguridad, comunicaciones, administración, respaldo y contingencia en la arquitectura de infraestructura y comunicaciones necesaria para el cumplimiento de los objetivos de Plan COPESCO Nacional.

Para la ejecución del Plan de Contingencia Informático, se cuenta con un Comité de Contingencia, conformado por:

a. Coordinadora del Área de Informática (Coordinadora del Plan de Contingencia Informático)
b. Coordinador (a) del Área de Logística
c. Analista en Tecnologías de Información

7.1.2. Funciones

a. Coordinador del Plan de Contingencia Informático

Es el canal de comunicación entre los equipos operativos a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan de Contingencia, los niveles de ejecución y el estado de los recursos informáticos que cubre el plan. Es el que autoriza la activación y puesta

en marcha del Plan de Contingencias TI cuando lo considere necesario de acuerdo con el reporte dado por el equipo de ejecución del plan.

b. Comité de Contingencia

El Comité del Plan de Contingencia es el órgano donde se coordinan y aprueban todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio.

Funciones y Roles:

- Velar por el buen funcionamiento de los diferentes sistemas de información y la infraestructura tecnológica de Plan COPESCO Nacional.
- Supervisar el funcionamiento de los servicios del centro de datos.
- Verificar y garantizar el correcto funcionamiento de las aplicaciones durante y después de la contingencia.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Coordinar la ejecución de las actividades del plan de pruebas.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.
- Coordinar con los recursos y/o proveedores externos necesarios para soportar y restaurar los servicios afectados por la contingencia.
- Proponer la incorporación y/o modificaciones del Plan de contingencia.

7.2. Fase 2: Identificación y priorización de riesgos

Denominamos INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

7.2.1. Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo

que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

7.2.2. Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Asimismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

7.2.3. Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

7.2.4. Evaluación del Riesgo

La evaluación al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración.

7.2.5. Definición de Eventos Controlables y no Controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos de Plan COPESCO Nacional, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

- Eventos Controlables, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

- Eventos No Controlables, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.

Esta identificación se hará en la matriz de riesgo explicada a continuación.

7.2.6. Definición de Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán como se indica en el cuadro N° 1.

Cuadro Nº 1. Cuadro de Impactos

IMPACTO	DESCRIPCIÓN	VALOR
Poco Impacto	Perdida de Información y/o equipamiento no sensitivo	1
Moderado Impacto	Perdida de Información Sensible.	2
Alto Impacto	Perdida de Información Sensible, retraso o interrupción.	3
Gran Impacto	Información crítica, daño serio, patrimonial.	4

Cuadro N.º 2. Cuadro de Probabilidad de Ocurrencia

PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN
Frecuente	Incidentes Repetidos
Probable	Incidentes Aislados
Ocasional	Sucede Alguna vez
Remoto	Improbable que suceda

Asimismo, la probabilidad de ocurrencia de un evento resulta de gran importancia para determinar qué tan posible es que dicho evento se presente en la realidad. La determinación de esta probabilidad se obtendrá de la estadística recogida de los eventos que se hayan presentado a lo largo de la administración del servicio por

otros proveedores, así como la información obtenida de otros planes de contingencia para servicios similares.

Evaluación = Impacto X Probabilidad.

Cuadro N.º 3. Evaluación del Riesgo

	POCO	MODERADO	ALTO	GRAN
FRECUENTE	1	2	3	4
PROBABLE	1	2	3	4
OCASIONAL	1	2	3	4
REMOTO	1	2	3	4

Finalmente, después de haber ponderado y validado objetivamente las probabilidades de ocurrencia y los impactos asociados, se establecerán las políticas que se han de considerar para determinar cuáles son aquellos eventos que formarán parte del Plan de Contingencia, como sigue:

- Todo evento cuya calificación sea de "Gran Impacto: 4", será considerado obligatoriamente dentro del Plan de Contingencia.

- Todo evento cuya exposición al riesgo sea mayor o igual a 0.15 será también considerado en el Plan de Contingencia (ver Cuadro N °4).
  El cuadro N °4 muestra la matriz de Riesgo de Contingencia, ponderado de acuerdo a los valores de riesgo e impacto en el servicio (operatividad).

Cuadro N.º 4. Matriz de riesgo de contingencia

ÍTEM	IDENTIFICACIÓN DEL RIESGO	PROBABILIDAD	IMPACTO	CALIFICACIÓN	ALERTA	CATEGORÍA
Riesgos Relacionados a Siniestros						
	INFRAESTRUCTURA					
1	Incendio	0.04	4	0.16		EC
2	Sismo	0.10	4	0.40		ENC

3	Inundación por desperfectos de los servicios sanitarios	0.02	1	0.02		EC
	SERVICIOS PÚBLICOS					
4	Interrupción de Energía Eléctrica	0.10	4	0.40		ENC
5	Falta de suministro de Agua	0.01	3	0.03		ENC
6	Interrupción de Servicios de Telefonía	0.01	3	0.03		ENC
7	Interrupción de Servicio de Hosting	0.02	3	0.06		ENC
	EQUIPO					
8	Falla de UPS	0.03	4	0.12		EC
Riesgos Relacionados a Sistemas de Información						
	INFORMACIÓN					
09	Extravío de Documentos	0.02	3	0.06		EC
10	Sustracción o Robo de Información	0.02	3	0.06		EC
	SOFTWARE					
11	Infección de Equipos por Virus	0.05	4	0.20		EC
12	Perdida de los Sistemas Centrales	0.05	4	0.20		EC
13	Perdida del Servicio de Correo	0.05	2	0.10		EC
14	Fallas del Motor de Base de Datos	0.04	4	0.16		EC
15	Falla del Sistema Operativo	0.04	4	0.16		EC
	COMUNICACIONES					

16	Fallas en la red de comunicaciones Interna	0.02	4	0.08		EC
17	Caída en el servicio de Internet	0.04	4	0.16		EC
	HARDWARE					
18	Fallas de Equipos Personales	0.02	2	0.04		EC
	RECURSOS OPERATIVOS Y LOGÍSTICOS					
19	Falla de Equipos Multimedia, Impresoras, Scanner y otros.	0.05	2	0.10		EC
Riesgos relacionados a recursos humanos						
	RECURSO HUMANO					
20	Ausencia Imprevista del personal de Soporte Técnico	0.05	3	0.15		EC
21	Ausencia del Personal Ejecutivo para la toma de decisiones de riesgo informático	0.05	3	0.15		EC
22	Falta de idoneidad en reserva de la información de la Base de Datos.	0.01	4	0.04		EC
Plan de Seguridad Física						
	INFRAESTRUCTURA					
23	Sustracción de Equipos y software Diversos	0.02	2	0.04		EC
24	Sabotaje	0.01	2	0.02		ENC
25	Vandalismo	0.01	3	0.03		ENC
26	Actos Terroristas	0.01	4	0.04		ENC

- **Nota:** El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.
- En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (EC), y No Controlables (ENC).

Después de todo lo expuesto, se elaborará la "Matriz de Riesgo de Contingencia" en la cual se tendrá en cuenta todos los eventos susceptibles de entrar en contingencia, indicando su Calificación y categorización (controlable / no controlable) para la elaboración del Plan de Contingencia.

Asimismo, se utilizarán los siguientes tópicos como una forma de agrupar a dichos eventos:

- Contingencias relacionadas a Siniestros
- Contingencias relacionadas a los Sistemas de Información
- Contingencias relacionadas a los Recursos Humanos
- Plan de Seguridad Física

7.3. Fase 3: Definición de eventos susceptibles de contingencia

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación:

- **Hardware**
  - Servidores
  - Estaciones de trabajo (Laptops y PC´s).
  - Impresoras, fotocopiadoras, Scanner.
  - Equipos Biométricos.
  - Equipos multimedia.

- **Comunicaciones**
  - Equipos de Internet.
  - Equipos de comunicaciones Switch.
  - Equipo de Telefonía fija.
  - Cableado de Red de Datos.

- **Software**
  - Software de Base de Datos: SQL Server, MySQL Server.

- Sistemas utilizados por Plan COPESCO Nacional: Sistema Integrado de Administración Financiera "SIAF-SP", Sistema Integrado de Gestión Administrativa "SIGA-MEF", Sistema de Gestión de Proyectos – Obras "SGPO".
- Software Base: Sistemas operativos y Ofimática.
- Antivirus para protección de servidores y estaciones de trabajo.

- **Información sobre sistemas informáticos**
  - Base de datos utilizados por los sistemas.
  - Respaldo de información generada con Software Base y de Ofimática.
  - Respaldo de las aplicaciones utilizadas por Plan COPESCO Nacional.
  - Respaldo de Base de Datos.
  - Respaldo de información y configuración de los Servidores.

- **Equipos Diversos**
  - UPS
  - Aire Acondicionado

- **Infraestructura Física**
  - Sede Principal: Av. José Gálvez Barrenechea N° 290 Urbanización Córpac – San Isidro.
  - Local Anexo: Calle 17 N° 525 Urbanización Córpac – San Isidro

- **Operativos**
  - Logística operativa (Suministros Informáticos)

- **Servicios Públicos**
  - Suministro de Energía Eléctrica.
  - Servicio de Telefonía Fija y Móvil.
  - Suministro de Agua.
  - Servicio de Web Hosting.

- **Recursos Humanos**
  - Disponibilidad de personal de dirección.
  - Disponibilidad de personal operativo.

7.4. Fase 4: Elaboración del Plan de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por el personal del Plan COPESCO Nacional.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan, así se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin. El contenido de todos los eventos que conformarán el Plan de Contingencia es:

- **Formato de Registro del Plan de Contingencia**
  Para una lectura fácil y rápida del Plan de Contingencia, se ha diseñado un formato, el mismo que describimos a continuación y que se compone de las siguientes partes:
- **Encabezado:** El formato tiene un encabezado, cuyo contenido se presenta como sigue:
- **Elaborado:** En todos los casos se indica "Plan COPESCO Nacional".
- **Código del Formato:** RC – XX (ver matriz de riesgo de Contingencia).
- **Nombre del evento:** Claro y de fácil entendimiento.
- **Cuerpo Principal**
  En el cual se desarrollará cada uno de los eventos que formarán parte del Plan de Contingencia y se describe el contenido que deberá ir en cada campo.

7.5. Fase 5: Plan de Pruebas del Plan de Contingencia

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- Metodología (descripción de la prueba a efectuarse)
- Alcances (áreas afectadas / personal involucrado)
- Resultados

7.5.1. Objetivos

Las pruebas del Plan de Contingencia Informático se establecen como un proceso continuo cuyos objetivos son:

- Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte del Plan de Ejecución del Plan de Contingencia respecto a una

posible interrupción de los procesos identificados como críticos para el servicio del Plan COPESCO Nacional.

- Identificar por medio de la prueba, las posibles causas que puedan atentar contra su normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).
- Determinar los roles y funciones que cumplirán los responsables en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.

7.5.2. Alcance

El plan de pruebas estará enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

7.5.3. Definición

El Plan de Contingencia Informático se debe probar por lo menos una (01) vez al año o cuando ocurra un evento determinado, como cambios en la organización, en los procesos o la tecnología.

Descripción de la Prueba

a. Prueba de campo - simulación parcial o segmentada

Se simula un tipo de impacto a través de los eventos de riesgo definidos. La prueba se limita a los activos tecnológicos mencionados en el alcance.

La prueba permite al Comité del Plan de Contingencia Informático ejecutar los procedimientos de contingencia y poder validar una o más partes del plan, haciendo uso del checklist de prueba.

b. Premisa

La prueba inicia desde que el Coordinador del Plan de Contingencia Informático coordina la activación de la contingencia.

c. Checklist - Prueba del Plan de Contingencia

Es una herramienta que se utiliza para la ejecución de las pruebas del Plan de Contingencia. Dicha herramienta permite al Comité del Plan de Contingencia Informático, controlar los tiempos de cada actividad a ejecutar durante las pruebas.

7.5.4. Lugar de la prueba

- Sede Principal: Av. José Gálvez Barrenechea N° 290 Urbanización Corpac – San Isidro.
- Local Anexo: Calle 17 N° 525 Urbanización Córpac – San Isidro

7.5.5. Cronograma de pruebas

Las pruebas relacionadas a este plan, se deberán ejecutar de forma anual, se precisa en el Anexo N° 01, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato de control y certificación de las pruebas detallado en el Anexo N° 02.

Las pruebas deben realizarse fuera del horario laboral, de ser el caso, a fin de no afectar la disponibilidad de los servicios.

7.5.6. Resultado de la prueba

Los resultados de las pruebas deberán ser presentados en un informe, el cual deberá contener al menos la siguiente información:

- Escenario de Pruebas
- Detalle de Ejecución de Pruebas
- Resultado de las Pruebas

7.6. Fase 6: Implementación del Plan de Contingencia

La implementación del presente plan se realizará a partir del segundo mes de su aprobación.

Para tal efecto, el Comité del Plan de Contingencia Informático, realiza las siguientes funciones:

- Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información.
- Participar en las pruebas y simulacros de desastres.

7.7. Fase 7: Monitoreo

Esta fase es primordialmente de mantenimiento, cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

Actividades principales a realizar:

- Revisión continua de infraestructura tecnológica, aplicaciones y sistemas de información.
- Revisión continua de copias de respaldo (Backup).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos.

8.- DESARROLLO DE LAS FASES Y ACTIVIDADES

8.1. Desarrollo de las Fases

El Área de Informática, plantea el desarrollo de los tópicos, utilizando la metodología expuesta anteriormente.

Este desarrollo incluirá las siguientes fases de la metodología:

1.- Identificación y priorización de riesgos
2.- Definición de eventos susceptibles de contingencia.
3.- Elaboración del Plan de Contingencia.

1.- Identificación y priorización de riesgos

En los **Cuadros N° 5 y N° 6** se resumen los eventos según la categorización de eventos controlables y no controlables:

Cuadro N.° 5. Eventos Controlados

Ítem	Eventos Controlados
1	Incendio
3	Inundación por desperfecto de los servicios sanitarios
8	Falla de UPS
9	Extravió de documentos
10	Sustracción o robo de información
11	Infección de equipos por virus
12	Perdidas de los Sistemas Centrales
13	Perdida del servicio de correo
14	Falla del motor de la Base de Datos
15	Falla del Sistema Operativo
16	Fallas en la red de Comunicaciones Internas
17	Caída en el servicio de internet.
18	Fallas de Equipos Personales.
19	Fallas de equipos multimedia, impresoras, scanner y otros.

20	Ausencia imprevista del Personal de soporte Técnico
21	Ausencia de personal ejecutivo para la toma de decisiones ante riesgo informático.
23	Sustracción de Equipos y software Diversos

Cuadro N.º 6. Eventos No Controlados

Ítem	Eventos No Controlados
2	Sismo
4	Interrupción de Energía Eléctrica
5	Falta de Suministro de Agua
6	Interrupción de Servicios de Telefonía
7	Interrupción de Servicio de Hosting
22	Falta de idoneidad del personal en la reserva de información de la Base de Datos.
24	Sabotaje
25	Vándalos
26	Actos Terroristas

2.- Definición de Eventos de Susceptibles de Contingencia

El cuadro N.º 7 "Elementos vs. Subfactores", muestra la relación existente entre los elementos mínimos definidos por el Área de Informática, haciendo una referencia de todos los Planes de Contingencia relacionados al mismo e indicando a que subfactor desarrollado pertenecen.

Cuadro N.º 7. Elementos vs. Sub Factores a desarrollar

ELEMENTO	PLAN DE CONTINGENCIA DESARROLLADO		
	CODIGO	ALCANCE	SUBFACTOR
HARDWARE			
Servidores	RC-04	Servicios Públicos	Contingencia Suministros
	RC-11	Información	Contingencia Sistemas Información
	RC-12	Software	Contingencia Sistemas Información
	RC-13	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información
	RC-16	Software	Contingencia Sistemas Información
	RC-25	Infraestructura	Contingencia Seguridad Física

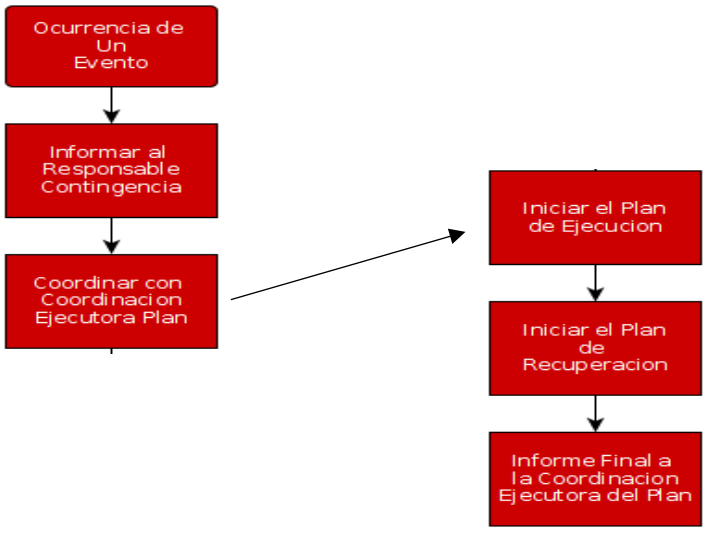
Estaciones de Trabajo (Laptops y Pc's)	RC-04	Servicios Públicos	Contingencia Suministros
	RC-10	Información	Contingencia Sistemas Información
	RC-12	Software	Contingencia Sistemas Información
	RC-18	Comunicaciones	Contingencia Sistemas Información
	RC-25	Infraestructura	Contingencia Seguridad Física
	RC-26	Infraestructura	Contingencia Seguridad Física
Equipos Biométricos	RC-04	Servicios Públicos	Contingencia Suministros
	RC-15	Software	Contingencia Sistemas Información
	RC-16	Software	Contingencia Sistemas Información
Fotocopiadoras, Impresoras, Scanner y/o Equipos Multimedia	RC-19	Operativo	Contingencia Sistemas Información
Equipos de Internet	RC-17	Información	Contingencia Sistemas Información
Equipos Multimedia	RC-18	Operativo	Contingencia Sistemas Información
COMUNICACIONES			
Equipos de Comunicaciones, Switch y Conectores RJ-45	RC-17	Comunicaciones	Contingencia Sistemas Información
Equipos de Telefonía Fija	RC-17	Comunicaciones	Contingencia Sistemas Información
Equipos de Telefonía IP	RC-17	Comunicaciones	Contingencia Sistemas Información
Enlaces de Cobre	RC-17	Comunicaciones	Contingencia Sistemas Información
Cableado de Red y Datos	RC-17	Comunicaciones	Contingencia Sistemas Información
SOFTWARE			
Software de Base de Datos (SQL Server, MySQL Server)	RC-12	Software	Contingencia Sistemas Información
	RC-14	Software	Contingencia Sistemas Información
Aplicativos usados por el PLAN COPESCO NACIONAL	RC-09	Información	Contingencia Sistemas Información
	RC-10	Información	Contingencia Sistemas Información
	RC-11	Software	Contingencia Sistemas Información
	RC-12	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información

Software Base (Sistemas Operativos y Ofimática)	RC-16	Software	Contingencia Sistemas Información
	RC-17	Comunicaciones	Contingencia Sistemas Información
	RC-12	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información
	RC-16	Software	Contingencia Sistemas Información
Antivirus para Servidores y Estaciones de Trabajo	RC-12	Software	Contingencia Sistemas Información
	RC-13	Software	Contingencia Sistemas Información
	RC-14	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información
	RC-16	Software	Contingencia Sistemas Información
INFORMACIÓN			
Base de Datos utilizadas por los aplicativos	RC-12	Software	Contingencia Sistemas Información
	RC-14	Software	Contingencia Sistemas Información
Respaldo de los aplicativos usados por PLAN COPESCO NACIONAL	RC-12	Software	Contingencia Sistemas Información
	RC-14	Software	Contingencia Sistemas Información
Respaldo de Base de Datos	RC-12	Software	Contingencia Sistemas Información
	RC-14	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información
Respaldos de Información y configuración de los servidores	RC-12	Software	Contingencia Sistemas Información
	RC-15	Software	Contingencia Sistemas Información
EQUIPOS DIVERSOS			
UPS	RC-04	Servicios Públicos	Contingencia Siniestros
Aire Acondicionado	RC-04	Servicios Públicos	Contingencia Siniestros
INFRAESTRUCTURA FÍSICA			
Oficinas: Sede Principal: Av. José Gálvez Barrenechea N° 290 Urbanización Corpac – San Isidro.	RC-01	Infraestructura	Contingencia Siniestros
	RC-02	Infraestructura	Contingencia Siniestros
	RC-03	Infraestructura	Contingencia Siniestros
	RC-04	Infraestructura	Contingencia Siniestros
	RC-05	Infraestructura	Contingencia Siniestros
	RC-25	Infraestructura	Contingencia Seguridad Física
Local Anexo: Calle 17 N° 525 Urbanización	RC-26	Infraestructura	Contingencia Seguridad Física

Córpac – San Isidro			
SERVICIOS PÚBLICOS			
Suministro de Energía Eléctrico	RC-04	Servicios Públicos	Contingencia Siniestros
Servicio de Telefonía Fija	RC-06	Servicios Públicos	Contingencia Siniestros
Servicio de Hosting	RC-07	Servicios Públicos	Contingencia Siniestros
Suministro de Agua	RC-05	Servicios Públicos	Contingencia Siniestros
RECURSOS HUMANOS			
Disponibilidad de Personal de Dirección	RC-21	Recursos Humanos	Contingencia Recursos Humanos
	RC-22	Recursos Humanos	Contingencia Recursos Humanos
	RC-25	Infraestructura	Contingencia Seguridad Física
	RC-26	Infraestructura	Contingencia Seguridad Física
	RC-20	Recursos Humanos	Contingencia Recursos Humanos
Disponibilidad Personal Operativo	RC-22	Recursos Humanos	Contingencia Recursos Humanos
	RC-25	Infraestructura	Contingencia Seguridad Física
	RC-26	Infraestructura	Contingencia Seguridad Física

3.- Elaboración del Plan de Contingencia

Flujo general que explica la forma de responder ante la ocurrencia de un evento de contingencia:



Flujo general

Cuadro N.° 8. Funcionarios responsables de cada evento de contingencia identificado:

SINIESTROS			
Código	Descripción del Evento de Contingencia	Responsables, Titulares o sus Representantes	Teléfonos
RC-01	Incendio	Coordinador del Área de Logística	(051) 4119500
RC-02	Sismo	Coordinador del Área de Logística	(051) 4119500
RC-03	Inundación por desperfectos de los servicios sanitarios	Coordinador del Área de Logística	(051) 4119500
RC-04	Interrupción de Energía Eléctrica	Coordinador del Área de Logística	(051) 4119500
RC-05	Falta de suministro de Agua	Coordinador del Área de Logística	(051) 4119500
RC-06	Interrupción de Servicios de Telefonía	Coordinadora del Área de Informática	(051) 4119500
RC-07	Interrupción de Servicios de Hosting	Coordinadora del Área de Informática	(051) 4119500
RC-08	Falla de UPS	Coordinadora del Área de Informática	(051) 4119500
SISTEMAS DE INFORMACIÓN			
Código	Descripción del Evento de Contingencia	Responsables, Titulares o sus Representantes	Teléfonos
RC-09	Extravió de Documentos	Coordinador del Área de Logística	(051) 4119500
RC-10	Sustracción o Robo de Información	Coordinador del Área de Informática	(051) 4119500
RC-11	Infección de Equipos por Virus	Coordinador del Área de Informática	(051) 4119500
RC-12	Perdida de los Sistemas Centrales	Coordinador del Área de Informática	(051) 4119500
RC-13	Perdida del Servicio de Correo	Coordinador del Área de Informática	(051) 4119500
RC-14	Falla del Motor de la Base de Datos	Coordinador del Área de Informática	(051) 4119500
RC-15	Falla del Sistema Operativo	Coordinador del Área de Informática	(051) 4119500
RC-16	Fallas en la red de Comunicaciones Internas	Coordinador del Área de Informática	(051) 4119500

RC-17	Caída en el servicio de Internet	Coordinador del Área de Informática	(051) 4119500
RC-18	Falla de Equipos Personales	Coordinador del Área de Informática	(051) 4119500
RC-19	Falla en los equipos multimedia, impresoras, scanner y otros	Coordinador del Área de Informática	(051) 4119500

RECURSOS HUMANOS			
Código	Descripción del Evento de Contingencia	Responsables, Titulares o sus Representantes	Teléfonos
RC-20	Ausencia imprevista del Personal de soporte Técnico	Coordinadora del Área de Informática	(051) 4119500
RC-21	Ausencia de Personal Ejecutivo para la toma de Decisiones ante situaciones de riesgo informático	Coordinadora del Área de Informática	(051) 4119500
RC-22	Falta de idoneidad del personal en la reserva de la información de la Base de Datos	Coordinadora del Área de Informática	(051) 4119500

SEGURIDAD FÍSICA			
Código	Descripción del Evento de Contingencia	Responsables, Titulares o sus Representantes	Teléfonos
RC-23	Sustracción de Equipos y Software Diversos	Coordinador del Área de Logística Coordinadora del Área de Informática	(051) 4119500
RC-24	Sabotaje	Coordinador del Área de Logística	(051) 4119500
RC-25	Vandalismo	Coordinador del Área de Logística	(051) 4119500
RC-26	Actos Terroristas	Coordinador del Área de Logística	(051) 4119500

8.2. Desarrollo de las Actividades

1.- Sub Factor: Contingencia Relacionada a Siniestros

El siguiente cuadro N.º 9, es un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Siniestros.

Cuadro N.º 9.

Código del Formato	Descripción del evento de Contingencia	Probabilidad Ocurrencia	Impacto	Calificación	Alerta
CONTINGENCIA RELACIONADAS A SINIESTROS					
INFRAESTRUCTURA					
RC-01	Incendio	0.04	4	0.16	
RC-02	Sismo	0.10	4	0.40	
RC-03	Inundación por desperfectos de los servicios sanitarios	0.02	1	0.02	
SERVICIOS PÚBLICOS					
RC-04	Interrupción de Energía Eléctrica	0.10	4	0.04	
RC-05	Falta de suministro de Agua	0.01	3	0.03	
RC-06	Interrupción de Servicios de Telefonía	0.01	3	0.03	
RC-07	Interrupción de Servicios de Internet	0.01	3	0.03	
EQUIPO					
RC-08	Falla del UPS	0.04	4	0.16	

RC-01	**EVENTO:** Incendio	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.
Este evento incluye los siguientes elementos mínimos identificados por el Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- Centro de Datos: Av. José Gálvez Barrenechea N.º 290, San Isidro - Lima
- Cuarto de comunicaciones: Calle 17 N° 525 Urb. Córpac, San Isidro - Lima

Recursos Humanos:

- Personal debidamente entrenado para afrontar el evento.

(b) Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de Plan COPESCO nacional sin exponer la seguridad de las personas.

(c) Criticidad

El Plan COPESCO Nacional determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones de la Sede Central y el Local Anexo.

(e) Personal Encargado

El Coordinador del Área de Logística, es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

(f) Coordinaciones de prevención de riesgo

Realizar inspecciones de seguridad periódicamente.

- Mantener las conexiones eléctricas seguras en el rango de su vida útil.

- Charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Acatar las indicaciones del INDECI, en torno al evento.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del Plan COPESCO Nacional responsable de las acciones de prevención y ejecución de la contingencia.

Igualmente se contará con los siguientes elementos para la detección y extinción de un posible incendio, los cuales cubrirán los ambientes del "Centro de Datos" y áreas afines a Informática de Plan COPESCO Nacional:

- Implementar detectores de humo en el "Centro de Datos".
- Considerar la Implementación de la Central de detección de incendios.
- Mantener actualizado los extintores.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

La contingencia se activará al ocurrir un evento que involucre fuego dentro de las instalaciones de Plan COPESCO nacional.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento

(b) Procesos relacionados antes del Evento.

- Identificar la ubicación de las estaciones manuales de alarma contra incendio.
- Identificar la ubicación de los extintores.
- Conocer el número de emergencia del Departamento de seguridad y Vigilancia del Plan COPESCO Nacional.
- Tener número de teléfono del personal responsable en seguridad Informática y contingencia de Plan COPESCO Nacional.
- Conocer el número de emergencia de los bomberos.

(c) Personal que autoriza la contingencia.

El Coordinador del Área de Logística puede activar la contingencia.

(d) Descripción de las actividades después de activar la contingencia.

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable del Plan COPESCO Nacional.
- Evacuar el área.
- En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata.

- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de Plan COPESCO Nacional en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectados.

(e) Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación es la unidad administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de Plan COPESCO Nacional.

(b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio

(c) Mecanismos de comprobación

El jefe de la unidad afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

(d) Mecanismos de Recuperación

Se efectuará de acuerdo a las instrucciones impartidas que se menciona en el punto **a.**

(e) Desactivación del Plan de Contingencia

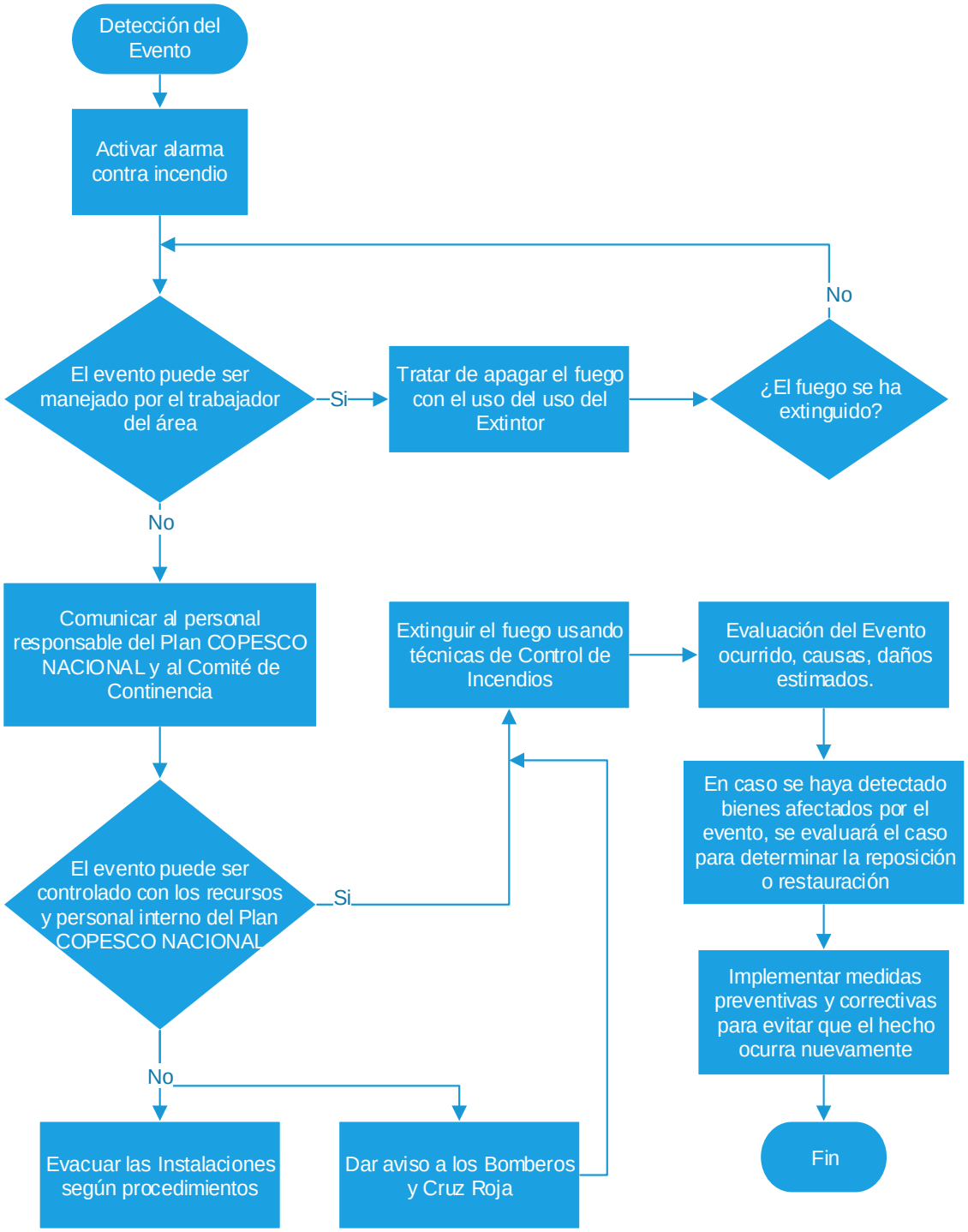
El Coordinador del Área de Logística, o su representante desactivarán el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

(f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Coordinador del Área de Logística luego de lo cual se determinará las acciones a tomar.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-01



RC-02	**EVENTO:** Sismo	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno.
Este evento incluye los siguientes elementos mínimos identificados por el Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Infraestructura:

- Sede Central: Av. José Gálvez Barrenechea N.º 290, San Isidro - Lima
- Local Anexo: Calle 17 N° 525 Urbanización Córpac – San Isidro

Recursos Humanos:

- Personal

(b) Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de Plan COPESCO Nacional sin exponer la seguridad de las personas.

(c) Criticidad

El Plan COPESCO Nacional determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones de la Sede Central y el Local Anexo.

(e) Personal Encargado

El Coordinador del Área de Logística, es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

(f) Coordinaciones de prevención de riesgo

- Contar con un plan de evacuación de las instalaciones del Plan COPESCO Nacional, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realizar simulacros de evacuación con la participación de todo el personal de la Sede Central y del Local Anexo.
- Mantener las salidas libres de obstáculos.

- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

El proceso de contingencia se activará inmediatamente después de ocurrir el evento

(b) Procesos relacionados antes del Evento.

- Tener la lista de los empleados por oficinas actualizadas.
- Mantenimiento del orden y limpieza.
- Inspecciones diarias de seguridad interna.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades

(c) Personal que autoriza la contingencia.

El Coordinador del Área de Logística puede activar la contingencia.

(d) Descripción de las actividades después de activar la contingencia.

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones del Coordinador del Área de Logística utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.
- Verificar que todo el personal de Plan COPESCO Nacional que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario. (ver procedimiento RC-25 en caso se presente una emergencia médica).
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.
- En todo momento se coordinará con personal de mantenimiento de Plan COPESCO Nacional, para las acciones que deban ser efectuadas por ellos.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección del Plan COPESCO Nacional en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

(e) Duración

Los procesos de evacuación del personal de Plan COPESCO Nacional serán calmados y demorará 5 minutos como máximo.
La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación es la Dirección Administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones del Plan COPESCO Nacional.

(b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio

(c) Mecanismos de comprobación

Director y/o Coordinador del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

(d) Mecanismos de Recuperación

Se efectuará de acuerdo a las instrucciones impartidas que se menciona en el punto **a.**

(e) Desactivación del Plan de Contingencia

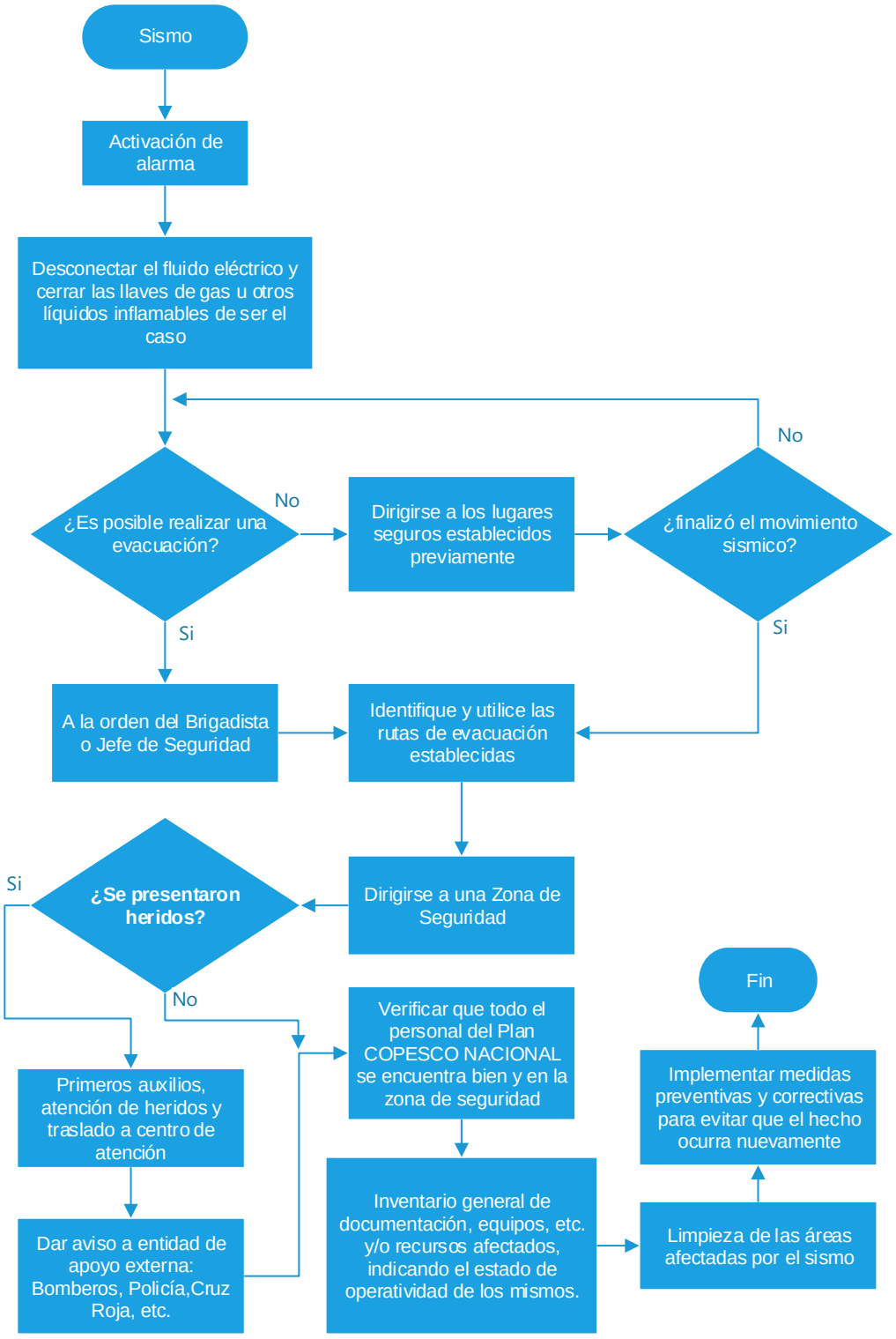
El Coordinador del Área de Logística o su representante desactivarán el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

(f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Coordinador del Área de Logística luego de lo cual se determinará las acciones a tomar.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-02



RC-04	**EVENTO:** Interrupción de Energía Eléctrica	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Falla general del suministro de energía eléctrica.

Este evento incluye los siguientes elementos mínimos identificados por el Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware:

- Servidores
- Estaciones de Trabajo

Equipos Diversos:

- UPS.

(b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

(c) Criticidad

Este evento de considera como CRITICO.

(d) Entorno

Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones del Plan COPESCO Nacional.

(e) Personal Encargado

El Coordinador del Área de Logística y/o Coordinador del Área de Informática de Plan COPESCO Nacional son responsables de realizar las coordinaciones necesarias para restablecer el fluido eléctrico.

(f) Coordinaciones de prevención de riesgo

- Durante las operaciones diarias del servicio u operaciones de Plan COPESCO Nacional se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.

- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Contar con UPS para proteger los servidores, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones de Plan COPESCO Nacional (puertas, contactos magnéticos, etc.)
- Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.
- Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

Corte de suministro de energía eléctrica en los ambientes del Plan COPESCO Nacional

(b) Procesos relacionados antes del Evento.

Cualquier actividad del servicio dentro de las instalaciones de Plan COPESCO Nacional.

(c) Personal que autoriza la contingencia.

El Coordinador del Área de Logística y/o Coordinador del Área de Informática pueden activar la contingencia.

(d) Descripción de las actividades después de activar la contingencia.

- Informar al Coordinador del Área de Logística y/o Coordinador del Área de Informática del problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas de Plan COPESCO Nacional y coordinar las acciones necesarias
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no el indicado anteriormente.
- En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción hasta que regrese el fluido eléctrico.
- Se debe verificar si la falla es general en la zona o solo en las instalaciones de Plan COPESCO Nacional.
- De detectarse que la falla solo corresponde a las instalaciones propias, se debe verificar si la falla es en los circuitos internos, de lo contrario se debe dar aviso a la Empresa Prestadora del Servicio de Energía Eléctrica para que en el menor tiempo proceda a corregir este problema.

(e) Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación es la Dirección Administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de Plan COPESCO Nacional.

(b) Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
Se informará a la Coordinación Ejecutora del Plan el problema presentado y el procedimiento usado para atender el problema.
En función a esto, se tomarán las medidas preventivas del caso.

(c) Mecanismos de comprobación

El jefe de la Unidad de Administración y/o Coordinador del Área de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

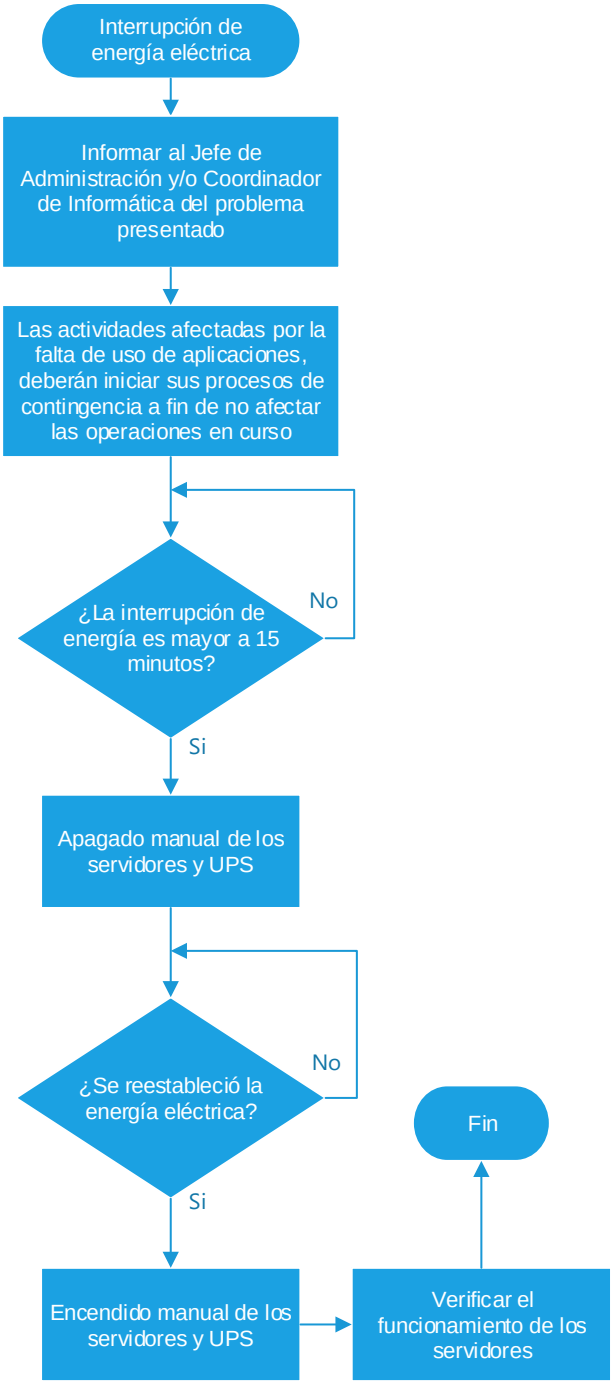
(d) Desactivación del Plan de Contingencia

El jefe de la Unidad de Administración y/o Coordinador del Área de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

(e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

DIAGRAMA DE EVENTO RC-04



RC-08	**EVENTO:** Falla del UPS	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Es un proceso de permanencia de autonomía ante caídas del servicio eléctrico del proveedor de servicio y/o Falla Eléctrica de los circuitos internos de la Entidad del Plan COPESCO Nacional.
Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- Centro de Datos: Av. José Gálvez Barrenechea N.º 290, San Isidro – Lima
- Cuarto de comunicaciones: Calle 17 N° 525 Urb. Córpac, San Isidro - Lima

Hardware:

- Servidores.
- Equipos de Internet
- Central Telefónica Asterisk.

(b) Objetivo

Establecer las acciones que se ejecutaran ante un apagado del Centro de Datos a fin de minimizar el tiempo de interrupción de las operaciones de Plan COPESCO Nacional sin exponer la seguridad de las personas.

(c) Criticidad

Plan COPESCO Nacional determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones del Centro de Datos de la Sede Central.

(e) Personal Encargado

Coordinador del Área de Informática del Plan COPESCO Nacional es el responsable en la supervisión del correcto funcionamiento del Centro de Datos.

(f) Coordinaciones de prevención de riesgo

Realizar inspecciones de seguridad periódicamente.

- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Charlas sobre el uso y manejo de Sistemas de Almacenamiento UPS.
- Contar con un Sistema de Almacenamiento que soporte toda la Carga del Centro de Datos de Plan COPESCO Nacional.
- Contar con un sistema de Almacenamiento de Contingencia que soporte toda la carga del Centro de Datos.
- Contar con una relación de teléfonos de emergencia que incluya a los responsables de las acciones de prevención y ejecución de la contingencia.
- Implementar detectores de falta de Energía en el "Centro de Datos".

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

La contingencia se activará al ocurrir un evento
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

(b) Procesos relacionados antes del Evento.

- Identificar la ubicación de los manuales de manejo de UPS.
- Identificar la ubicación de las Baterías de respaldo en caso de fallas de batería.
- Conocer el sistema de encendido manual del UPS de contingencia.

(c) Personal que autoriza la contingencia.

Coordinadora del Área de Informática puede activar la contingencia.

(d) Descripción de las actividades después de activar la contingencia.

- Tratar de encender manualmente el UPS de Contingencia en caso de Falla del encendido automático.
- Comunicar al personal responsable de Plan COPESCO Nacional.
- En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de finalizada la contingencia, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados a los equipos.
- En caso de daños de algún Servidor prestar asistencia técnica inmediata
- En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.

(e) Duración

La duración de la contingencia dependerá del tiempo que demande controlar la Falla del Sistema de Almacenamiento de Energía - UPS.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El Coordinador del Área de Informática de Plan COPESCO Nacional, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los directores y/o jefes de unidades para la reanudación de los trabajos operativos con las aplicaciones de Plan COPESCO Nacional.

(b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio

(c) Mecanismos de comprobación

El jefe de Unidad afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones han sido afectadas y cuáles son las acciones tomadas.

(d) Mecanismos de Recuperación

Se efectuará de acuerdo a las instrucciones impartidas que se menciona en el punto **a.**

(e) Desactivación del Plan de Contingencia

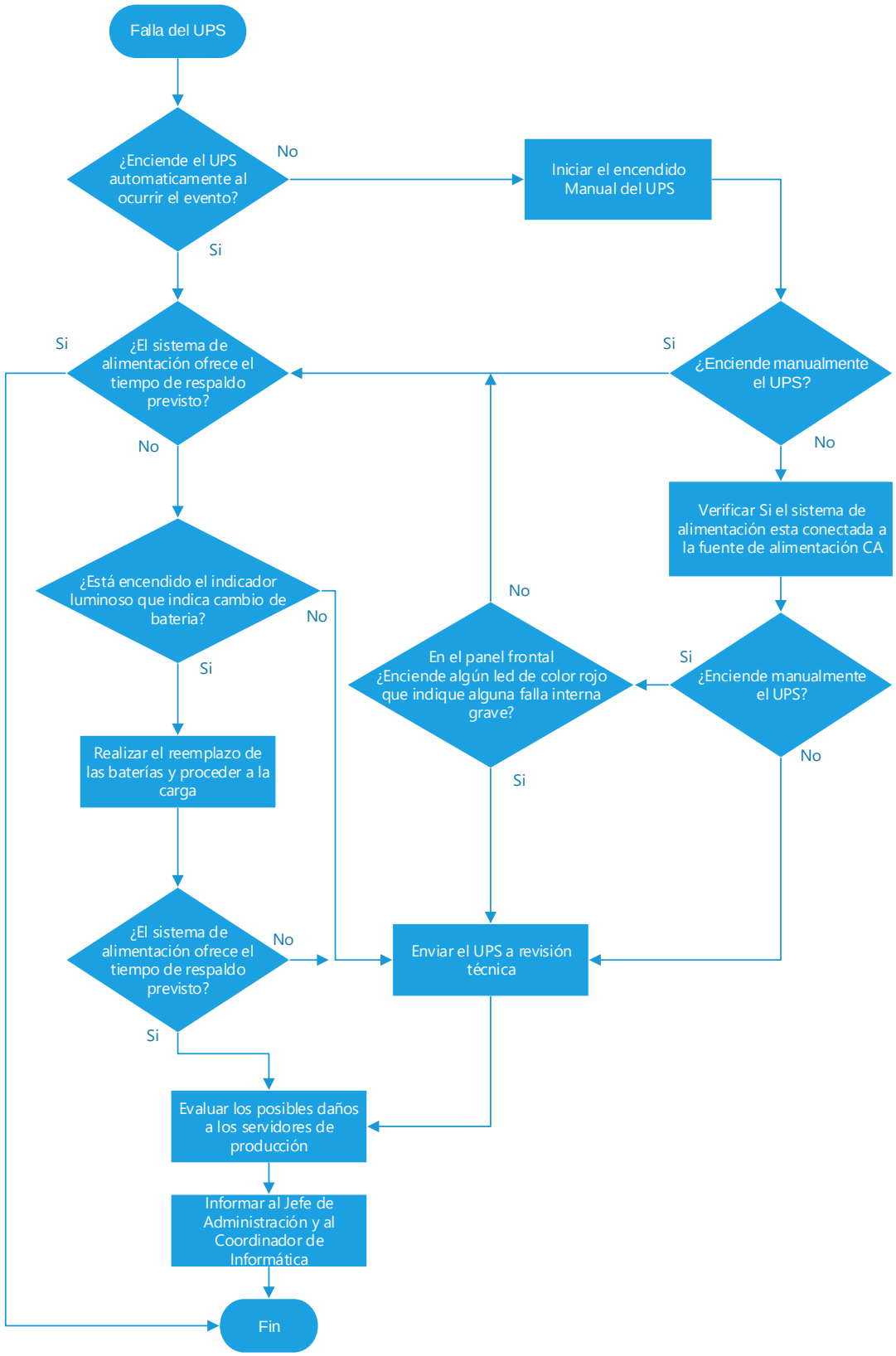
El jefe de Administración o sus representantes desactivarán el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

(f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el jefe de Administración luego de lo cual se determinará las acciones a tomar.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-08



2.- Sub Factor: Contingencias relacionadas a los sistemas de información.

El siguiente cuadro N.º 10, es un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Siniestros.

Cuadro N.º 10.

Código del Formato	Descripción del evento de Contingencia	Probabilidad Ocurrencia	Impacto	Calificación	Alerta
CONTINGENCIA RELACIONADAS A SISTEMAS DE INFORMACIÓN					
INFORMACIÓN					
RC-09	Extravió de Documentos	0.02	3	0.06	
RC-10	Sustracción o Robo de información	0.02	3	0.06	
SOFTWARE					
RC-11	Infección de Equipos por Virus	0.05	4	0.20	
RC-12	Perdida de los sistemas Centrales	0.05	4	0.20	
RC-13	Perdida del Servicio de Correo	0.01	2	0.02	
RC-14	Falla del Motor de Base de Datos	0.04	4	0.16	
RC-15	Falla del sistema Operativo	0.04	4	0.16	
COMUNICACIONES					
RC-16	Fallas en la Comunicación de Red Interna	0.02	4	0.08	
RC-17	Caída en el servicio de Internet	0.04	4	0.16	
HARDWARE					
RC-18	Fallas en los Equipos Personales	0.02	2	0.04	
RECURSOS OPERATIVOS Y LOGÍSTICOS					
RC-08	Falla del UPS	0.01	2	0.02	

RC-11	**EVENTO:** Infección de Equipos por Virus	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo. Además, un virus informático puede dañar o eliminar los datos de un equipo.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Hardware:
- Servidores
- Estaciones de Trabajo

Software:
- Software Base.
- Aplicativos usados por el Plan COPESCO Nacional.

(b) Objetivo

Restaurar la operatividad de los equipos después de eliminar los virus o reinstalar las aplicaciones dañadas.

(c) Criticidad

El nivel de este evento es considerado CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones de la Sede Central y el Local Anexo.

(e) Personal Encargado

La Coordinadora del Área de Informática de Plan COPESCO Nacional es responsable en la supervisión del correcto funcionamiento de las estaciones PC´s

(f) Coordinaciones de prevención de riesgo

- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación de quemadores de CD, etc. en estaciones de trabajo que no lo requieran.

- Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

(b) Procesos relacionados antes del Evento.

- Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

(c) Personal que autoriza la contingencia.

- Coordinadora del Área de Informática.
- Analista en Tecnologías de Información.

(d) Descripción de las actividades después de activar la contingencia.

- Informar a la Coordinadora del Área de Informática del problema presentado.
- Desconectar la estación infectada de la red de Plan COPESCO Nacional.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.).
- Eliminar el agente causante de la infección.
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema:
  - Formatear el equipo
  - Personalizar la estación para el usuario
- Conectar la estación a la red de Plan COPESCO Nacional.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

(e) Duración

La duración del evento no deberá ser mayor a DOS HORAS en caso se confirme la presencia de un virus. Esperar la indicación del personal de soporte para reanudar el trabajo.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El Analista en Tecnologías de Información, luego de restaurar el correcto funcionamiento de la estación de trabajo (PC), coordinará con el usuario responsable y/o jefe del área para reanudar las labores de trabajo con el equipo.

(b) Descripción

Se informará al Coordinador del Área de Informática el tipo de virus encontrado y el procedimiento usado para removerlo.
En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal de Plan COPESCO Nacional.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

(c) Mecanismos de comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la Coordinación Ejecutora del Plan para su revisión.

(d) Desactivación del Plan de Contingencia

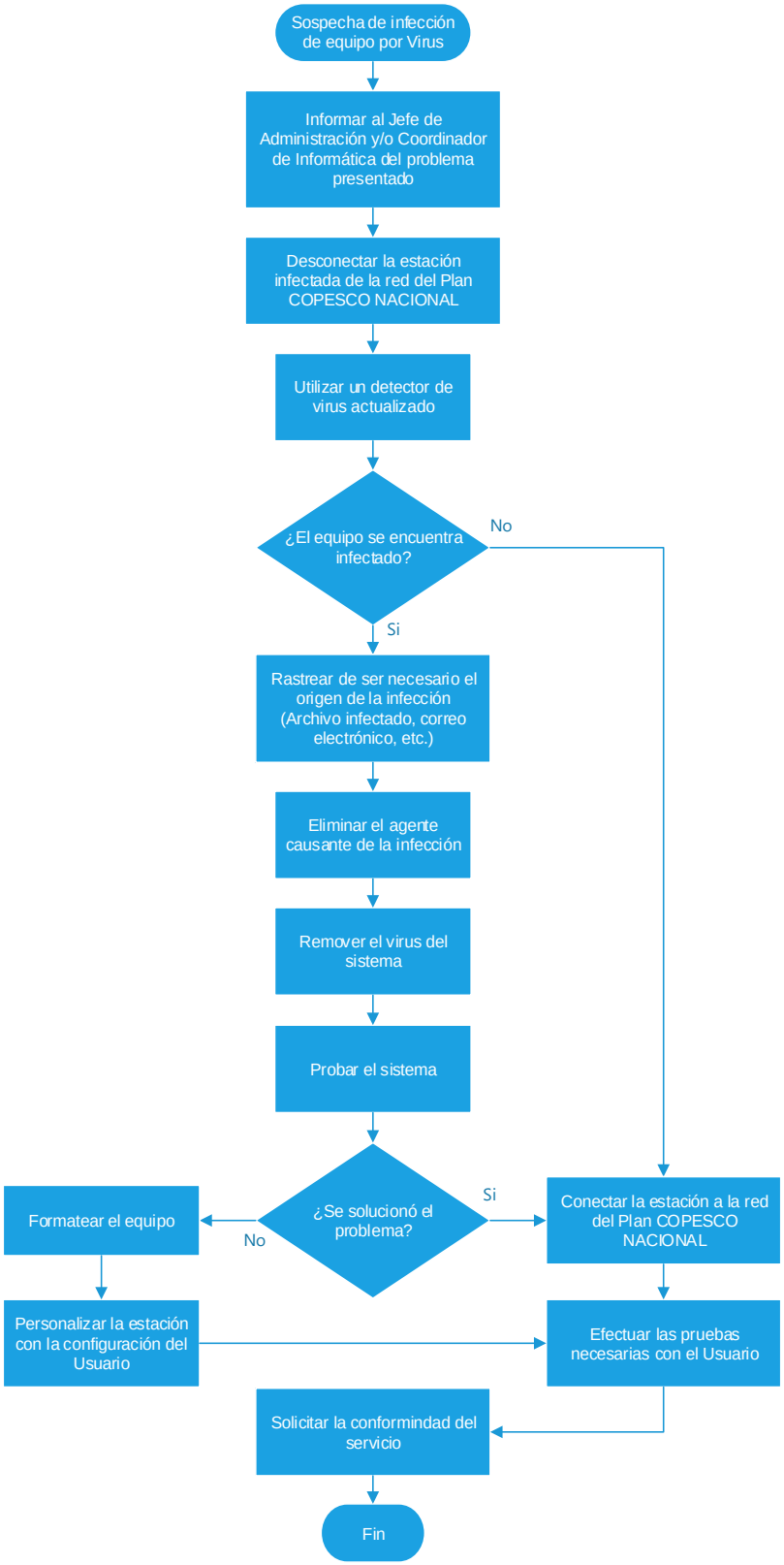
Con el aviso del Analista en Tecnologías de Información, se desactivará el presente Plan.

(e) Proceso de Actualización

El problema de infección presentado en la estación de trabajo, no debe detener la Aplicación de actualización de datos en las Aplicaciones de Plan COPESCO Nacional.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-11



RC-12	**EVENTO:** Pérdida de los Sistemas Centrales	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Falla en el control de computadoras, en el interfaz hombre-máquina, recursos de hardware y software de Plan COPESCO Nacional.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Hardware:
- Servidores

Software:
- Aplicativos usados por Plan COPESCO Nacional (SIAF-SP, SIGA, SISTEMA 10, Sistema de Gestión de Proyectos – Obras "SGPO").

Información:
- Respaldo de Base de Datos
- Respaldo de las Aplicaciones utilizadas por el Plan COPESCO Nacional.

(b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar las funciones de los elementos identificados.

(c) Criticidad

El nivel de este evento es considerado CRITICO.

(d) Entorno

Se puede producir durante la operatividad, afectando a las estaciones de trabajo y/o servidores de aplicaciones usados para dar soporte a las operaciones.

(e) Personal Encargado

La Coordinadora del Área de Informática del Plan COPESCO Nacional es responsable de coordinar las acciones necesarias para asegurar el correcto funcionamiento de las aplicaciones.

(f) Coordinaciones de prevención de riesgo

Se debe asegurar de cubrir los siguientes aspectos:

- Contar con los backup diarios de datos de las aplicaciones en producción en la institución se encuentren directamente alojados en los servidores de Plan COPESCO Nacional o alojados en el servicio de hosting contratado por la entidad: Copias de Respaldo.
- Contar con servicios de soporte vigentes para los principales causantes del evento:
- El Plan COPESCO Nacional debe asegurarse de mantener acuerdos con sus proveedores de servicio.
- Revisión periódica de los logs de actividad de los servidores para prevenir su mal funcionamiento.
- Estaciones de trabajo y servidores deberán contar con antivirus actualizados.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Falla de Acceso a Aplicaciones.
- Mensaje Pérdida de Conexión al BD.

(b) Procesos relacionados antes del Evento.

- Cualquier proceso relacionado con el uso de las aplicaciones en los servidores de Plan COPESCO Nacional.

(c) Personal que autoriza la contingencia.

- La Coordinadora del Área de Informática.

(d) Descripción de las actividades después de activar la contingencia.

- Informar a la Coordinadora del Área de Informática del problema presentado.
- Verificar si el equipo se encuentra con un problema de Hardware y/o Software.
- Rastrear de ser necesario el origen del problema.
- Eliminar el agente causante
- Remover pieza averiada en caso de ser tipo HotSwap
- Recuperar última versión estable del sistema.
- Probar el sistema.
- En caso no solucionarse el problema:
  - Generar Backup Offline
  - Formatear equipo.
  - Reinstalar Sistema.
- Conectar el sistema a la red de Plan COPESCO Nacional.
- Efectuar las pruebas necesarias.
- Solicitar conformidad del servicio.
- En caso de no recuperar el sistema remitirse a los planes de recuperación del sistema.

(e) Duración

La duración del evento estará en función de la complejidad del problema encontrado. Esperar la indicación del Coordinador del Área de Informática de Plan COPESCO Nacional para reanudar la operación normal con las aplicaciones.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

La Coordinadora del Área de Informática, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los directores y/o jefes de áreas para la reanudación de los trabajos operativos con las aplicaciones de Plan COPESCO Nacional.

(b) Descripción

Se informará a la Alta Dirección la causa que motivó la paralización del servicio.
En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

(c) Mecanismos de comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

(d) Desactivación del Plan de Contingencia

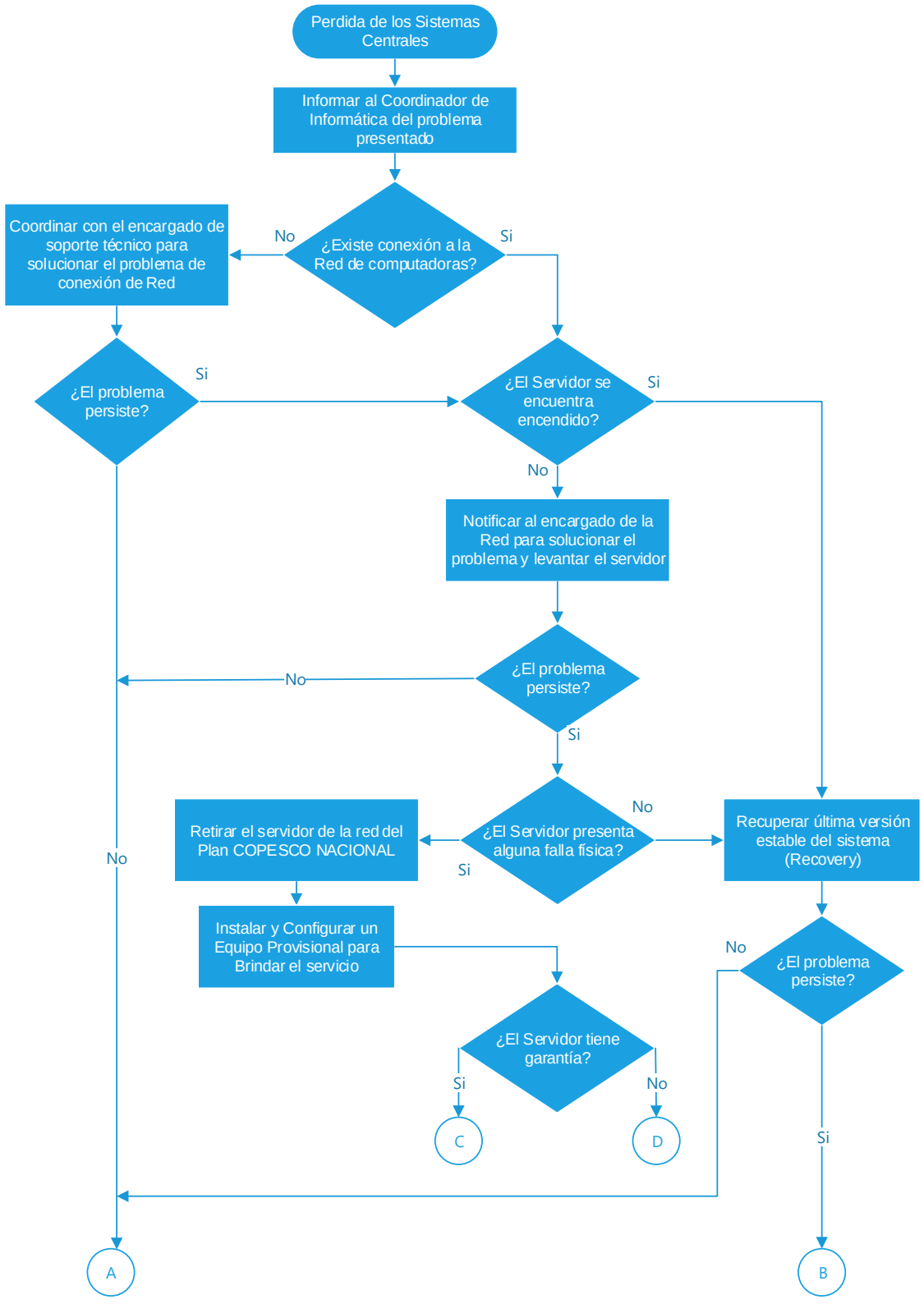
Con el aviso de la Coordinadora del Área de Informática del Plan COPESCO Nacional, se desactivará el presente plan.

(e) Proceso de Actualización

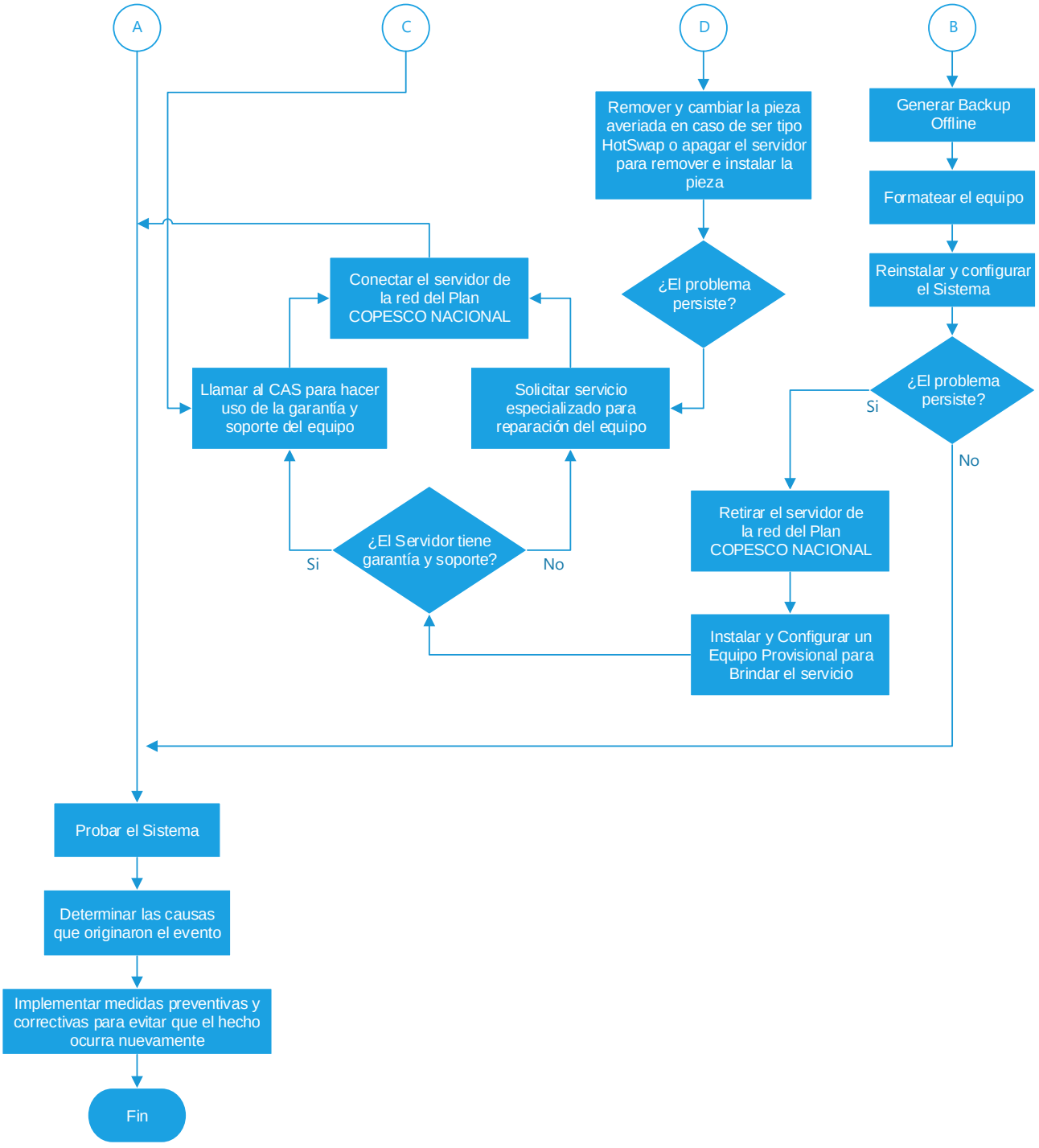
En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o jefes de áreas, para iniciar las labores de actualización de los sistemas.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-12



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"



RC-14	**EVENTO:** Falla en Motor de Base de Datos	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Ausencia del servicio principal para almacenar, procesar y proteger los datos, para acceso controlado y procesamiento de transacciones rápidos para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de Plan COPESCO Nacional.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Hardware:
- Servidores

Software:
- Aplicativos usados por el Plan COPESCO Nacional.

Información:
- Respaldo de Base de Datos
- Respaldo de Software Base.

(b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar los datos de las aplicaciones ejecutadas en los servidores centrales.

(c) Criticidad

El nivel de este evento es considerado CRITICO.

(d) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del Plan COPESCO Nacional.

(e) Personal Encargado

La Coordinadora del Área de Informática realizará las acciones correspondientes.

(f) Coordinaciones de prevención de riesgo

- Revisión periódica de los log's de la BD para prevenir mal funcionamiento de la Base de Datos.

- Contar con los backups diarios de datos de las aplicaciones en producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de datos.
- La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso**:** Copias de Respaldo.
- Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante del producto.
- Contar con servicios de soporte vigentes para el software de gestión de BD. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

(b) Procesos relacionados antes del Evento.

- Respaldo disponible para el uso de las aplicaciones en los servidores de Plan COPESCO Nacional

(c) Personal que autoriza la contingencia.

- Coordinadora del Área de Informática.

(d) Descripción de las actividades después de activar la contingencia.

- Sistemas de Proveedores. - De producirse una falla al momento de la operación de estos sistemas por efecto del programa ejecutable (cliente) o base de datos, deberá ser comunicado y coordinado inmediatamente con el proveedor, para su corrección.

- Sistemas Desarrollados por Plan COPESCO Nacional. - De producirse una falla al momento de la operación de estos sistemas, el Coordinador del Área de Informática asumirá, delegará o coordinará los trabajos de corrección o modificación.

(e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las CUATRO horas.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones de Plan COPESCO Nacional es el Coordinador del Área de Informática.

(b) Descripción

Se informará al Coordinador del Área de Informática de Plan COPESCO Nacional la causa del problema presentado y el procedimiento usado para atender el problema.
En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal del Plan COPESCO Nacional.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

(c) Mecanismos de comprobación

La Coordinadora del Área de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

(d) Desactivación del Plan de Contingencia

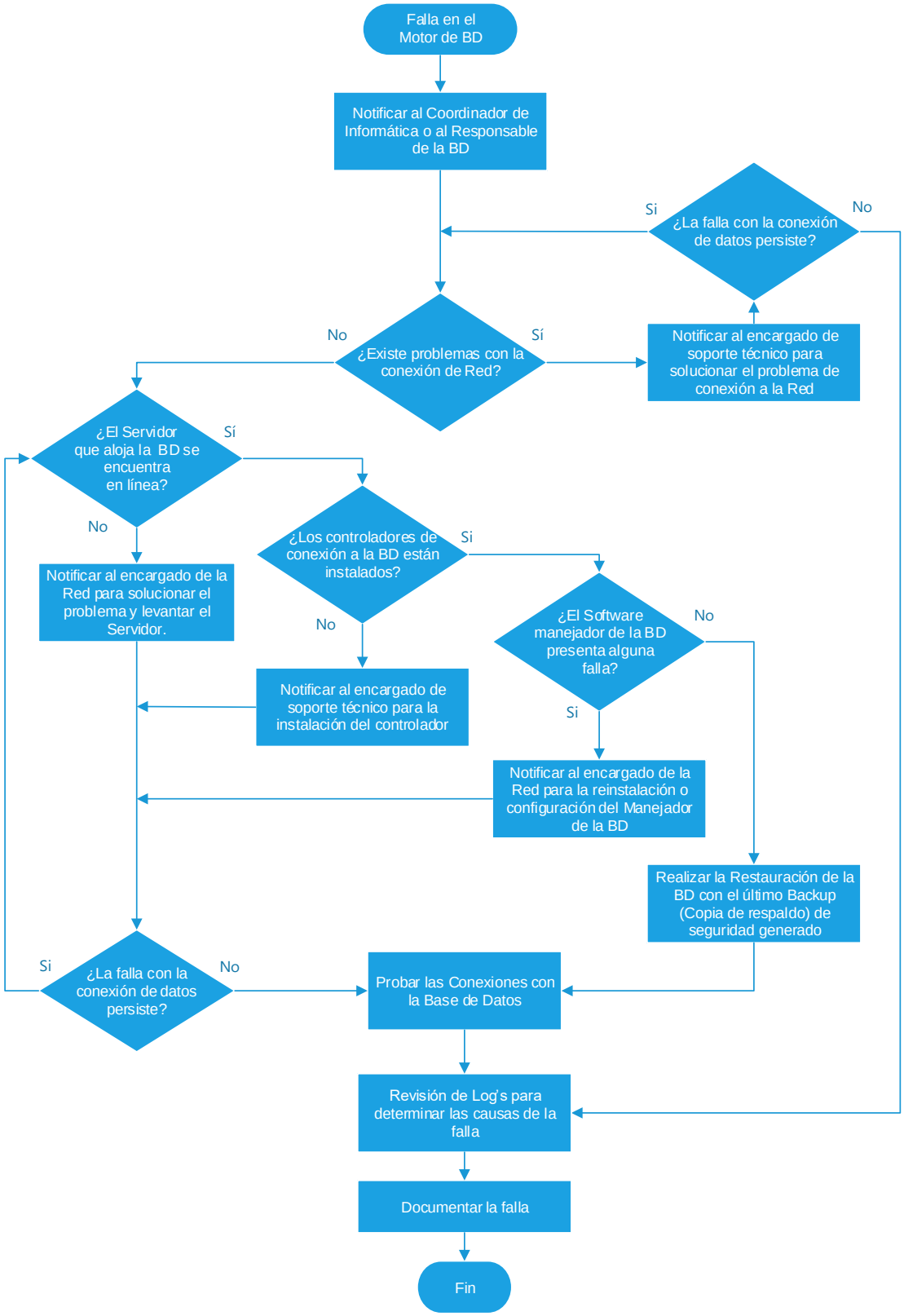
La Coordinadora del Área de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con la BD de las aplicaciones.

(e) Proceso de Actualización

En base al informe presentado que identifica las causas de la pérdida del sistema operativo en las estaciones de trabajo y/o servidores, se determinará las acciones de preventivas necesarias que deberán incluirse en el presente plan.
En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o jefes de áreas, para iniciar las labores de actualización de los sistemas.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-14



RC-15	**EVENTO:** Falla del Sistema Operativo	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Falla en el control de computadoras, en el interfaz hombre-máquina, recursos hardware y software de Plan COPESCO Nacional.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Hardware:

- Servidores

Software:

- Aplicativos usados por el Plan COPESCO Nacional.

Información:

- Respaldo de Base de Datos
- Respaldo de los Aplicativos por Plan COPESCO Nacional.

(b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar las funciones de los elementos identificados.

(c) Criticidad

El nivel de este evento es considerado CRITICO.

(d) Entorno

Se puede producir durante la operatividad, afectando a las estaciones de trabajo y/o servidores de aplicaciones usados para dar soporte a las operaciones.

(e) Personal Encargado

La Coordinadora del Área de Informática es responsable de coordinar las acciones necesarias para asegurar el correcto funcionamiento de las aplicaciones.

(f) Coordinaciones de prevención de riesgo

- Contar con los backups diarios de datos de las aplicaciones en producción en la institución.

- Contar con servicios de soporte vigentes para los principales causantes del evento:
  - El Plan COPESCO Nacional debe asegurarse de mantener acuerdos con sus Proveedores de Servicio.
- Revisión periódica de los log's de actividad de los servidores para prevenir su mal funcionamiento.
- Estaciones de trabajo y servidores deberán contar con antivirus actualizados.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Detención de las funciones de trabajo en estaciones de trabajo y/o servidores de aplicaciones.
- Identificación de falla en el monitor de los servidores de aplicaciones y/o estaciones de trabajo.

(b) Procesos relacionados antes del Evento.

- Respaldo disponible de los sistemas operativos para la ejecución de las aplicaciones en los servidores.

(c) Personal que autoriza la contingencia.

- Coordinadora del Área de Informática.

(d) Descripción de las actividades después de activar la contingencia.

En el caso de las estaciones de trabajo:

- Proceder a la revisión de la estación de trabajo para determinar la causa de la falla.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema:
  - Formatear el equipo
  - Personalizar la estación para el usuario
  - Conectar la estación a la red del Archivo.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

En el caso de los servidores de aplicaciones:

- Direcciones y/o Jefaturas:
  - Reportar el problema al área de informática.
  - Coordinar las acciones a realizarse y el tiempo aproximado de interrupción del servicio.
  - Comunicar a los directores y/o jefes de áreas para que se tomen las acciones del caso y no se afecte en sus operaciones.

(e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las CINCO horas.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones de Plan COPESCO Nacional es el Coordinador del Área de Informática.

(b) Descripción

Se informará a la Coordinadora del Área de Informática la causa del problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal del Plan COPESCO Nacional.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

(c) Mecanismos de comprobación

La Coordinadora del Área de Informática presentará un informe a la Coordinación Ejecutora del Plan, explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

(d) Desactivación del Plan de Contingencia

La Coordinadora del Área de Informática de Plan COPESCO Nacional desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

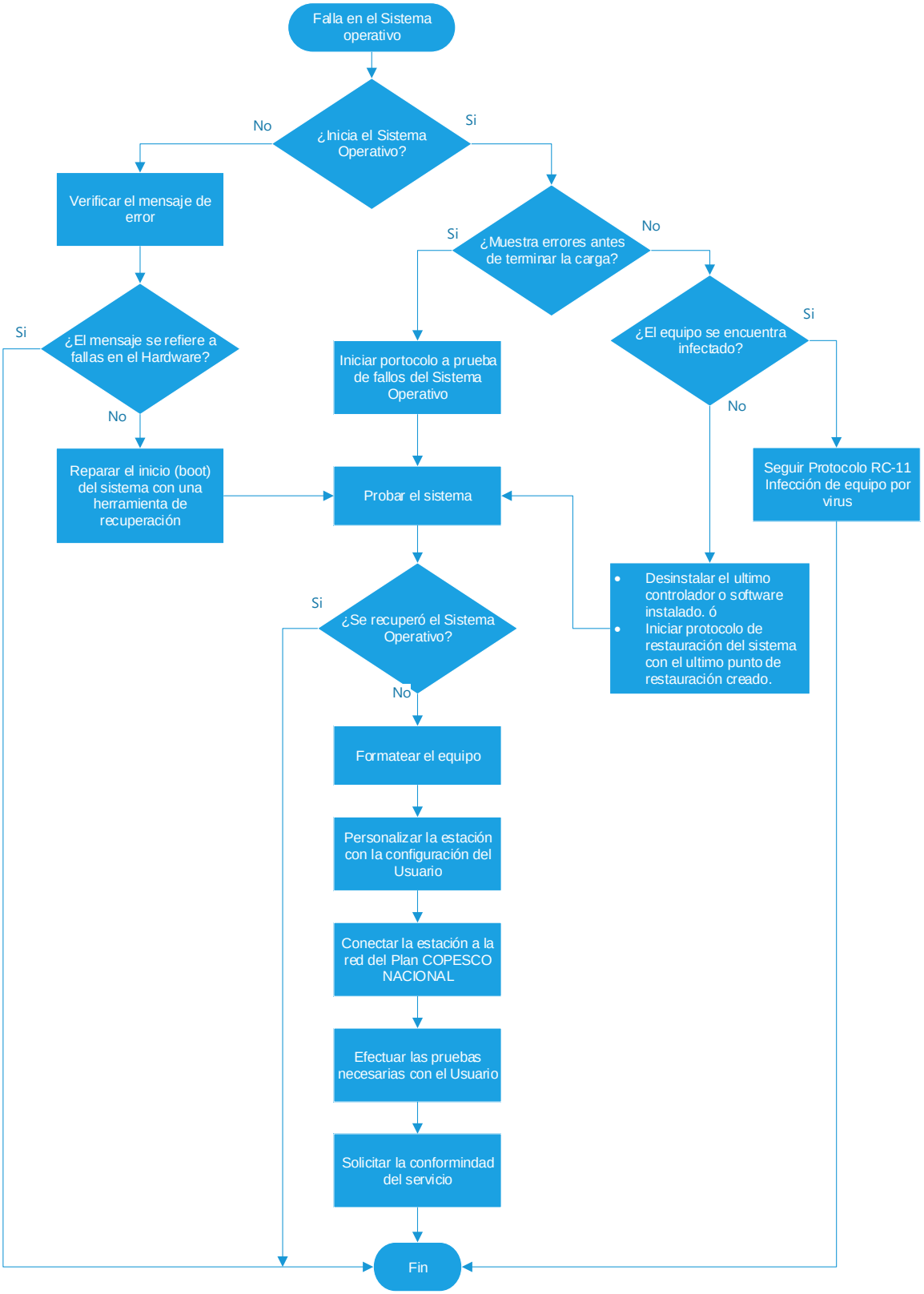
(e) Proceso de Actualización

En base al informe presentado que identifica las causas de la pérdida del sistema operativo en las estaciones de trabajo y/o servidores, se determinará las acciones de prevención a tomar.

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o jefes de áreas, para iniciar las labores de actualización de los sistemas.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-15



RC-17	EVENTO: Caída en el servicio de Internet	Versión: 3.0
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Caída en el servicio de Internet de Plan COPESCO Nacional.

Este evento incluye los siguientes elementos mínimos identificados por el Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Hardware:
- Servidores
- Computadoras Personales

Software:
- Servicio de Internet
- Suspensión de los servicios de correo y de los aplicativos críticos de la entidad.

(b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar las funciones de los elementos identificados.

(c) Criticidad

El nivel de este evento es considerado CRITICO.

(d) Entorno

Se puede producir durante la operatividad, afectando a las estaciones de trabajo y/o servidores de aplicaciones usados para dar soporte a las operaciones.

(e) Personal Encargado

La Coordinadora del Área de Informática es responsable de coordinar las acciones necesarias para asegurar el correcto funcionamiento del servicio.

(f) Coordinaciones de prevención de riesgo

Se debe asegurar de cubrir los siguientes aspectos:

- Contar con un enlace secundario de contingencia.
- El Plan COPESCO Nacional debe asegurarse de mantener acuerdos con sus Proveedores de Servicio.
- Revisión periódica del servicio de Internet a fin de mitigar caídas.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Falta de acceso a Internet
- Falta de acceso a sistemas y/o aplicativos.

(b) Procesos relacionados antes del Evento.

- Cualquier proceso relacionado con el uso de las aplicaciones en los servidores de Plan COPESCO Nacional.

(c) Personal que autoriza la contingencia.

- Coordinadora del Área de Informática.

(d) Descripción de las actividades después de activar la contingencia.

- Proceder a la revisión de acceso a los equipos de Internet para determinar la causa de la falla.
- Verificar si los equipos se encuentran apagados.
- Reiniciar los equipos del servicio.
- Probar el sistema.
- En caso no solucionarse el problema: Llamar al proveedor que brinda el servicio de internet.
- Efectuar las pruebas necesarias.

(e) Duración

La duración del evento estará en función de la complejidad del problema encontrado. Esperar la indicación del Coordinador del Área de Informática de Plan COPESCO Nacional para reanudar la operación normal con las aplicaciones.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El Coordinador del Área de Informática de Plan COPESCO Nacional, luego de verificar la corrección del problema de acceso a INTERNET, coordinará con los jefes de unidad y/o coordinadores de áreas para la reanudación de los trabajos operativos con las aplicaciones de Plan COPESCO Nacional.

(b) Descripción

Se informará a la Alta Dirección la causa que motivó la paralización del servicio Internet. En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

(c) Mecanismos de comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

(d) Desactivación del Plan de Contingencia

Con el aviso del Coordinador del Área de Informática del Plan COPESCO Nacional, se desactivará el presente plan.

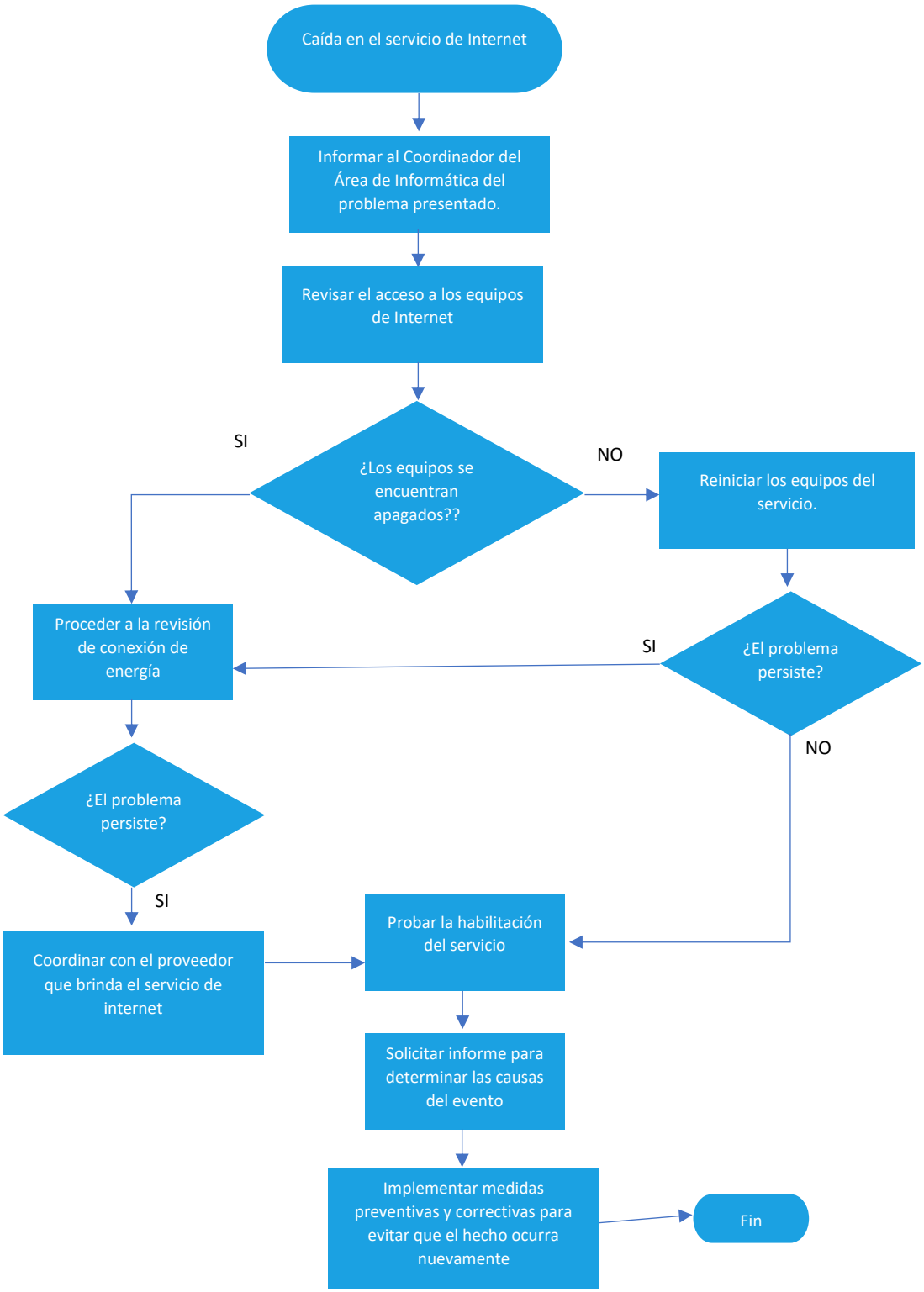
(e) Proceso de Actualización

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o jefes de áreas, para iniciar las labores de actualización de los sistemas.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

DIAGRAMA DE EVENTO RC-17

CAÍDA EN EL SERVICIO DE INTERNET
(PROCEDIMIENTO DE CONEXIÓN 01)



3.- Sub Factor: Contingencia Relacionada a los Recursos Humanos

A continuación, en el cuadro N.º 12 se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Recursos Humanos que se describirán en detalle más adelante:

Cuadro N.º 12.

Código del Formato	Descripción del evento de Contingencia	Probabilidad Ocurrencia	Impacto	Calificación	Alerta
CONTINGENCIA RELACIONADAS A RECURSOS HUMANOS					
RECURSOS HUMANOS					
RC-20	Ausencia imprevista del personal técnico	0.05	3	0.15	
RC-21	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático.	0.05	3	0.15	
RC-22	Falta de idoneidad del personal en la reserva de la información de la Base de Datos.	0.01	4	0.04	

RC-20	**EVENTO:** Ausencia imprevista del personal de soporte técnico	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Ausencias del personal de soporte técnico relevante (enfermedad, renuncias, ceses), en toma decisiones claves que garantice el normal funcionamiento de servidores y redes de la institución.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Recursos Humanos:

- Personal

(b) Objetivo

Asegurar la continuidad del servicio informático de Plan COPESCO Nacional.

(c) Criticidad

El Plan COPESCO Nacional determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones de la Sede Central y el Local Anexo.

(e) Personal Encargado

La Coordinadora del Área de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

(f) Coordinaciones de prevención de riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales, por lo que se considera lo siguiente:

- Como primera prevención, la Coordinadora del Área de Informática, se asegurará en capacitar al personal del área de informática con el fin que cumpla el perfil, conocimiento y capacidad para reemplazar la ausencia ante la presencia de este evento.
- Como segunda prevención, la Coordinadora del Área de Informática se asegurará en tener como mínimo a dos profesionales.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labores.
- Para el control del personal se cuenta con un software de control de asistencia, de donde se proveerá información al Coordinador del Área de Informática, para que tome las acciones preventivas correspondiente.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Reporte de inasistencia del personal de soporte técnico, etc.
- El proceso de contingencia se activa durante las DOS (02) HORAS iniciales del día.

(b) Procesos relacionados antes del Evento.

Se podría dar por:

- Conocimiento de la Coordinadora del Área de Informática por parte del reporte de inasistencia del Sistema de Control de Asistencia.
- Conocimiento de la Coordinadora del Área de Informática por comunicación telefónica por parte del personal de soporte técnico ausente o algún familiar.

(c) Personal que autoriza la contingencia.

- Coordinadora del Área de Informática.

(d) Descripción de las actividades después de activar la contingencia.

- Confirmada la inasistencia del personal técnico, la Coordinadora del Área de Informática asignará la responsabilidad a un profesional del área capacitado para reemplazar en las funciones que el personal poseía.
- De ser permanente, la Coordinadora del Área de Informática solicitará al jefe de la Unidad de Administración de Plan COPESCO Nacional, el reemplazo del personal.
- En el caso que la inasistencia sea de la Coordinadora del Área de Informática, las funciones temporales serán asumidas por un profesional del área de informática, el cual deberá ser designado por el jefe de Administración.
- En el caso supuesto que no existan profesionales del área que asuman las funciones del personal existente, se notificará al director ejecutivo de Plan COPESCO Nacional para las acciones correspondientes.
- De ser permanente la inasistencia de la Coordinador del Área de Informática, será el jefe de Administración quien notifique y solicite al director ejecutivo de Plan COPESCO Nacional, el reemplazo del personal.

(e) Duración

Máximo OCHO (08) horas. El fin del presente evento es la presencia del reemplazo que asume la responsabilidad; hasta que se confirme la presencia del personal de soporte técnico en caso de renuncia u otras por fuerza mayor.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación es la Coordinadora del Área de Informática, cuyo rol principal es asegurar el normal funcionamiento del servicio informático.

(b) Descripción

- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

(c) Mecanismos de comprobación

La Coordinadora del Área de Informática presentará un informe a la Coordinación Ejecutora del Plan, explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

(d) Desactivación del Plan de Contingencia

La Coordinadora del Área de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

(e) Proceso de Actualización

En base al informe presentado por la Coordinadora del Área de Informática y las causas identificadas en el servicio informático se determinará las acciones a tomar

RC-22	**EVENTO:** Ausencia imprevista del personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático.	**Versión: 3.0**
	ENTIDAD RESPONSABLE: Plan COPESCO Nacional	**ENTIDAD INVOLUCRADA:** Plan COPESCO Nacional

1.- PLAN DE PREVENCIÓN

(a) Descripción del Evento

Ausencias del personal de Dirección y/o jefaturas (enfermedad, renuncias, ceses), en toma decisiones claves que garantice el normal funcionamiento de las actividades.

Este evento incluye los siguientes elementos mínimos identificados por Plan COPESCO Nacional, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Recursos Humanos:

- Personal

(b) Objetivo

Asegurar la continuidad de las operaciones en las diferentes direcciones y/o jefaturas de Plan COPESCO Nacional, evitando el quiebre en la cadena de mandos, a través de reemplazos de personal ejecutivos.

(c) Criticidad

El Plan COPESCO Nacional determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

(d) Entorno

Este evento se puede dar en las instalaciones de la Sede Central y el Local Anexo.

(e) Personal Encargado

La Coordinadora del Área de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

(f) Coordinaciones de prevención de riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales que se presente a personal de Dirección y/o Jefatura, por lo que se considera lo siguiente:

- Como primera prevención, la Alta Dirección asegurará en capacitar a un empleado con más de 5 años de experiencia en la Institución que cumpla el perfil, conocimiento y capacidad para reemplazar ante el evento.

- Incluir como parte de las funciones del personal en comunicar anticipadamente la inasistencia a su centro de labores, siempre y cuando se trate de ocasiones premeditadas.

2.- PLAN DE EJECUCIÓN

(a) Eventos que activan la Contingencia

- Reporte de inasistencia de algún director y/o jefe de Unidad.

- El proceso de contingencia se activa durante las DOS HORAS iniciales del día.

(b) Procesos relacionados antes del Evento.

Se podría dar por:

- Falta de decisión del director y/o jefe de Unidad para aplicar soluciones ante algún inconveniente en las actividades u operaciones de su competencia, donde se detecte la ausencia.

- Reporte de Control de Asistencia referente a inasistencias.

(c) Personal que autoriza la contingencia.

- El encargado de autorizar el proceso de contingencia es el director Administrativo.

(d) Descripción de las actividades después de activar la contingencia.

- Confirmado la inasistencia del director ejecutivo, se coordinará el reemplazo temporal con los jefes de línea del Plan Contingencia Nacional.

- Confirmado la inasistencia de un jefe de unidad, el director ejecutivo designará la encargatura temporal del área a uno de los coordinadores de área de Plan COPESCO Nacional.

(e) Duración

Máximo tres horas. El fin del presente evento es la presencia del reemplazo, o el empleado más antiguo que esté capacitado para que asuma la responsabilidad; hasta que se confirme la presencia del director y/o jefe de unidad o nuevo director y/o jefe de unidad en caso de renuncia u otras por fuerza mayor.

3.- PLAN DE RECUPERACIÓN

(a) Personal Encargado

El personal encargado del Plan de Recuperación es la Coordinadora del Área de Informática, cuyo rol principal es asegurar el normal funcionamiento del Servicio Informático.

(b) Descripción

- Regularización en las coordinaciones pendiente durante la ausencia.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

(c) Mecanismos de comprobación

La Coordinadora del Área de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operaciones ha sido afectado y cual son las acciones tomadas.

(d) Desactivación del Plan de Contingencia

La Coordinadora del Área de Informática desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

(e) Proceso de Actualización

En base al informe presentado por el director y/o jefe de Unidad y las causas identificadas en la operatividad, se determinará las acciones a tomar.

4.- Sub Factor: Contingencia relacionada a seguridad física.

En el cuadro N.º 13 se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a la Seguridad Física.

Cuadro N.º 13.

Código del Formato	Descripción del evento de Contingencia	Probabilidad Ocurrencia	Impacto	Calificación	Alerta
PLAN DE SEGURIDAD FÍSICA					
INFRAESTRUCTURA					
RC-23	Sustracción de Equipos y software Diversos	0.02	2	0.04	
RC-24	Sabotaje	0.01	2	0.02	
RC-25	Vandalismo	0.01	3	0.03	
RC-26	Actos Terroristas	0.01	4	0.04	

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

ANEXO N° 01

CRONOGRAMA DE PRUEBAS

N°	ACTIVIDAD	INICIO	FIN
		SEMESTRE II	
1	Corte de energía eléctrica del data center principal, ubicado en Av. Gálvez Barrenechea N° 290.	julio	diciembre
2	Desconexión del servicio de Internet.	julio	diciembre
3	Desconexión del aire acondicionado principal del data center principal, ubicado en Av. Gálvez Barrenechea N° 290.	julio	diciembre
4	Sustracción o robo de información, validación de acceso a puertos USB.	julio	diciembre
5	Control de acceso a instalaciones de la entidad, validación de acceso al data Center.	julio	diciembre
6	Perdida del servicio de web hosting que tiene en producción el Sistema de Gestión de Proyectos - Obras "SGPO".	julio	diciembre
7	Desconexión de servidor que tiene en producción el Sistema Integrado de Administración Financiera - "SIAF-SP".	julio	diciembre

Las fechas de inicio y fin de las actividades están sujeto a variación.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

ANEXO N° 02
FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

I. DATOS GENERALES	
Prueba N°	
Escenario de Prueba	(Descripción del escenario a probar/certificar)
Responsable	(responsable del escenario de prueba a probar/certificar)
Lugar	(Lugar de prueba)
Hora de Inicio	
Hora de Fin	

II. INFORMACION DEL PROCESO	
Metodología	(Detallar lo que se va a hacer en la prueba)
Alcance	(Definir hasta donde va a abarcar)
Condiciones de Ejecución	Nombre equipo / servidor / PC de prueba

III. DESARROLLO DE LA PRUEBA

IV. RESULTADO DE LA PRUEBA		
Resultado:	Satisfactorio:	
	Satisfactorio con Observaciones:	
	Deficiente:	

Observaciones:	(En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados)

V. FIRMA DE LOS RESPONSABLES DE LA PRUEBA

Participante	Cargo	Firma