FONDO MUNICIPAL DE INVERSIONES DEL CALLAO
FINVER CALLAO S.A.

PLAN DE CONTINGENCIA INFORMÁTICO EN EL FONDO MUNICIPAL DE INVERSIONES DEL CALLAO – FINVER CALLAO S.A.

GERENCIA DE PLANEAMIENTO, PRESUPUESTO E INFORMÁTICA

2023

FINVER CALLAO S.A.
Vº Bº
GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

INDICE

FINVER CALLAO S.A. Vº Bº GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

INTRODUCCIÓN

La creciente dependencia de las organizaciones en las tecnologías de la información y comunicaciones hace que la continuidad de sus servicios sea vital para su éxito. Sin embargo, los eventos adversos como desastres naturales, fallos técnicos, ciberataques, entre otros, pueden interrumpir la operación normal de los sistemas informáticos y afectar la productividad y eficiencia de la entidad. Por ello contar con un Plan de Contingencia Informático es fundamental para garantizar la recuperación de los servicios de tecnología de la información y Comunicaciones en el menor tiempo e impacto posible. Este plan establece los procedimientos y medidas preventivas y correctivas necesarias para asegurar la continuidad de los servicios críticos de la entidad en caso de un evento adverso, minimizando así los riesgos y garantizando la satisfacción de los usuarios y la protección de la información.

FINVER CALLAO S.A.
Vº Bº
GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

40

CAPÍTULO 1. FINALIDAD

La finalidad de un plan de contingencia para la empresa FINVER CALLAO S.A. es garantizar la continuidad de sus servicios críticos en caso de eventos adversos que pueden afectar la operación normal de los sistemas informáticos. La dependencia cada vez mayor de las Tecnologías de la Información y Comunicaciones hace que la planificación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación sean esenciales para minimizar los riesgos y garantizar la eficiente y efectiva reanudación de los servicios en el menor tiempo posible e impacto posible. En este sentido, el plan de contingencia establece medidas preventivas y correctivas, así como procedimientos de recuperación de datos, comunicación, seguridad entre otros, que permiten una gestión eficiente de las situaciones de crisis y garantizan la satisfacción de los usuarios y la protección de la información crítica de la empresa.

38

CAPÍTULO 2. OBJETIVOS

FINVER CALLAO S.A.
Vº Bº
GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

27

Objetivos

A continuación, se presenta los objetivos generales y específicos del Plan de Contingencia informático de acuerdo a las necesidades de FINVER CALLAO S.A.

Objetivos Generales:

- Asegurar la continuidad de los servicios críticos de la empresa FINVER CALLAO S.A. en caso de eventos adversos que puedan afectar la operación normal de los sistemas informáticos.
- Minimizar los riesgos asociados con la perdida de datos, interrupciones en los servicios y la vulneración de la seguridad de la información.

Objetivos Específicos:

- Identificar los riesgos potenciales que puedan afectar la operación de los sistemas informáticos de la empresa FINVER CALLAO S.A.
- Establecer medidas preventivas y correctivas que permitan minimizar los riesgos identificados y asegurar la disponibilidad, integridad y confidencialidad de la información.
- Establecer procedimientos de recuperación en caso de interrupciones o fallas en los sistemas informáticos, incluyendo la recuperación de datos y la verificación de la integridad de la información.
- Establecer procedimientos de comunicación y coordinación entre los responsables de la contingencia, el personal de la entidad y los proveedores de servicios externos, asegurando una gestión eficiente de la situación de crisis.
- Capacitar al personal de FINVER CALLAO S.A. para que pueda responder adecuadamente ante una contingencia informática y asegurar la actualización periódica del plan de contingencia mediante pruebas y revisiones.
- Garantizar el cumplimiento de las regulaciones y normativas asociadas a la protección de datos y seguridad informática.

FINVER CALLAO S.A. Vº Bº GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

36

CAPÍTULO 3. ALCANCE

El alcance del plan de contingencia informático de FINVER CALLAO S.A. abarca todos los sistemas y servicios tecnológicos de la información críticos para el funcionamiento de la entidad. Esto incluye, pero no se limita a servidores, redes, sistemas de almacenamiento de datos, aplicaciones y dispositivos electrónicos. El Plan de Contingencia también considera los riesgos asociados con las interrupciones del servicio en los proveedores externos de servicios y las fallas en los sistemas de comunicación. Se establecerán medidas preventivas y correctivas para minimizar los riesgos identificados y se definirán procedimientos detallados para la recuperación de datos y sistemas en caso de una interrupción inesperada. El plan de contingencia se aplicará a todos los empleados de la entidad y se llevarán a cabo pruebas periódicas para garantizar la efectividad de los procesos de recuperación.

CAPÍTULO 4. BASE LEGAL

BASE LEGAL:

- Ley N° 29664, ley que crea el Sistema Nacional de Gestión de Riesgo de Desastres (SINAGERD).
- Resolución N°1641-1990 Creación de FINVER CALLAO S.A.
- Resolución de Presidencia N°013-2023-FINVER-CALLAO S.A. /PD que aprueba el Reglamento de Organización y Funciones de FINVER CALLAO S.A.
- Resolución Ministerial N°004-2016-PCM – 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 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N°028-2015-PCM, aprueba Lineamientos para la Gestión de la Continuidad Operatividad de entidades públicas en los tres niveles de gobierno.

FINVER CALLAO S.A.
Vº Bº
GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

CAPÍTULO 5. MARCO TEÓRICO

5.1. Plan de Contingencia Informático.

Es un documento que contiene un conjunto de procedimientos y medidas preparadas por una organización para hacer frente a situaciones imprevistas o de emergencia relacionadas con la tecnología de la información. En otras palabras, es un plan de acción diseñado para mitigar y responder a los efectos negativos de posibles interrupciones, fallas o desastres en los sistemas informáticos de la entidad.

Este plan 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.

5.2. Incidente

Se refiere a cualquier evento no deseado o no autorizado que afecta la integridad, confidencialidad o disponibilidad de los sistemas informáticos. Puede ser causado por una variedad de factores incluyendo errores humanos, fallas de hardware o software, malware, ataques cibernéticos, entre otros. Un incidente informático puede tener consecuencias graves, como la pérdida de datos, el robo de información confidencial o la exposición de vulnerabilidades en los sistemas informáticos.

5.3. Método de análisis de riesgo

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

En el Anexo 1, se detalla la metodología utilizada en el presente Plan.

FINVER CALLAO S.A. Vº Bº GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

30

5.4. Plan de prevención

Es un conjunto de medidas proactivas diseñadas para evitar que ocurran incidentes no deseados o no autorizados en un sistema o ambiente determinado. El objetivo principal de un plan de prevención es identificar los riesgos y vulnerabilidades existentes y tomar medidas preventivas para reducir o eliminar las posibilidades de que se produzcan incidentes. Un plan de prevención puede incluir actividades como la formación y educación de los usuarios, la actualización de software y hardware, la implementación de medidas de seguridad adicionales, la realización de auditorías de seguridad y supervisión constante del sistema.

5.5. Plan de ejecución

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

5.6. 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.

5.7. 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.

FINVER CALLAO S.A. Vº Bº GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

CAPÍTULO 6. METODOLOGÍA

28

El desarrollo del presente Plan seguirá la siguiente metodología basada en (7) fases:

- Fase 1: Planificación.
- Fase 2: Determinación de vulnerabilidades y escenarios de contingencia.
- Fase 3: Estrategias.
- Fase 4: Elaboración del Plan de contingencia Informático.
- Fase 5: Definición y ejecución del Plan de pruebas
- Fase 6: Implementación del Plan de Contingencia.
- Fase 7: Monitoreo.

A continuación, se detalla cada fase:

6.1 Fase 1: Planificación

6.1.1 Organización

La gerencia de Planeamiento, presupuesto e Informática (GPPI) tiene dentro de sus funciones administrar la integridad, confiabilidad y seguridad en el acceso a los sistemas informáticos de la entidad así como también establecer mecanismos de autenticación de usuarios, gestión de data perteneciente a las diversas unidades orgánicas, mantener los sistemas informáticos y la estructura necesaria para el cumplimiento de los objetivos del Fondo Municipal de Inversiones del Callao, así como asegurar y brindar soporte a los mismos.

GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

Figura N°1 – Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones

El Gerente de Planeamiento, Presupuesto e Informática debe gestionar cada uno de los equipos detallados en la Figura N°1. Para lograr esto es fundamental que el coordinador cuente con su personal de apoyo técnico en cada uno de los equipos y la relación de teléfonos de contacto de cada miembro con el fin de poder establecer una comunicación inmediata al momento de cada fase. En particular el coordinador debe tener una línea telefónica disponible en caso de tener que comunicarse con proveedores especializados. Asimismo, los correos electrónicos registrados deben estar alojados en una plataforma en la nube que garantice su disponibilidad. Los equipos que conforman el plan de contingencia debe ser actualizada constantemente y compartida con el personal correspondiente:

- Personal de la Gerencia de Planeamiento, Presupuesto e Informática.
- Gerente General
- Personal de la Sub Gerencia de Logística.

6.1.2 Roles, funciones y Responsabilidades dentro del Plan

A continuación, se describe los roles responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

a. Coordinador de Continuidad Informática

Está representado por el/la Gerente de Planeamiento, Presupuesto e Informática y tiene las siguientes funciones:

- Coordinar, dirigir y tomar decisiones sobre las acciones y estrategias a seguir en caso de una contingencia.
- Decidir cuándo activar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.
- Supervisar y guiar a los equipos operativos de contingencia informática en el desarrollo de sus tareas.
- Evaluar la magnitud de la contingencia y sus posibles efectos sobre la infraestructura tecnológica.
- Mantener informado a la Gerencia General sobre la contingencia, recuperación y posibles contratiempos durante la ejecución del plan.
- Supervisar y monitorear la recuperación de la infraestructura tecnológica de la información en el centro de datos.
- Comunicarse con los proveedores para el reemplazo del Hardware, Software o servicios afectados.

- Declarar la finalización de las operaciones del Plan de contingencia Informático y Recuperación de servicios de tecnologías de la información y comunicaciones una vez se hayan restablecido las operaciones.

b. Equipo de prevención

Está representado por el Personal de la Gerencia de Planeamiento, Presupuesto e Informática, tiene la responsabilidad de llevar a cabo acciones preventivas antes de que ocurra una contingencia informática, con el objetivo de evitar la materialización de este. En caso de que ocurra una contingencia, el equipo debe estar preparado y contar con todos los recursos necesarios para recuperar los servicios de tecnologías de la información y comunicaciones en el menor tiempo posible. A continuación, se detallan las funciones que corresponden a este equipo:

- Establecer y supervisar los procedimientos de seguridad de los servicios informáticos.
- Coordinación de las pruebas de restauración de hardware y software.
- Participación en las pruebas y simulacros de contingencias.
- Verificación del mantenimiento preventivo realizado en los equipos del centro de datos.
- Verificar las tareas de copias de respaldo (Backup)
- Mantener actualizado el inventario de hardware y software utilizado en el centro de datos.
- Ejecutar y verificar las tareas de copias de respaldo.
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y componentes del centro de datos.
- Llevar el control detallado del mantenimiento realizado a cada equipo y componente.
- Elaborar informes técnicos periódicos.
- Verificar la actualización de la relación de servidores, red, documentación de configuraciones de equipos y software de gestión
- Monitorear la red y definir medidas preventivas para minimizar o evitar contingencias y realizar pruebas previas de recuperación.
- Monitorear el funcionamiento de la Central Telefónica.
- Mantener actualizada la lista de anexos y teléfonos.
- Coordinar y verificar que se realicen las copias de respaldo de la base de datos de los aplicativos informáticos en un ambiente adecuado.

FINMER CALLAO S.A. V° B° GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

c. Equipo de emergencia

El objetivo de este equipo es llevar a cabo las tareas necesarias para enfrentar una contingencia o siniestro, con el fin de reducir los efectos negativos que puedan tener sobre los sistemas tecnológicos y los datos del Fondo Municipal de Inversiones del Callao. Su principal función es preservar la integridad de la información y prevenir su pérdida o daño. A continuación, se presenta las medidas que serán tomadas por los miembros del equipo durante la emergencia.

- Notificar la contingencia o siniestro al coordinador
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en el centro de Datos de FINVER CALLAO S.A.
- Ejecutar las medidas de emergencia en los equipos telefónicos y la central telefónica del centro de datos, y comunicar al coordinador.
- Verificar el estado de los sistemas de la información alojados en los servidores y aplicaciones.
- Se realizará un registro de los aplicativos informáticos afectados.
- Contactar a los proveedores de equipos y/o servicios de ser necesario para mitigar la contingencia.
- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final al coordinador.

d. Equipo de Restauración

Este equipo tiene como función principal ejecutar las acciones necesarias luego de que la contingencia o siniestro este controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos de FINVER CALLAO S.A. De manera conjunta con los miembros titulares de la entidad. A continuación, se detalla sus funciones:

- Deben iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del centro de datos de FINVER CALLAO S.A.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecte servidores.
- Notificar al coordinador las acciones de recuperación ejecutadas.

FINVER CALLAO Vº Bº GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

- Iniciar el proceso de recuperación de los servicios relacionados a la comunicación interna y externa de la entidad.
- Realizar la evaluación de condiciones de los equipos de comunicaciones durante la emergencia.
- En caso se requiera desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya una evaluación de condiciones de los equipos informáticos y servicios luego de efectuado el proceso de recuperación.

Cabe precisar que los equipos podrían ejecutar sus actividades de manera paralela, de tal forma que no dependan uno del otro.

6.2 Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

Durante esta fase se llevará a cabo la tarea de reconocer las aplicaciones esenciales, los recursos necesarios y el tiempo máximo de recuperación para los servicios de tecnología de la información y comunicaciones. Para ello, se tendrán en cuenta todos los factores que podrían ocasionar eventos que requieran activar el plan de contingencia.

6.2.1 Procesos y Recursos Críticos

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Tabla N°1 – Procesos y recursos críticos de Tecnologías Informáticas

Proceso Critico	Aplicaciones y/o Recursos críticos	Tiempo de Recuperación
Gestión de Redes e infraestructura de tecnologías de la información	Equipos de Comunicaciones	12h
	Equipos de protección eléctrica del centro de datos (UPS)	24h
	Sistema de aire acondicionado del Centro de Datos	24h
	Cableado de Red de datos	24h
	Sistema de almacenamiento (Storage)	24h
	Medios de Respaldo	24h
	Servidores de red críticos : Directorio activo, File server,	96h
	Central Telefónica	12h
Gestión de sistemas de información y base de datos	Base de datos y fuentes utilizados por el sistema contable	48h
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	48h
Operación y mantenimiento de Tecnología de la Información	Personal crítico responsable de los procesos informáticos	4h

6.2.2 Identificación de Amenazas

Este paso permite identificar aquellas amenazas que pudieran vulnerar los servicios tecnológicos informáticos de FINVER CALLAO S.A., considerando la ubicación geográfica, el contexto actual del centro de datos, así como una percepción global.

Tabla N°2 – Amenazas a los servicios de Tecnologías de la Información

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros naturales
02	Inundación y aniego en el centro de datos	
03	Incendio en el centro de datos	
04	Falla en telecomunicaciones	Tecnológicos
05	Delito Informático	
06	Falla de Hardware y Software	
07	Falla en el Suministro eléctrico de las instalaciones de la entidad	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de Tecnologías de la información	Humano
09	Pandemia y/o Epidemia	Ambiental

Una vez que se han establecido las posibles amenazas que puedan impactar los recursos críticos de tecnología de la información, se procede a evaluar su nivel de probabilidad para poder identificar cuáles de ellas se tendrán en cuenta en la evaluación de riesgos. A continuación, se presenta el detalle del resultado obtenido:

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel de probabilidad estimada
01	Terremoto/Sismo	2	4	Moderado
02	Inundación y aniego en el centro de datos	0	1	Menor
03	Incendio en el centro de datos	0	1	Menor
04	Falla en telecomunicaciones	3	4	Moderado
05	Delito Informático	1	2	Moderado
06	Falla de Hardware y Software	4	5	Alto
07	Falla en el Suministro eléctrico de las instalaciones de la entidad	5	5	Alto
08	Ausencia o no disponibilidad del personal critico de Tecnologías de la información	2	1	Menor
09	Pandemia y/o Epidemia	1	2	Menor

6.2.3 Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos informáticos de FINVER CALLAO S.A. frente a cada amenaza.

- Cámaras de vigilancia en las instalaciones de la entidad
- Mantenimiento a Unidad de respaldo eléctrico.
- Mantenimiento para equipos de aire acondicionado del centro de datos.
- Detector de incendio en el gabinete de datos.
- Respaldo de información
- Solución antivirus instalada en los servidores en red y computadoras.
- Servicios de alojamiento y correo electrónico en la nube con un proveedor que cuenta con todas las medidas de seguridad y respaldo.

6.2.4 Evaluación del Nivel de riesgo

Con el objetivo de establecer el nivel de riesgo de un recurso de tecnología de la información crítico para FINVER CALLAO S.A., se tuvieron en cuenta los siguientes controles existentes que reducen el impacto de la posible amenaza mencionada en el apartado 6.2.2. Según la aplicación de la metodología de riesgo descrita en el Anexo1, se ha obtenido el siguiente resultado:

FINVER CALLAO V° B° GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

Tabla N°4 – Resultado de la evaluación de riesgos de los servicios de tecnologías de la información

Recursos críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en el centro de datos	Incendio en el centro de datos	Falla de Comunicaciones	Delitos Informáticos	Falla de Hardware y Software	Falla en el Suministro eléctrico de las instalaciones de la entidad	Ausencia o no disponibilidad del personal critico de Tecnologías de la información	Pandemia y/o Epidemia
Equipos de Comunicaciones	2	1	1	3	3	3	3	1	1
Equipos de protección eléctrica del centro de datos (UPS)	2	1	1	1	1	2	3	1	1
Sistema de aire acondicionado del Centro de Datos	2	1	1	1	1	1	3	1	1
Cableado de Red de datos	2	1	1	2	1	1	3	1	1
Sistema de almacenamiento (Storage)	2	2	1	2	2	2	3	1	1
Medios de Respaldo	2	1	1	2	2	2	3	1	1
Servidores de red criticos : Directorio activo, File server,	2	2	1	2	2	2	3	1	1
Central Telefónica	2	1	1	1	1	1	3	1	1
Base de datos y fuentes utilizados por el sistema contable	2	1	1	2	2	2	3	1	1
Estaciones de trabajo del personal critico (computadoras personales y portátiles)	2	2	2	2	2	2	3	1	1
Personal critico responsable de los procesos informáticos	2	1	1	1	2	1	1	1	1

1: Nivel bajo de ocurrencia

2: Nivel moderado de ocurrencia

3: Nivel alto de ocurrencia

FINVER CALLAO
Vº Bº
GERENCIA DE PLANEAMIENTO PRESUPUESTO E INFORMATICA

20

6.2.5 Escenarios de riesgo

- Destrucción e indisponibilidad del centro de datos por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- Interrupción de comunicaciones por fallas en el suministro eléctrico del centro de datos y/o en los gabinetes de comunicaciones de la entidad.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el plan de contingencia informático.

Tabla N°5 – Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad del establecimiento	La situación descrita implica que, debido a un terremoto o incendio, el centro de datos sufra un fallo en su funcionamiento o incluso su destrucción. Este evento podría causar interrupciones en los servicios y daños a los equipos informáticos y componentes que se encuentran alojados en el establecimiento.	Extremo
Falla en el funcionamiento de los sistemas de información y portales web	La afirmación se refiere a la posibilidad de que los servidores físicos o virtuales sufran un fallo tanto físico como lógico, lo que podría impedir el acceso a la información o servicios que normalmente se brindan a través de ellos. En otras palabras, la falta de disponibilidad podría deberse a un problema en el hardware o software que los sustenta.	Extremo
Interrupción de comunicaciones por fallas en el suministro eléctrico del centro de datos y/o en el gabinete de comunicaciones de la entidad	Este escenario consiste en el corte o interrupción de las comunicaciones en la entidad, así como en los servicios que se brindan a los clientes internos, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como corte de energía eléctrica, lo cual ocasionaría caída de servicios informáticos hasta la línea de los usuarios finales.	Extremo

6.3 Fase 3: Estrategias del Plan de Contingencia

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre.

6.3.1 Estrategias de prevención de tecnologías de la información

A. Almacenamiento y respaldo de la información (Backups)

- Gestión de copias de respaldo (Backup) de la información almacenada y procesada en el centro de datos tomando en cuenta la frecuencia de

respaldo de información, los medios, la frecuencia de rotación, así como los criterios de identificación.

- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.
- Se utiliza lugares alternativos externos para el almacenamiento de las copias de respaldo.

B. Sitios Alternos para el Centro de datos

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Propios de la entidad.
- Instalaciones de la Municipalidad Provincial del Callao.
- Instalaciones alquiladas.

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

C. Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.
- Si es necesario, adquirir o habilitar hardware y software, así como transportarlos al sitio alterno de ser el caso.
- Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.

- Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa.

- Equipo compatible existente: Equipo existente en sitios alternativos.

*Comprar los equipos cuando se necesitan pueden ser parte de una mejora financiera, pero puede incrementar de manera significativa el tiempo de

recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación comience rápidamente*

D. Entrenamiento y personal de reemplazo

- Todo el personal de la Gerencia de Planeamiento, Presupuesto e Informática debe entrenarse en el proceso de recuperación de los servicios de Tecnologías de la información. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.

E. Renovación Tecnológica

- Se realizará dos revisiones anuales para evaluar la obsolescencia tecnológica de las partes internas de los servidores informáticos. Si es necesario, se llevará a cabo la renovación correspondiente.
- Se llevará un registro de los problemas de deterioro que puedan surgir en los equipos de almacenamiento, procesamiento y comunicaciones. Con base en las estadísticas, se adquirirán equipos de contingencia para garantizar la continuidad de las operaciones.

F. Activación del trabajo remoto

- Verificación y validación de acceso seguro, en remoto a los sistemas y servicios de tecnología de información.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse se cuente con todos los mecanismos de seguridad informáticos.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le puede habilitar el equipo asignado, que se encuentre en FINVER CALLAO S.A., para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, bajo la responsabilidad de la Sub Gerencia de Logística.

6.3.2 Estrategias frente a emergencias en tecnologías de la información

Las estrategias para afrontar emergencias incluyen todas las medidas que se deben tomar durante un desastre o situación crítica, con el objetivo de proteger la información de FINVER CALLAO S.A. y asegurar la continuidad de los servicios informáticos. En este sentido, se establecen acciones específicas para minimizar las pérdidas que puedan surgir en caso de una emergencia o desastre. A continuación, se detallan las acciones que se llevarán a cabo, tanto durante, como después de una contingencia.

Acciones durante la contingencia:

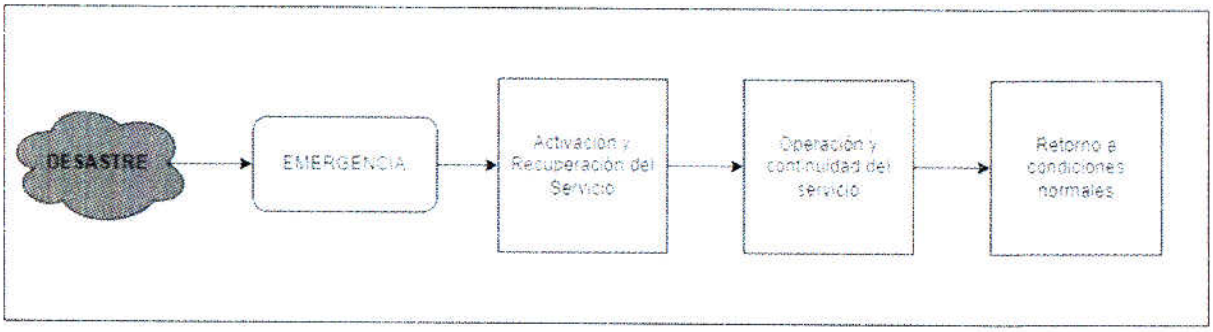
- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad, notificar y reunir a los demás integrantes del equipo de emergencia y restauración de tecnologías de la información.
- Informar a la Gerencia General sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo, si lo amerita.
- Determinar si el área de tecnologías es segura para el personal y los equipos (en caso de una catástrofe)
- Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

6.3.3 Estrategia para la restauración de tecnologías de la información

Las estrategias para la restauración o recuperación de la información y los servicios informáticos de FINVER CALLAO S.A., se enfocan en las acciones que se deben tomar después de un evento critico o desastre, con el objetivo de estabilizar la infraestructura tecnológica y recuperar la información. Para ello, se establecen pautas para que el personal de la Gerencia de Planeamiento, Presupuesto e Informática pueda garantizar la continuidad de las operaciones de la entidad.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Figura N°3 – Ciclo de la estrategia de recuperación de Tecnologías de la Información



16

La priorización de la restauración de los servicios de tecnologías de información de FINVER CALLAO S.A. se ejecutará de acuerdo a lo indicado en la siguiente tabla de información:

Tabla N°6 – Prioridad de atención durante la restauración de TIC

Prioridad de atención	Descripción
1	Atención Prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos e internos como Portal web institucional, Servidores, Central telefónica.
2	Atención Normal: Equipos no relacionados con la atención a los usuarios y manejo de bajo volumen de información

Acciones después de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

6.4 Fase 4: Elaboración del Plan de contingencia y recuperación de Servicios de Tecnologías de la Información

Una vez identificados los eventos de contingencia y los escenarios de riesgo, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente.

El Plan de contingencia y recuperación de los servicios de tecnologías de la información comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N°7 – Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
2	Delito Informático (ataque)	Extremo	FPC-02
3	Falla de Hardware y software	Extremo	FPC-03
4	Falla de Suministro Eléctrico	Alto	FPC-04

15

6.5 Fase 5: Definición y Ejecución del Plan de Pruebas

El plan de pruebas está 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.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutadas por los equipos operativos de la Gerencia de Planeamiento, Presupuesto e Informática.

6.6 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 Gerente de Planeamiento, Presupuesto e Informática realizará las siguientes funciones:

- Supervisar las actividades de copias de respaldo y restauración.
- Organizar las pruebas de restauración de hardware, software y servicios de tecnologías de la información.
- Participar en las pruebas.

6.7 Fase 7: Monitoreo

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

- Realizar mantenimiento de la documentación técnica de operación de servicios de tecnologías de la información.
- Revisión continua de los servidores de FINVER CALLAO S.A.
- Revisión continua del sistema de copias de respaldo.
- Revisión y mantenimiento de los sistemas de soporte eléctrico del centro de datos de FINVER CALLAO S.A.

ANEXOS

- Anexo 1 — Listado de equipos del Centro de Datos y Gabinetes de comunicación clasificados por prioridad de atención.
- Anexo 2 — Formatos de Plan de contingencia informático y recuperación de servicios de tecnologías de la información por evento de riesgo.

ANEXO 1

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICAIONES

N°	Tipo de Equipo	Rol	Descripción	Prioridad
1	Servidor	Controlador de Dominio	Servidor de dominio de red (Directorio Activo)	1
2	Servidor	Repositorio de información	File Server, Servidor de archivos, donde se encuentra la información de las carpetas compartidas de red	1
3	Switch	Comunicaciones	Switch Core, Switch de distribución	1
4	Central Telefónica	Comunicaciones	Conexión entre áreas internas	2
5	UPS	Energia	Equipo de Suministro eléctrico para servidores y equipos de comunicaciones	1
6	Aire Acondicionado	Acondicionamiento	Aire acondicionado para el centro de datos	1

ANEXO 2

FORMATOS DEL PLAN DE CONTINGENCIA INFORMATICO Y RESTAURACION DE SERVICIOS DE TECNOLOGIAS DE LA INFORMACION

FINVER CALLAO **Evento: Delito Informático** **FPC-01**

1. PLAN DE PREVENCION

a. Descripción del evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (Hacking) y/o malware.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, rootkits, bootkits, rogues, etc.

Este evento Incluye los siguientes elementos mínimos identificados por FINVER CALLAO S.A., los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware:

- Servidores
- Estaciones de trabajo

Software:

- Software Base

b. Objetivo

Restaurar la operatividad de los equipos de los servidores y estaciones ubicadas en el centro de Datos y en las oficinas de FINVER CALLAO S.A.

c. Entorno

Este evento puede darse en cualquiera de los servidores y estaciones ubicadas en el centro de datos y oficinas de FINVER CALLAO S.A.

d. Personal Encargado

La gerencia de Planeamiento, Presupuesto e Informática es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de tecnologías de la información de acuerdo a sus funciones.

e. Condiciones de Prevención de Riesgo

- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de las 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 y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- Restricción del acceso a internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación o restricción de lectoras y/o quemadores de CD en las estaciones de trabajo que no lo requieran.
- Des habilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al personal de GPPI, sobre Ethical Hacking a los sistemas operativos, servidores y sistemas informáticos.
- Ejecución de ataques de Hacking Ético por terceros profesionales.

f. Acciones del equipo de Prevención de Tecnologías de la Información

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- Documentar y validad los manuales de restauración de los sistemas de información en producción.

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 del equipo (sistema operativo y aplicaciones).

b. Procesos relacionados antes del evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c. Personal que autoriza la contingencia

El Coordinador de continuidad de Tecnología de la información puede activar la contingencia.

d. Personal encargado

Equipo de Emergencia de TIC.

e. Descripción de las actividades después de activar la contingencia

- Desconectar o retirar de la red de datos de FINVER CALLAO S.A , el servidor o la estación infectada o vulnerada.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir remover el malware/virus del sistema.
- Probar el sistema.

- En caso no solucionarse el problema, formatear el equipo y restaurar la copia de respaldo.

f. Duración

La duración del evento no deberá ser mayor a Dos Horas en caso se confirme la presencia de un virus en estaciones de trabajo y de Cuatro Horas en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a. Personal Encargado

El equipo de restauración de Tecnologías de la Información, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, Laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o Gerente del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b. Descripción de Actividades

Se informará al Gerente de Planeamiento, Presupuesto e Informática el tipo de malware/virus o tipo de ataque encontrado y el procedimiento usado para removerlo.

Esas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un equipo de cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible.
- Reinicio del servicio, prueba y afinamiento del sistema de información
- Conectar el servidor o estación a la red de FINVER CALLAO S.A.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de información afectado.
- Comunicar el restablecimiento del servicio.

En función a esto la Gerencia de Planeamiento, Presupuesto e Informática tomara las medidas preventivas del caso enviando una alerta vía correo electrónico.

c. Mecanismos de Comprobación

Se llenará el formato de incidentes y se informará al Gerente de Planeamiento, Presupuesto e Informática. El personal técnico de soporte presentara un informe a el Gerente de Planeamiento, Presupuesto e Informática, explicando que parte del servicio u operaciones se ha visto afectadas y cuáles son las acciones tomadas.

d. Desactivación del Plan de Contingencia

Con el aviso del coordinador/a se desactivará el presente Plan de Contingencias.

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de base de datos, aplicaciones y archivos
- Storage.

Software

- Aplicativos usados por FINVER CALLAO S.A.

Información

- Información contenida en base de datos
- Información contenida en repositorios de información

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de las imágenes de los servidores.

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones de FINVER CALLAO S.A.

d) Personal encargado

Equipo de prevención de Tecnologías de la información.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores para prevenir mal funcionamiento de los mismos.
- Contar con los Backups de la información contenida en los servidores, así como las imágenes de los mismos.
- Contar con los servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento en general.

f) Acciones del Equipo de Prevención de Tecnologías de Información

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar, supervisar el mantenimiento preventivo a los equipos y componentes del centro de datos.

- Mantener actualizado el inventario de hardware utilizado en FINVER CALLAO S.A.
- Realizar el monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

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

b) Procesos Relacionados antes del Evento

Disponibilidad de las copias de respaldo.

Disponibilidad de instaladores de sistemas operativos y motor e base de datos.

c) Personal que autoriza la contingencia

El/La coordinador/a de Continuidad de Tecnologías de la Información debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia

- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo.
- Verificando que dicho equipo cuente con garantía, de lo contrario se implementara un nuevo servidor virtual configurado de acuerdo a lo requerido.
- Solicitar las cintas de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3. PLAN DE RECUPERACION

a. Personal Encargado

El equipo de Restauración de Tecnologías de la Información luego de validar la corrección del problema de acceso a los servidores y el/la coordinador/a de continuidad de tecnologías de la información informara al Gerente de Planeamiento, Presupuesto e Informática para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b. Descripción de actividades

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falta de los servidores.

Se debe realizar como mínimo las siguientes actividades:

- Instalación y puesta a punto de un equipo de cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.

- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.
- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos a los usuarios finales
- Remitir un mensaje electrónico a los usuarios de FINVER CALLAO S.A. informando la reanudación de los servicios.

En función a esto se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

1. PLAN DE PREVENCION

a) Descripción del Evento

Falla general del suministro de energía eléctrica en el Centro de datos de la entidad.

Este evento incluye los siguientes elementos mínimos identificados por FINVER CALLAO S.A., los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información
- Estaciones de trabajo.
- Equipos de comunicaciones.

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Este evento puede darse en cualquiera de las instalaciones de FINVER CALLAO S.A., considerando la ubicación y los antecedentes que se tienen de cortes repentinos de energía eléctrica.

d) Personal Encargado

El/La Sub Gerente de Logística y el coordinador de continuidad de Tecnologías de la Información son los responsables de realizar las coordinaciones para restablecer el suministro eléctrico.

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicios u operaciones de FINVER CALLAO S.A. se contará con UPS necesario para asegurar el suministro eléctrico en los equipos considerados como críticos.
- Equipo UPS cuenta con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variara de acuerdo a la función que cumpla el UPS.
- Realización de pruebas periódicas al UPS para asegurar su correcto funcionamiento.
- Verificación del cableado eléctrico, una vez por año.
- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deber ser instalados en los ambientes críticos.

f) **Acciones del Equipo de Prevención de Tecnologías de la Información**

- Revisar periódicamente y de forma conjunta con el área de logística las instalaciones eléctricas del Centro de datos.
- Coordinar y supervisar el mantenimiento preventivo de pozo tierra, aire acondicionado.
- Verificar que la red eléctrica utilizada en el centro de datos sea estabilizada. En caso no existan se debe gestionar la implementación.
- Revisar la presencia de exceso de humedad en la sala donde se encuentra ubicado el gabinete de datos.

2. PLAN DE EJECUCION

a. **Eventos que activan la contingencia**

Corte de suministro de energía eléctrica en las instalaciones de FINVER CALLAO S.A.

b. **Procesos Relacionados antes del evento**

Cualquier actividad de servicio dentro de las instalaciones.

c. **Personal que autoriza la contingencia**

El coordinador de continuidad de tecnologías de la información puede activar la contingencia.

d. **Descripción de las actividades después de activar la contingencia**

- Informar a la sub Gerencia de logística del problema presentado.
- Comunicar a la empresa prestadora de servicio de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las gerencias y sub gerencias de FINVER CALLAO S.A.
- En caso la interrupción de energía eléctrica en el centro de datos sea mayor a dos (02) horas, se deberá gestionar con la sub gerencia de logística el apersonamiento inmediato del proveedor de grupo electrógeno.

e. **Duración**

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

3. PLAN DE RECUPERACION

a) **Personal Encargado**

El equipo de restauración de Tecnologías de la Información, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) **Descripción de actividades**

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información.

Se debe realizar como mínimo las siguientes actividades:

- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguiente detalle:
    - ✓ Equipos de comunicaciones (Router, Switches)
    - ✓ Equipos de almacenamiento
    - ✓ Servidores físicos
    - ✓ Servidores virtuales

- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.