# MEMORANDO N° 000295-2023-INVERMET-OGPMP

**A** : **ROCIO SUSANA VIVANCO YOVERA**
**COORDINADORA DE LA UNIDAD FUNCIONAL DE INFOMÁTICA**
**UNIDAD FUNCIONAL DE INFORMÁTICA**

**ASUNTO** : Aprobación del documento PN-UFINIF-01 Plan de Contingencia Informático, en el marco del Sistema Integrado de Gestión (SIG).

**REFERENCIA** : Informe N° 000184-2023-OGPMP-UFINF

**FECHA** : Lima, 01 de septiembre de 2023

Es grato dirigirme a usted en relación al asunto y documento de la referencia, mediante el cual se presenta el Plan de Contingencia Informático, según se detalla en el Cuadro N° 01:

| ITEM | CODIGO | TIPO DE DOCUMENTO | NOMBRE DEL DOCUMENTO | VERSIÓN |
|---|---|---|---|---|
| 1 | PN-UFINIF-01 | Plan | Plan de Contingencia Informático | 1.0 |
| 2 | - | Anexo 1 | Integrantes del Comité de Contingencia Informática | - |
| 3 | - | Anexo 2 | Integrantes de los Equipos de Recuperación de TI | - |
| 4 | - | Anexo 3 | Directorio del personal de TI | - |
| 5 | - | Anexo 4 | Directorio de proveedores | - |
| 6 | - | Anexo 5 | Fichas descriptivas de los sistemas informáticos | - |

En ese contexto, le comunico que el equipo SIG de la Oficina de Planificación y Modernización (OPM) revisó y aprobó la documentación, la misma que hago mía y suscribo los documentos revisados del citado cuadro.

Asimismo, una vez realizada la firma del documento deberá remitirlo a este despacho para ser ingresado a la Gestión Documental del SIG y proceder con su difusión, conforme a lo establecido en el procedimiento PR-GG-01 Elaboración, aprobación, actualización, control y difusión de documentos del sistema integrado de gestión del INVERMET.

Del mismo modo, deberá revisar constantemente junto a su equipo de trabajo, la documentación del Sistema Integrado de Gestión.

Finalmente, deberá realizar la **Difusión Interna entre su personal** y la correcta **Implementación de la Documentación** en comentario, en coordinación con la Oficina General de Planificación, Modernización y Presupuesto_ SIG-OPM.

Atentamente,

**CESAR HILARIO MANCILLA AGUILAR**
**JEFE DE LA OFICINA GENERAL DE PLANIFICACIÓN, MODERNIZACIÓN Y PRESUPUESTO**

OGPMP/CMA/sñb
Adj.: Lo indicado

# PLAN DE CONTINGENCIA INFORMÁTICA

OFICINA GENERAL DE PLANIFICACIÓN, MODERNIZACIÓN Y PRESUPUESTO

UNIDAD FUNCIONAL DE INFORMÁTICA

| Código: PN-UFINF-01 | Versión 1.0 |
|---|---|

| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
|---|---|---|
| Unidad Funcional de Informática | Oficina de Planificación y Modernización | Oficina General de Planificación, Modernización y Presupuesto |
| | Oficina General de Planificación, Modernización y Presupuesto | |

## Control de Cambios

| Nº VERSIÓN | DETALLE DE LA MODIFICACIÓN | ELABORADO POR: | REVISADO POR: | APROBADO POR: | FECHA |
|---|---|---|---|---|---|
| 1.0 | Versión inicial del documento | Unidad Funcional de Informática | Oficina de Planificación y Modernización<br>Oficina General de Planificación, Modernización y Presupuesto | Oficina General de Planificación, Modernización y Presupuesto | 31/08/2023 |

# Contenido

## RESUMEN EJECUTIVO

En el presente documento se describe el Plan de Contingencia Informática del Fondo Metropolitano de Inversiones – INVERMET, mediante el cual se declaran las medidas provisionales para reestablecer las prestaciones de los sistemas informáticos de la Entidad, luego de ocurrida alguna emergencia o interrupción excepcional de dichos sistemas.

Este documento está concebido para ser utilizado por el personal de la Unidad Funcional de Informática (UFINF) de la Oficina General de Planificación Modernización y Presupuesto de INVERMET. Su contenido está organizado en 11 apartados, cuyo contenido se indica a continuación.

El apartado 1 contiene una reseña introductoria sobre el fin y el contenido del Plan de Contingencia Informática.

El apartado 2 describe el propósito general y los objetivos específicos del Plan de Contingencia Informática.

El apartado 3 detalla la normativa aplicable al Plan de Contingencia Informática.

El apartado 4 describe de forma sumaria el ámbito de aplicación del presente plan en lo referente a los sistemas informáticos considerados.

El apartado 5 proporciona detalles sobre los sistemas informáticos cubiertos, los tipos de evento de interrupción contemplados, así como los roles y funciones para la ejecución y mantenimiento del Plan de Contingencia Informática.

El apartado 6 especifica el conjunto de actividades que los diferentes equipos operativos deben realizar anticipadamente con el fin de permanecer preparados para afrontar situaciones de contingencia.

El apartado 7 describe los lineamientos de respuesta a la interrupción de cada sistema informático individual, de acuerdo a los mecanismos de recuperación disponibles para el efecto.

El apartado 8 desarrolla las diferentes fases del proceso de respuesta a eventos de desastre: acciones iniciales para el manejo de la crisis, notificación al personal y activación del plan, restauración de las capacidades y operación en contingencia, y así como el retorno a las condiciones de funcionamiento normales.

El apartado 9 describe las acciones orientadas al adiestramiento y ensayo de las estrategias de recuperación establecidas, de manera que pueda contarse con procedimientos probados y una organización entrenada en la ejecución del plan.

El apartado 10 expone diversas pautas para la revisión y actualización de la documentación del Plan de Contingencia Informática.

El apartado 11 recopila toda aquella información de apoyo cuyo detalle es preciso disponer al momento de activarse el plan ante una emergencia.

## 1. INTRODUCCIÓN

El Fondo Metropolitano de Inversiones - INVERMET considera que la información es el principal patrimonio institucional necesario para el desarrollo de sus actividades u operaciones de forma confiable y oportuna, por lo que deben proveerse guías de acción que permitan afrontar adecuadamente las contingencias y desastres que puedan dañar a sus sistemas de información.

El Plan de Contingencia Informática es un documento táctico operativo cuyo fin fundamental es apoyar a la restitución de los sistemas informáticos a cargo de la Unidad Funcional de Informática (UFINF) de la Oficina General de Planificación, Modernización y Presupuesto de INVERMET, reduciendo los efectos de una eventual indisponibilidad mediante la formulación y adopción de una estrategia de recuperación ordenada y priorizada, una organización claramente establecida y procedimientos de actuación desarrollados de manera tal que permitan asegurar la recuperación de las operaciones de las tecnologías de la información (TI).

En el presente plan, se ha especificado tanto el alcance como la organización requerida para la implementación del mismo y se han contemplado escenarios de contingencia que incluyen incidentes mayores y eventos de desastre, presentándose las estrategias que han sido elaboradas para coordinar y acometer la recuperación de los sistemas y servicios informáticos comprendidos dentro del alcance establecido. Además de dichas estrategias, que constituyen acciones a realizarse durante y después de la ocurrencia de los eventos contingentes, se presentan las acciones previas a estos eventos que se llevarán a cabo con fines preventivos. Finalmente, se exponen las acciones de entrenamiento, pruebas y mantenimiento del plan, orientadas a conservar su vigencia y sostenibilidad.

La planificación y el desarrollo de una capacidad de respuesta y recuperación ante las contingencias que afectan a los sistemas informáticos ofrece beneficios tales como:

- Determinar acciones preventivas que reduzcan el grado de vulnerabilidad de las operaciones de TI.
- Facilitar la oportuna toma de decisiones ante la ocurrencia de anomalías o fallas en la tecnología de soporte.
- Asegurar la estabilidad operativa y de la organización frente a circunstancias de siniestros.
- Contribuir a generar una cultura de seguridad y control.

El plan descrito en este documento se complementa con los siguientes planes adicionales estrechamente relacionados:

- Plan de Gestión de Crisis de TI: en el que se describe el conjunto de acciones iniciales a realizar ante la ocurrencia de emergencias.

- Plan de Pruebas de Contingencia Informática: en el que se detalla el procedimiento general de prueba del plan de contingencia desarrollado.

El presente y los mencionados planes complementarios conforman, conjuntamente, el denominado Plan Integral de Contingencia Informática (PICI) del Fondo Metropolitano de Inversiones - INVERMET.

## 2. OBJETIVOS

El presente Plan de Contingencia Informática tiene como propósito general poner a disposición, bajo un esquema organizado, viable y ágil, un conjunto de medidas indispensables que permitan enfrentar una interrupción mayor en las operaciones o una situación de desastre, de modo que se restablezcan los servicios y sistemas de información afectados dentro de un periodo de tiempo aceptable.

Los objetivos específicos del Plan son los siguientes:

- Definir la estructura organizacional necesaria para dirigir y realizar las actividades de contingencia informática.
- Formular el proceso ordenado y progresivo de reposición de los sistemas informáticos.
- Establecer las actividades de coordinación entre los diferentes puntos de contacto ante un incidente crítico y severo.
- Identificar los mecanismos y procedimientos de recuperación de las operaciones de tecnologías de la información.
- Precisar los periodos de tiempo requeridos para la recuperación.
- Familiarizar a los equipos de recuperación sobre aspectos de respuesta a las emergencias y elaboración de pruebas de contingencia.
- Asegurar que los procedimientos de recuperación sean probados y actualizados de manera periódica, fortaleciendo su confiabilidad.
- Mantener y actualizar la documentación de los procedimientos de recuperación establecidos.

## 3. BASE LEGAL

- Ley Nº 27972 Ley Orgánica de Municipalidades.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.
- Decreto Legislativo N° 604, que crea el Sistema Nacional de Informática
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital

- Decreto Supremo N° 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital.
- Resolución Contraloría General Nº 320-2006-GC que aprueba las Normas de Control Interno para el Sector Público.
- Decreto Ley N° 22830, Ley de creación del INVERMET.
- Ordenanza N° 2315-2021, que aprueba el Reglamento del INVERMET
- Decreto de Alcaldía Nº 02-2022, que aprueba el Manual de Operaciones del Fondo Metropolitano de Inversiones.

## 4. ALCANCE

El Plan de Contingencia Informática desarrollado en este documento es de aplicación para aquellos sistemas informáticos que han sido considerados como críticos para la continuidad de los servicios institucionales de INVERMET ante determinados eventos de interrupción operativa.

El alcance de este Plan no incluye la restitución de componentes particulares de los sistemas informáticos referidos, considerándose que en tal caso se deben aplicar los correspondientes procedimientos de manejo de incidentes operacionales establecidos en las áreas técnicas responsables, debido a que tales incidentes no constituyen escenarios que justifiquen la activación de los procedimientos de coordinación y gestión de respuesta descritos en el presente Plan de Contingencia Informática.

## 5. CONDICIONES OPERATIVAS DEL PLAN

### 5.1 SISTEMAS INFORMÁTICOS CONSIDERADOS

El presente Plan de Contingencia Informática comprende la recuperación de los siguientes sistemas informáticos de INVERMET:

1) Sistema de Trámite Documentario
2) Sistema Integrado de Administración Financiera (SIAF)
3) Sistema Integrado de Gestión Administrativa (SIGA)
4) Sistema de Valores en Custodia
5) Sistema de Boletas de Pago en Línea
6) Sistema de Valorizaciones
7) Portal web institucional
8) Sistema de Fedatarios
9) Servicio de directorio (MS Active Directory)
10) Servicios de almacenamiento, respaldo y recuperación de datos

Como se verá posteriormente en relación a la estrategia de recuperación individual **(apartado 7 de este documento**), para cada uno de los sistemas informáticos considerados en el presente Plan se ha elaborado una ficha descriptiva en el que se describen detalles referidos a:

- los responsables de la operación del sistema;
- la ubicación física de la plataforma tecnológica de soporte;
- breve descripción de la funcionalidad y la arquitectura del sistema;
- dependencias con otros sistemas o funciones;
- características técnicas de la plataforma tecnológica de soporte;
- especificaciones de las capacidades técnicas existentes para la recuperación local –esto es, sin requerir traslado a un local alterno– y el respectivo tiempo estimado de recuperación.

De este modo, en las mencionadas fichas descriptivas se encuentra la información sobre los recursos tecnológicos requeridos para la operación normal de los respectivos sistemas informáticos.

### 5.2 ESCENARIOS DE CONTINGENCIA

El presente Plan de Contingencia Informática se aplicará en dos escenarios generales de paralización de las operaciones de TI:

- Cuando algunos de los sistemas informáticos considerados se detienen o interrumpen por una falla drástica que los afecta e impide su operación.
- Cuando todos y de manera simultánea los sistemas informáticos considerados son interrumpidos a causa de un siniestro o desastre.

Ambos escenarios generales comprenden la ocurrencia de eventos repentinos e inesperados que, intrínsecamente, pueden imposibilitar la operación normal de los sistemas informáticos por un periodo de tiempo estimado considerable, lo que a su vez podría conducir a la interrupción prolongada de las operaciones y funciones de negocio que son apoyados por los sistemas informáticos afectados.

De este modo, los escenarios de contingencia mencionados excluyen a incidentes cuyo impacto sobre las plataformas tecnológicas es menor o no requieren periodos extensos de tiempo para su resolución. Así, el reemplazo o instalación programada de equipamiento nuevo, las interrupciones de corta duración y la pérdida de información en el Centro de Cómputo de INVERMET o a nivel de los equipos de usuario final, son situaciones fuera del alcance del presente plan pues pertenecen más bien al ámbito de la gestión operativa de las tecnologías de la información.

Se ha considerado que el primer escenario de contingencia indicado, donde los sistemas informáticos son interrumpidos parcial o individualmente, pueda tener lugar debido principalmente a fallas en los equipos o fallas por error humano que,

de no ser controladas oportunamente, podrían desencadenar una paralización permanente de las operaciones de TI. Para este tipo de escenario se adopta una estrategia de recuperación individual de los sistemas informáticos afectados.

El segundo escenario de contingencia establecido se origina en circunstancias adversas como incendio, sismo, apagón, vandalismo o convulsión social, que alteran y comprometen la continuidad de las operaciones de los sistemas informáticos que se alojan en el Centro de Cómputo Principal de INVERMET. Se han contemplado dos situaciones posibles de indisponibilidad de los sistemas informáticos dentro de este escenario:

- Indisponibilidad total del Centro de Cómputo de INVERMET

  Esta situación se presenta cuando el Centro de Cómputo se encuentre inoperativo o en alto riesgo como resultado del evento acontecido, por lo que los sistemas informáticos se interrumpen y no pueden ser operados en tales circunstancias.

- Indisponibilidad de la Base de Datos Oracle

  Esta situación se produce cuando el sistema de gestión de base de datos Oracle, que brinda soporte centralizado a los principales sistemas de información de INVERMET, se paraliza totalmente e impide el acceso a la información almacenada y a los servicios de respaldo de la misma.

Para ambas situaciones de indisponibilidad propias de este escenario de contingencia, se adopta una estrategia de recuperación de desastres.

## 5.3 ESTRUCTURA DE ORGANIZACIÓN PARA LA CONTINGENCIA

Con el objeto de llevar a cabo las acciones de contingencia descritas en el presente plan, la estructura de organización requerida está compuesta por el Comité de Contingencia Informática, el Coordinador de Contingencia Informática y los Equipos de Recuperación de TI.

A continuación, para cada uno de los elementos indicados de la organización requerida para la contingencia, se describirán las características de su conformación y las correspondientes funciones.

### 5.3.1 Comité de Contingencia Informática

El Comité de Contingencia Informática (CCI) es el encargado de establecer un marco de gestión para el establecimiento, implementación, supervisión, monitoreo, mejora y cumplimiento de las estrategias de respuesta y recuperación en la UFINF de INVERMET, así como la distribución y designación de responsabilidades y funciones de las personas que se encarguen de la respectiva operación.

***Consideraciones generales***

a) Los representantes que conformen el Comité de Contingencia Informática deberán asumir las funciones que les corresponda de acuerdo a lo dispuesto en el presente documento.

b) El Comité de Contingencia Informática es la única instancia responsable de autorizar la ejecución de los procedimientos de recuperación consignados en el Plan de Contingencia Informática, según los escenarios de contingencia que correspondan.

c) El Comité deberá reunirse de manera ordinaria por lo menos dos veces al año, o cuando lo considere oportuno y debido a circunstancias que así lo requieran, podrá convocar a reuniones extraordinarias

d) El Comité deberá preparar, por cada reunión que realice, una agenda que permita organizar los asuntos a tratar en la sesión y registrar en acta de reunión respectiva las conclusiones y acuerdos alcanzados.

***Conformación del Comité de Contingencia Informática***

El Comité de Contingencia Informática está conformado por el Jefe de la Oficina General de Planificación, Modernización y Presupuesto, así como por representantes de la Unidad Funcional de Informática (UFINF) de INVERMET, con cargos relevantes para las tareas involucradas.

La información actualizada sobre la conformación y la relación de miembros designados del Comité se muestra en el **Anexo 1**.

***Funciones del Comité de Contingencia Informática***

a) Aprobar los documentos asociados al Plan y sus procedimientos de recuperación.

b) Definir las estrategias de recuperación e impulsar la implementación de las mismas a fin de asegurar los esquemas de contingencia de INVERMET.

c) Proponer normativas, procedimientos y controles sobre aspectos de contingencia informática.

d) Proponer funciones y responsabilidades específicas relativas a la contingencia informática.

e) Asegurar el cumplimiento y actualización del Plan de Contingencia Informática.

f) Monitorear cambios significativos que pudieran variar los riesgos contingentes sobre los sistemas informáticos considerados.

g) Definir y aprobar los lineamientos para la implementación de un programa de capacitación y entrenamiento para el personal de la UFINF.

h) Revisar y analizar los eventos de contingencia informática para definir y establecer las políticas o controles que permitan administrar el evento en forma adecuada.

i) Monitorear el cumplimiento de los mecanismos de control (indicadores) de la contingencia informática.

### 5.3.2 Coordinador de Contingencia Informática

El Coordinador de Contingencia Informática es el responsable de planificar, actualizar y supervisar la actualización y ejecución del Plan de Contingencia Informática.

***Funciones del Coordinador de Contingencia Informática***

a) Coordinar permanentemente con el Comité de Contingencia Informática y los Equipos de Recuperación de Tecnologías de la Información.

b) Planificar, controlar y supervisar el Plan de Contingencia Informática en coordinación con los líderes de los Equipos de Recuperación.

c) Analizar los resultados de la ejecución del Plan y coordinar con los Equipos de Recuperación para establecer las modificaciones requeridas.

d) Planificar, controlar, supervisar e informar la ejecución del Plan de Pruebas de Contingencia Informática.

e) Hacer seguimiento en coordinación con los Equipos de Recuperación, a

la implementación de las mejoras y levantamiento de observaciones encontradas producto de los resultados de la prueba.

f) Presentar al Comité de Contingencia Informática los resultados de las pruebas de contingencia.

g) Elevar al Comité de Contingencia Informática, para su consideración, las propuestas normativas, controles y procedimientos sobre aspectos de contingencia informática que estime conveniente.

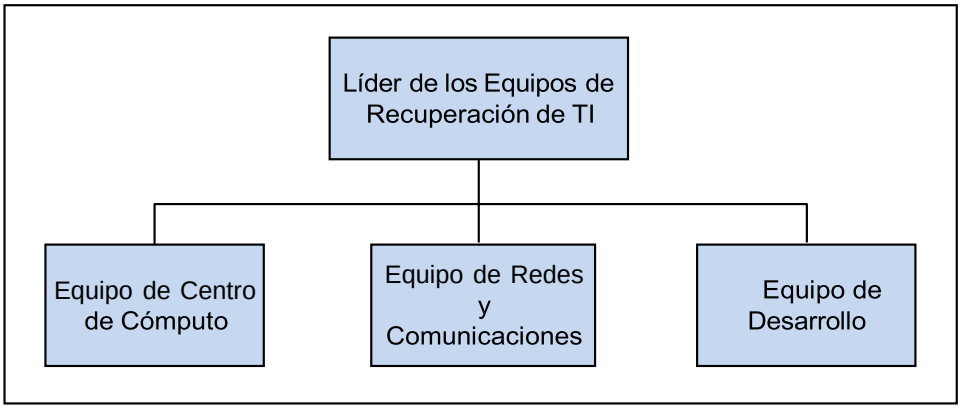
h) Resguardar, mantener y gestionar toda documentación generada por el Comité de Contingencia Informática.

### 5.3.3 Equipos de Recuperación de Tecnologías de la Información

Los Equipos de Recuperación de Tecnologías de la Información tienen la responsabilidad de proporcionar, con objetivos y responsabilidades específicas, el apoyo operativo necesario en las tareas de respuesta y recuperación de los sistemas informáticos, enfocándose en los ámbitos técnicos de su conocimiento y experiencia particulares.

***Estructura organizacional***

Los Equipos de Recuperación de TI, en adelante Equipos de Recuperación, se organizan en diferentes áreas funcionales con especializaciones técnicas, de acuerdo a la estructura que se muestra en el siguiente diagrama.




Los Equipos de Recuperación están comandados por el Líder de Equipos de Recuperación de TI.

En el **Anexo 2** se muestra información actualizada sobre los integrantes de los diferentes Equipos de Recuperación y sus respectivos líderes de equipo.

Los Equipos de Recuperación participan activamente en la realización de las actividades técnicas operativas tanto en las pruebas de contingencia como en

la ejecución del plan durante los eventos de contingencia.

El Líder de Equipos de Recuperación de TI dirige y supervisa la ejecución de las actividades previstas en el Plan de Contingencia Informática ejecutadas por los integrantes de dichos equipos.

***Funciones del Líder de Equipos de Recuperación de TI***

a) Comunicar al equipo la UFINF de la ocurrencia de un evento de contingencia.

b) Asegurar que todos los equipos de recuperación cuenten con sus procedimientos de contingencia actualizados.

c) Dirigir las acciones de los equipos de recuperación durante las pruebas o eventos de contingencia.

d) Coordinar activamente con el equipo de recuperación durante la prueba o eventos de contingencia, informando sobre el estado situacional e incidentes que se presenten.

e) Detener las pruebas de contingencia ante un incidente que afecte e imposibilite continuar con las mismas.

f) Coordinar con los equipos de recuperación la implementación de las oportunidades de mejora identificadas como resultado de las pruebas.

g) Coordinar los traslados de equipos y recursos necesarios para la operación en contingencia.

h) Notificar a proveedores e instituciones el esquema de atención a brindar mientras dure la contingencia.

i) Coordinar el restablecimiento de los sistemas y servicios proporcionados por terceros.

***Funciones del Equipo de Recuperación del Centro de Cómputo***

a) Preparar y mantener actualizada la documentación técnica de sistemas requerida para elaborar el Plan de Contingencia Informática.

b) Verificar el cumplimiento de los procedimientos de respaldo de los sistemas y plataformas a su cargo.

c) Participar en las pruebas de contingencia informática.

d) Efectuar la evaluación preliminar de daños en el centro de cómputo.

e) Realizar las actividades preliminares de respuesta que conlleven a la activación y operatividad de las bases de datos y sistemas centrales.

f) Verificar la disponibilidad de las aplicaciones y datos requeridos para la operación de los sistemas informáticos recuperados.

g) Asistir técnicamente en la validación de los sistemas informáticos.

h) Registrar las incidencias y cambios realizados durante las actividades de respuesta y recuperación.

i) Coordinar el soporte a los usuarios de INVERMET.

***Funciones del Equipo de Recuperación de Redes y Comunicaciones***

a) Preparar y mantener actualizada la documentación técnica de redes y configuración de equipos de comunicaciones, requerida para elaborar el Plan de Contingencia Informática.

b) Verificar el cumplimiento de los procedimientos de respaldo de los equipos de redes y comunicaciones.

c) Participar en las pruebas de contingencia informática.

d) Efectuar la evaluación preliminar de daños en los equipos de redes y comunicaciones.

e) Coordinar con las firmas proveedoras de los servicios de comunicaciones contratados para asegurar la operatividad de los mismos.

f) Habilitar los enlaces de contingencia, recuperar las configuraciones de los equipos de comunicaciones, y restablecer las conexiones.

g) Verificar la operación de las conexiones y equipos de comunicaciones recuperados.

h) Registrar las incidencias y cambios realizados durante las actividades de respuesta y recuperación.

***Funciones del Equipo de Recuperación de Desarrollo***

a) Preparar y mantener actualizada la documentación técnica de las aplicaciones, requerida para elaborar el Plan de Contingencia Informática.

b) Asegurar la debida protección del código fuente de las aplicaciones.

c) Coordinar con los otros Equipos de Recuperación para la resolución de incidentes en las aplicaciones.

d) Diseñar y efectuar las pruebas de acceso y funcionamiento de las aplicaciones.

e) Validar con los usuarios finales la completa operatividad de las aplicaciones restauradas.

## 6. ACTIVIDADES DE PREVENCIÓN

Las actividades de prevención constituyen una fase del planeamiento de la contingencia informática que se orienta a la reducción de vulnerabilidades mediante el empleo de medidas para prevenir, detectar o detener posibles incidentes que, si no se mantienen bajo control, podrían resultar en desastre (incidente severo y prolongado).

Las actividades que se describen a continuación tienen por finalidad preparar las condiciones que favorecen al óptimo desempeño del Plan de Contingencia Informática, por lo que deben ser realizadas regularmente.

1) Actividades del Comité de Contingencia Informática

   a) Proponer la implementación de salvaguardas físicas pertinentes para la prevención de desastres, tales como uso de sistemas de detección de humo, supresión de fuego, aire acondicionado, suministro de energía ininterrumpida (UPS), generador de energía, sensores de control ambiental (temperatura y humedad), control de acceso físico, almacenamiento externo de las copias de seguridad.

   b) Proponer la implementación de salvaguardas procedimentales pertinentes para la prevención de desastres, tales como programación regular de copias de seguridad, inspecciones de seguridad y salud en el trabajo, simulacros de sismo, entrenamiento en uso de extinguidores, programas de concientización en seguridad.

   c) Asegurar que se lleven a cabo acciones de adiestramiento para el personal técnico operativo que permitan reforzar el conocimiento y obtener mayores destrezas en:

      - los procedimientos operativos estandarizados que se hayan establecido, a fin de evitar o reducir las fallas por error humano;
      - los procedimientos de mantenimiento establecidos para los sistemas informáticos en uso, a fin de evitar o reducir las fallas de los equipos.

   d) Revisar periódicamente el Plan de Contingencia Informática para tratar los cambios en la organización, los sistemas informáticos, los entornos de operación, o los problemas encontrados durante la implementación, ejecución o prueba del plan.

2) Actividades del Líder de Equipos de Recuperación de TI

   a) Respecto a recursos y materiales aplicados a la infraestructura

      - Validar el funcionamiento y los esquemas de operación de:
        - Servidores y componentes
        - Redes de comunicación de voz y datos
        - Instalaciones y sistemas redundantes
        - Aplicaciones

- Respaldos
- Planes y procedimientos de recuperación de TI

b) Respecto a la preparación y actualización de respaldos
   - Asegurar la ejecución de los respaldos de información según el procedimiento y la frecuencia establecidos.

c) Respecto a la disponibilidad del personal
   - Validar el plan respecto a la vigencia del personal existente.
   - Validar la información proporcionada por el personal.

d) Respecto al procedimiento interno de notificación
   - Efectuar pruebas de validación de teléfonos fijos y celulares.

e) Respecto a proveedores
   - Actualizar la lista de proveedores.
   - Validar los números de teléfono de los proveedores externos.

3) Actividades del Equipo de Recuperación del Centro de Cómputo

a) Revisar y mantener actualizado el inventario de sistemas y aplicaciones.

b) Revisar y mantener actualizados los procedimientos operativos de las plataformas informáticas y de la infraestructura técnica de apoyo.

c) Verificar periódicamente que se cumplan en forma apropiada los procedimientos operativos de los sistemas y plataformas a su cargo.

d) Revisar, analizar y actualizar los procedimientos de recuperación de los sistemas y plataformas a su cargo.

e) Asegurar el cumplimiento de las políticas y procedimientos de respaldo de la información.

4) Actividades del Equipo de Recuperación del Redes y Comunicaciones

a) Verificar que se mantienen actualizados los diagramas del Centro de Cómputo, los diagramas de red, las especificaciones de hardware, la configuración de los equipos y los procedimientos de recuperación.

b) Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias de comunicaciones.

c) Verificar la ejecución de los procedimientos de respaldo de la configuración de los equipos de comunicaciones, en cumplimiento de las políticas establecidas.

5) Actividades del Equipo de Recuperación de Desarrollo

a) Mantener actualizado el inventario de las aplicaciones y sus versiones.

b) Revisar y mantener actualizados los procedimientos de validación de la funcionalidad de las aplicaciones consideradas en el Plan de Contingencia Informática.

c) Asegurar los respaldos de los códigos fuente y versiones de las aplicaciones.

d) Implementar procedimientos que faciliten la resolución de incidentes en la operación de las aplicaciones.

A fin de facilitar las coordinaciones requeridas para la realización de las actividades señaladas, en el **Anexo 3** se proporciona la información de contacto necesaria para identificar y ubicar a los especialistas de la UFINF.

Asimismo, en el **Anexo 4** se brinda la información de contacto de los proveedores a los que se podría acudir para solicitar su apoyo.

Finalmente, las actividades de entrenamiento y pruebas de contingencia consideradas en el presente plan constituyen medidas efectivas para el objetivo de reducir potenciales fallas y errores en los propios procedimientos de recuperación.

## 7. ESTRATEGIA DE RECUPERACIÓN INDIVIDUAL DE SISTEMAS

En el **Anexo 5** de este Plan se presentan fichas descriptivas de cada uno de los sistemas informáticos, en las que se han incluido reseñas sobre los mecanismos disponibles para su recuperación local. En dicho anexo, se podrá observar que la mayoría de los sistemas informáticos tiene alguna capacidad de recuperación local que puede estar basada en disposiciones alternativas como redundancia de la plataforma tecnológica, réplica física o virtual de equipos informáticos, u operación en alta disponibilidad. Para cada sistema informático que no cuenta con un esquema de recuperación local, en la respectiva ficha se ha manifestado la recomendación para su pronta habilitación, considerando que estos sistemas son activos críticos para INVERMET.

Luego de ocurrido el evento que da lugar a la indisponibilidad de algunos de los sistemas informáticos, se realizan las siguientes acciones:

a) El Equipo de Recuperación del Centro de Cómputo o el de Redes y Comunicaciones, según sea el caso, llevará a cabo una evaluación del estado de situación de los sistemas informáticos afectados, informando inmediatamente al Coordinador de Contingencia Informática.

   Estos, a su vez, comunicarán lo evaluado al Líder de los Equipos de Recuperación de TI.

b) El Líder de los Equipos de Recuperación de TI y los miembros de los Equipos de Recuperación analizan la situación encontrada y proponen el curso de acción a tomar, dependiendo de los daños encontrados y las facilidades técnicas para la rehabilitación de los sistemas informáticos afectados. El Líder de los Equipos de Recuperación de TI reporta lo acordado al Coordinador de Contingencia Informática.

c) El Coordinador de Contingencia Informática comunica al Comité de Contingencia Informática el estado de situación, las acciones en curso y el tiempo estimado que tomará la recuperación de los sistemas informáticos. El Comité notifica la situación a las unidades de organización afectadas de INVERMET.

d) Los Equipos de Recuperación realizan los preparativos necesarios para la operación en contingencia de los sistemas informáticos afectados: activación manual de mecanismos de recuperación si fuese preciso, configuración de parámetros operativos, desplazamiento de equipos y materiales, verificación de las plataformas informáticas de contingencia.

e) Los Equipos de Recuperación llevan a cabo las labores técnicas de detalle que correspondan a las tareas generales requeridas para reiniciar las operaciones de cada sistema informático individual, según se señalan en el **Anexo 6**. Estas tareas se llevarán a cabo una vez que estén disponibles las plataformas hardware y software requeridas para la operación de cada sistema informático a recuperar.

f) En casos de eventos que afecten simultáneamente a múltiples plataformas tecnológicas que brindan soporte a más de uno de los sistemas informáticos considerados para la contingencia, los esfuerzos de recuperación se deberán efectuar de acuerdo al orden de prioridad que se muestra en el **Anexo 7**.

g) Una vez que los Equipos de Recuperación de Centro de Cómputo, y de Redes y Comunicaciones finalizan las actividades técnicas con las que se restablecen las plataformas informáticas, el Equipo de Recuperación de Desarrollo validará el funcionamiento correcto de las aplicaciones respectivas, comunicando los resultados al Líder de los Equipos de Recuperación de TI y/o al Coordinador de Contingencia Informática.

h) El Coordinador de Contingencia Informática reporta la disponibilidad de los sistemas informáticos recuperados al Comité de Contingencia Informática, y este notifica a las unidades de organización de INVERMET que correspondan.

i) El Equipo de Recuperación de Desarrollo, brinda el soporte de los aplicativos durante el periodo que dure la operación de TI en contingencia. Asimismo, brindará soporte a los usuarios finales resolviendo consultas, eventos de incidencia y problemas que surjan como producto de la recuperación.

j) El Coordinador de Contingencia Informática con apoyo del Líder de los Equipos de Recuperación de TI, deberá verificar y coordinar las reparaciones, reemplazos o modificaciones necesarias para que las plataformas tecnológicas afectadas se encuentren nuevamente disponibles, estimando una fecha de reparación.

k) El Líder de los Equipos de Recuperación de TI, en conjunto con los líderes de los equipos de Centro de Cómputo, de Redes y Comunicaciones, y de Desarrollo, establecen colegiadamente que las instalaciones físicas, las plataformas tecnológicas y los sistemas de información están aptos para reanudar las operaciones desde sus ubicaciones físicas originales y en condiciones normales.

l) El Comité de Contingencia Informática, después de analizar y evaluar las condiciones de los diferentes sistemas informáticos, determina la estrategia de retorno a las condiciones normales, comunicando esta decisión al Líder de

Recuperación de TI para las acciones respectivas.

m) Los Equipos de Recuperación llevan a cabo los procedimientos técnicos de detalle para el retorno a las operaciones de manera permanente en la ubicación original, coordinando con los proveedores que se requiera de apoyo.

n) El Líder de los Equipos de Recuperación de TI coordina con los líderes de los diferentes equipos para asegurar que se hayan reportado y documentado los problemas encontrados, las decisiones tomadas y las acciones correctivas realizadas durante las actividades de recuperación en sus distintas etapas, finalizando el registro correspondiente e informando al Coordinador de Contingencia Informática.

o) El Coordinador de Contingencia Informática y los Equipos de Recuperación revisan y analizan las bitácoras de incidencias, informes de resultados o registros generados durante las actividades de recuperación a fin de identificar las lecciones aprendidas a incorporar en las actualizaciones del Plan de Contingencia Informática, y adecuar los recursos para futuros eventos.

Una vez que todas las acciones anteriores han sido completadas, el Comité de Contingencia Informática desactivará formalmente el proceso de recuperación del Plan de Contingencia Informática, notificando a los equipos de recuperación, proveedores de servicios y contratistas involucrados.

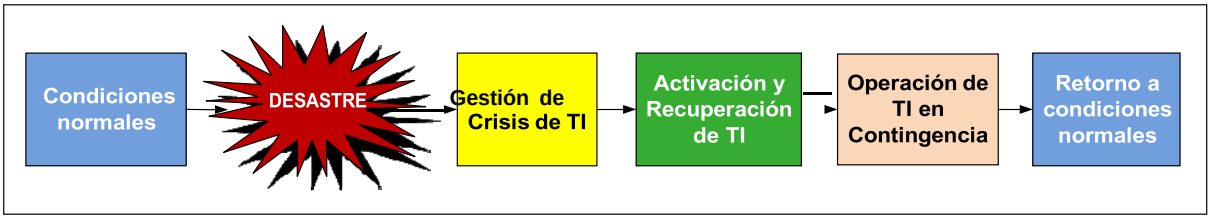
## 8. ESTRATEGIA DE RECUPERACIÓN DE DESASTRES

Para volver a operar los sistemas informáticos de INVERMET, que quedan fuera de servicio luego de un evento grave que configura un escenario de desastre, se establece la siguiente secuencia de etapas que conducen a la restauración de estos sistemas:

- Gestión de Crisis
- Activación y Recuperación de TI
- Operación de TI en Contingencia
- Retorno a Condiciones Normales

La secuencia de las etapas del proceso de recuperación de desastres se muestra en la siguiente gráfica:

**ETAPAS DE LA RECUPERACIÓN DE DESASTRES**



De acuerdo a lo descrito en el apartado 5.2 sobre los escenarios de contingencia, las actividades de esta estrategia de recuperación se ejecutarán para situaciones de:

- Indisponibilidad total del Centro de Cómputo Principal de INVERMET
- Indisponibilidad de la Base de Datos Oracle

### 8.1 GESTIÓN DE CRISIS DE TI

En esta etapa se ponen en acción los mecanismos establecidos para una comunicación eficiente y efectiva entre los diversos equipos de recuperación y los proveedores que participan en la recuperación de las operaciones de los sistemas informáticos, en una situación de caos y condiciones adversas.

Un aspecto crítico a considerar cuando un evento de desastre se manifiesta es la amplia variedad de respuestas que adoptan las personas en situaciones de apremio y confusión, lo que a menudo predispone a personal de TI, competente en otras circunstancias, a efectuar prácticas menos eficientes. Con el fin de mantener un nivel normal de eficiencia, es importante disminuir la posibilidad de improvisar las acciones de emergencia mediante la documentación de las pautas y procedimientos a llevar a cabo inmediatamente después de ocurrido el evento.

La función de gestión de crisis de TI tiene el propósito fundamental de limitar la intensidad o impacto negativo que un evento pueda suscitar sobre la seguridad de las personas, y recopilar información inicial sobre la situación de las instalaciones físicas y otros activos de valor.

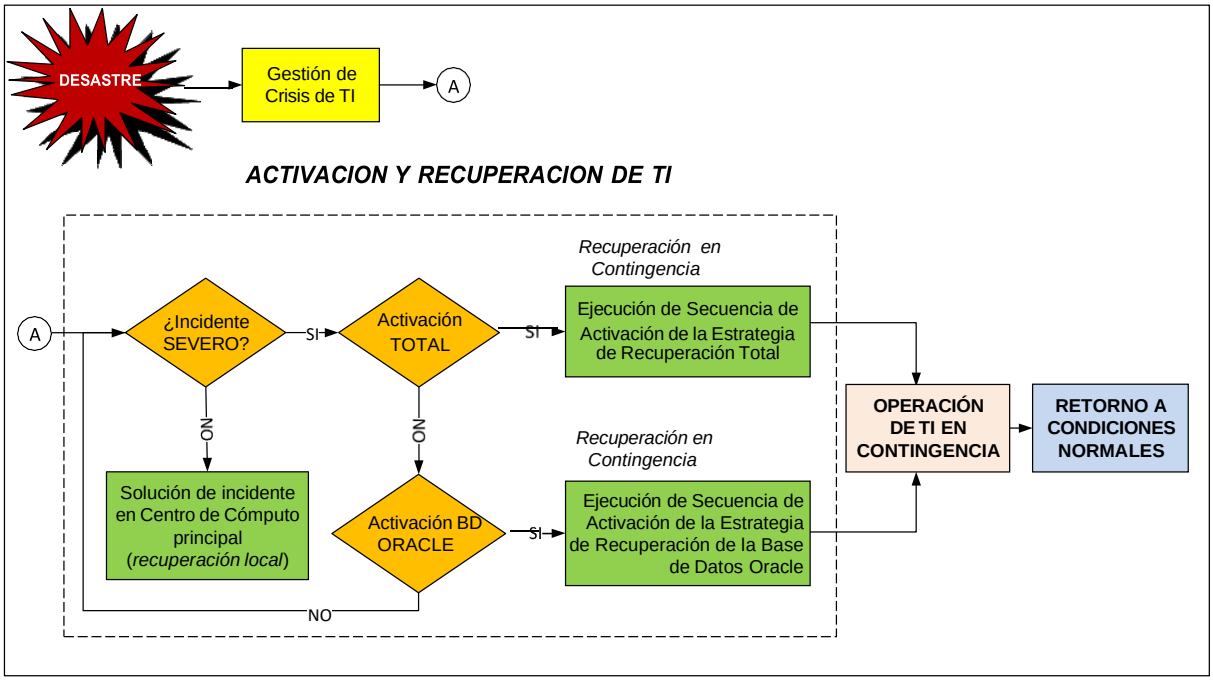
Durante el desarrollo de esta etapa de la recuperación de desastres, el Comité de Contingencia Informática asume las funciones de Comité de Gestión de Crisis de TI para efectos de coordinar y desplegar, en forma ordenada, las acciones de respuesta primaria al evento de desastre.

Los recursos, procedimientos, organización y responsabilidades que se desarrollan en esta etapa se encuentran descritas en los anexos del presente plan, que se irán describiendo a más detalle conforme se desarrollen las pruebas y se realicen las acciones correspondientes para cada recuperación.

### 8.2 ACTIVACIÓN Y RECUPERACIÓN DE TI

La estrategia de recuperación establecida ante una situación de desastre e indisponibilidad total del Centro de Cómputo principal o de indisponibilidad de la Base de Datos Oracle, es restablecer los sistemas informáticos en el Centro de Procesamiento de Datos de la sede principal o de Contingencia provisto. Esto requiere que las plataformas tecnológicas disponibles en las instalaciones sean activadas por el equipo de recuperación para su puesta en producción, y que los Equipos de Recuperación se trasladen y ubiquen en las posiciones para la efectiva recuperación de los sistemas informáticos.

El flujo general de actividades que se desarrollan en esta etapa se grafica en la ilustración mostrada a continuación:




En dicho flujo de actividades, previamente a las acciones de activación que correspondan a las situaciones de indisponibilidad mencionadas, se considera la posibilidad de que, como producto de la evaluación del estado de situación llevada a cabo en la etapa de Gestión de Crisis de TI, se encuentre que el impacto final del evento sobre las operaciones de TI no sea severo y se puedan restaurar los sistemas informáticos afectados mediante acciones de recuperación local, en cuyo caso se aplicarían las estrategias alternativas de recuperación individual de los sistemas según se describe en el apartado 7 del presente documento.

Una vez determinada la necesidad de proceder a la activación de la recuperación en el Centro de Procesamiento de Datos principal o de Contingencia, en cualquiera de las situaciones previstas (indisponibilidad total del centro de cómputo principal o indisponibilidad de la base de datos de producción de INVERMET) se realizan varias tareas que, por su naturaleza, conforman las siguientes tres sub etapas:

a) Activación de plataformas tecnológicas en el Centro de Procesamiento de Datos de Contingencia

Luego de declarado el desastre en la etapa de gestión de crisis, INVERMET comunicará a la Unidad Funcional de Informática para que inicie la activación de las plataformas tecnológicas de contingencia que correspondan.

Los especialistas se comunicarán con los proveedores de los diferentes servicios de requerir activar las plataformas tecnológicas de cómputo y comunicaciones en las instalaciones del Centro de Procesamiento de Datos.

b) Recuperación de los sistemas informáticos

Luego de que el Líder de Contingencia Informática reporta la activación de las plataformas tecnológicas, los especialistas de TI de la UFINF de INVERMET, realizan la revisión y validación de las plataformas y servicios técnicos contratados, y procede a la activación de los servicios de comunicaciones, bases de datos, servidores de aplicaciones y otros que dan soporte a los sistemas informáticos a recuperar.

c) Validación de los sistemas informáticos recuperados

Tras la culminación de las actividades de recuperación de los sistemas informáticos en las instalaciones, el Equipo de Desarrollo valida la disponibilidad y funcionalidad de los sistemas informáticos corroborando que los mismos están conformes y listos para su puesta en producción y entrega a los usuarios finales.

Sólo al concluir las tres sub etapas se procede con la siguiente etapa que corresponde a la operación de TI, mediante la cual se proveen los sistemas informáticos recuperados a los usuarios finales internos y externos de INVERMET.

Conforme vaya desarrollándose la activación de los sistemas informáticos en el Centro de Procesamiento de Datos, el Líder de los Equipos de Recuperación de TI realiza las siguientes acciones:

- Imparte directivas a los equipos de recuperación que vienen actuando según lo planificado.
- Comunica al Comité de Contingencia Informática el estado de la recuperación de los sistemas informáticos en el Centro de Procesamiento de Datos de Contingencia.

El Comité de Contingencia Informática mantiene una constante comunicación con la Gerencia General de INVERMET, informando sobre el avance de la ejecución de las estrategias de recuperación en el Centro de Procesamiento de Datos de INVERMET.

### 8.3 OPERACIÓN DE TI EN CONTINGENCIA

Luego de la puesta en marcha de los sistemas informáticos desde el Centro de Procesamiento de Datos, los Equipos de Recuperación realizarán las siguientes acciones:

a) El Equipo de Recuperación del Centro de Cómputo, así como el de Redes y Comunicaciones, mantendrán operativos a los sistemas informáticos desde las instalaciones.

b) El Equipo de Recuperación de Desarrollo, brinda el soporte de los aplicativos

durante el periodo que dure la operación de TI en contingencia. Asimismo, brindará soporte a los usuarios finales resolviendo consultas, eventos de incidencia y problemas que surjan como producto de la recuperación.

c) El equipo de profesionales brindará el soporte técnico en lo referente a los sistemas informáticos en modo de contingencia.

d) El Líder de los Equipos de Recuperación de TI mantiene una permanente comunicación con el Coordinador de Contingencia Informática, y a través de este, con el Comité de Contingencia Informática, informa sobre el estado de los sistemas informáticos y el desarrollo de las actividades que se ejecutan durante esta etapa.

Esta etapa durará hasta que INVERMET se encuentre en condiciones de volver a realizar sus operaciones normalmente.

### 8.4 RETORNO A CONDICIONES NORMALES

El regreso a la normalidad requiere previamente que la UFINF de INVERMET cuente con las plataformas tecnológicas, aplicaciones y servicios —según las especificaciones descritas en las fichas técnicas del **Anexo 5**— en el ambiente del Centro de Cómputo principal recuperado.

Para que los sistemas informáticos vuelvan a operar desde los ambientes del Centro de Cómputo de INVERMET se deben realizar las siguientes acciones:

a) El Líder de los Equipos de Recuperación de TI contacta a los diversos proveedores de servicios requeridos y evalúa la situación de los recursos afectados en el Centro de Cómputo principal. Asimismo, estima el tiempo de reparación o reemplazo de los componentes afectados y registra toda esta información para su envío al Coordinador de Contingencia Informática.

b) El Coordinador de Contingencia Informática con apoyo del Líder de los Equipos de Recuperación de TI, deberá verificar y coordinar la reparación del Centro de Cómputo principal y notificar el estado y fecha de reparación estimada al Coordinador de la Unidad Funcional de Informática de INVERMET.

c) El Líder de los Equipos de Recuperación de TI, en conjunto con los líderes de los equipos de Centro de Cómputo, de Redes y Comunicaciones, y de Desarrollo, establecen colegiadamente que las instalaciones físicas, las plataformas tecnológicas y los sistemas de información han sido recuperados y se encuentran aptos para reanudar las operaciones desde el Centro de Cómputo de INVERMET.

d) El Coordinador de Contingencia Informática comunica al Comité de Contingencia Informática sobre el estado del Centro de Cómputo de INVERMET, estimando la fecha de su probable disponibilidad.

e) El Comité de Contingencia Informática, después de analizar y evaluar las condiciones del Centro de Cómputo de INVERMET, determina la estrategia de retorno a las condiciones normales, comunicando esta decisión al Líder de los Equipos de Recuperación de TI, para las acciones respectivas.

f) Una vez que se notifica la culminación de sus procedimientos de retorno a las condiciones normales, los Equipos de Recuperación realizan las pruebas de verificación de los sistemas informáticos retornados, de acuerdo a lo descrito en el **Anexo 8**, a fin de corroborar la disponibilidad de dichos sistemas en las instalaciones de INVERMET.

g) Luego de la culminación satisfactoria de las pruebas de verificación indicadas, el Comité de Contingencia Informática declara recuperados y en estado operativo a los sistemas informáticos, notificando la situación a todos los Órganos Funcionales afectados de INVERMET.

h) El Líder de los Equipos de Recuperación de TI coordina con los líderes de los diferentes equipos para asegurar que se hayan reportado y documentado los problemas encontrados, las decisiones tomadas y las acciones correctivas realizadas durante las actividades de recuperación en sus distintas etapas, finalizando el registro correspondiente e informando al Coordinador de Contingencia Informática.

i) El Coordinador de Contingencia Informática y los Equipos de Recuperación revisan y analizan las bitácoras de incidencias, informes de resultados o registros generados durante las actividades de recuperación a fin de identificar las lecciones aprendidas a incorporar en las actualizaciones del Plan de Contingencia Informática, y adecuar los recursos para futuros eventos.

Una vez que todas las acciones anteriores han sido completadas, el Comité de Contingencia Informática desactivará formalmente el proceso de recuperación del Plan de Contingencia Informática, notificando a los equipos de recuperación, proveedores de servicios y contratistas involucrados

## 9. ENTRENAMIENTO Y PRUEBAS

El objetivo de contar con una capacidad viable de respuesta, recuperación y restauración de los sistemas informáticos en los escenarios de contingencia previstos no puede ser alcanzado tan solo con la producción del Plan de Contingencia Informática, pues este plan no constituye una obligación por única vez ni un proyecto con fechas de inicio y fin, sino que más bien representa una actividad regular de carácter institucional cuya sostenibilidad se garantiza mediante acciones como:

- Entrenar y poner al día al personal encargado de la implementación del Plan.
- Poner a prueba las estrategias, los procedimientos y los requerimientos de personal y de recursos.
- Volver a ensayar los objetivos no logrados de las pruebas diseñadas.
- Investigar sobre procesos y tecnologías para mejorar la eficiencia de la respuesta y recuperación.

Las acciones de entrenamiento tienen la intención de familiarizar al personal de TI de la UFINF con los roles y responsabilidades que les corresponde dentro del Plan de Contingencia Informática, así como conocer, revisar y validar el contenido del Plan y los detalles de las actividades y procedimientos de recuperación. De esta manera, las acciones de entrenamiento ayudarán a determinar la efectividad del Plan y a asegurar que el técnico está preparado para participar en las pruebas de contingencia, así como en los actuales eventos de interrupción.

El entrenamiento debería proporcionarse por lo menos una vez al año. El personal nuevo asignado a roles descritos en el Plan, especialmente los que corresponden a los Equipos de Recuperación, debería recibir el entrenamiento poco tiempo después de su designación. En último término, todo el personal participante en labores de contingencia debería estar entrenado al punto de que sean capaces de ejecutar sus respectivos roles y responsabilidades sin ayuda de la documentación actual del Plan.

Asimismo, es útil promover la rotación del personal integrante de los Equipos de Recuperación, de modo que aumente la base disponible de personal entrenado en la ejecución de los procedimientos del Plan durante un evento real.

Los contenidos a considerar en las acciones de entrenamiento deberían incluir los siguientes elementos:

- Exposición general del Plan: propósito, fases, escenarios de contingencia, estructura organizacional.
- Procesos operativos específicos de los Equipos de Recuperación.
- Responsabilidades individuales del personal.
- Coordinación y comunicación de los diferentes equipos de trabajo.
- Pruebas y ejercicios del Plan.

- Revisión, análisis y mantenimiento del Plan.

Por otra parte, se debe someter a prueba el Plan de Contingencia Informática para asegurar la capacidad de respuesta y recuperación de las operaciones en caso de desastre. De este modo, al igual que las acciones de entrenamiento, las pruebas ayudan a determinar la efectividad del Plan y la preparación de los responsables para su ejecución. Un beneficio adicional de las pruebas, más allá de que todas las actividades documentadas del Plan de Contingencia Informática resulten correctas, consiste en la posible identificación de elementos que deban ser ajustados en dicho Plan para que se aumente, de manera adecuada, su capacidad de respuesta frente a los escenarios de contingencia.

Para lograr este propósito, es necesario identificar y documentar los procedimientos que deberán ejecutarse en un ambiente de prueba, incluyendo los objetivos de la prueba particular, el escenario de la prueba y sus premisas. Asimismo, es necesario diseñar un programa de pruebas que asegure una frecuencia de ejecución por los participantes y/o equipos de recuperación, las etapas de las pruebas y los criterios para evaluar los resultados obtenidos en cada prueba, los que eventualmente podrían generar la necesidad de modificar el Plan de Contingencia Informática.

## 10. MANTENIMIENTO Y DISTRIBUCIÓN DEL PLAN

Los documentos del Plan de Contingencia Informática deberán ser revisados habitualmente con el fin de validar la eficacia de la estrategia y los procedimientos descritos en el Plan. Las revisiones, verificaciones y actualizaciones regulares se realizarán en cualquiera de las siguientes circunstancias que pueden ser causa de reajustes en los procedimientos de recuperación:

- Resultados de las pruebas de contingencia.
- Secuelas de la ocurrencia de un desastre o contingencia real.
- Mantenimiento y actualización de las aplicaciones informáticas.
- Renovaciones de la plataforma tecnológica de hardware y software.
- Reubicación física de áreas.
- Cambios en la estructura organizacional y sus funciones.
- Mejoras en la infraestructura de los locales.
- Mejoras en los procesos institucionales.
- Introducción de nuevas tecnologías.
- Nuevos controles de seguridad implementados.

La revisión integral del Plan de Contingencia Informática, en caso no se produzca ninguno de las circunstancias mencionadas, debe ser como mínimo una vez al año.

El procedimiento general de actualización del Plan comprende las fases de identificación de cambios, autorización de cambios y actualización del Plan, que se describen a

continuación.

a) Identificación de cambios

Los cambios que se propongan deberán basar su sustento en cualquiera de las circunstancias señaladas en los párrafos precedentes como factores o causas de reajustes al presente plan. Dichos cambios podrán ser propuestos por el personal integrante de los Equipos de Recuperación, los miembros del Comité de Contingencia Informática, personal que ejerce funciones de gestión de riesgos o funciones de auditoría interna.

Los cambios que se propongan serán informados, con el sustento del caso, al Coordinador de Contingencia Informática.

b) Autorización de cambios

Los cambios propuestos a los documentos del presente plan serán revisados y analizados por el Coordinador de Contingencia Informática conjuntamente con el personal de los Equipos de Recuperación que considere oportuno, a fin de determinar la conveniencia de las propuestas.

La responsabilidad de autorizar las modificaciones a realizar descansa sobre el Coordinador de Contingencia Informática, quien comunicará la decisión al Comité de Contingencia Informática.

c) Actualización del Plan

Una vez autorizados los cambios, el Comité de Contingencia Informática designa al personal de la UFINF de INVERMET responsable de la redacción de los mismos, el que procederá a efectuar dicha labor en coordinación con el personal que propuso las modificaciones.

La revisión y aprobación técnica de los documentos actualizados del Plan de Contingencia Informática se llevarán a cabo por el personal encargado de la UFINF de INVERMET, que correspondan según sus funciones.

Las modificaciones efectuadas sobre el Plan deberán estar registradas a modo de bitácora para facilitar la identificación de los cambios realizados en el transcurso del tiempo, generando así evidencia documentada de las revisiones llevadas a cabo. Para el efecto, se hará uso del Historial de Revisiones presentado en la primera página de los documentos del Plan de Contingencia Informática (el presente documento, el Plan de Gestión de Crisis de TI y el Plan de Pruebas de Contingencia Informática), cuadro que contiene los siguientes campos:

- Versión: del documento; ante cambios mayores la versión se identifica con números enteros (vers. 1.0; 2.0; etc.). Si los cambios son menores se utilizarán cifras decimales (p.ej., vers.1.1, 1.2, 2.1, 3.5).

- Fecha: En formato año/mes/día, contiene la fecha en que se inicia la vigencia del cambio en el Plan.
- Detalle de cambios realizados: Descripción de la modificación con referencias a las secciones del documento en donde se hacen las correcciones. De considerarse necesario, se señalará el motivo por el que se producen los cambios.
- Elaborado por: Nombre y apellidos de las personas responsables de la redacción de los cambios autorizados al Plan.
- Revisado por: Nombre y apellidos de los funcionarios responsables de la revisión del plan actualizado.
- Aprobado por: Nombre y apellidos de la Coordinadora de la UFIN de INVERMET, responsable de la aprobación técnica del plan actualizado.

Luego de actualizada la documentación del Plan, se deberán reemplazar los archivos digitales existentes en medios magnéticos u ópticos y de ser necesario, el soporte en papel, considerando retirar o eliminar todas las copias impresas existentes de la versión anterior. De esta manera se asegura que siempre esté en circulación solo la última versión actualizada.

La documentación actualizada del Plan será distribuida a los miembros del Comité de Contingencia Informática, los integrantes de los Equipos de Recuperación y los responsables de su elaboración, revisión y aprobación técnica, en correspondencia con las necesidades de su conocimiento y uso para efectos de entrenamiento, pruebas, ejecución y mantenimiento del Plan de Contingencia Informática.

## 11. ANEXOS

### Anexo 1: Integrantes del Comité de Contingencia Informática

En el siguiente cuadro se detalla la relación de integrantes que conforman el Comité de Contingencia Informática de INVERMET, los roles asignados y la función principal que desempeñan en dicho Comité.

| Integrante | Rol | Función principal |
|---|---|---|
| Jefe de la Oficina General de Planificación, Modernización y Presupuesto | Presidente del Comité | Aprobar lineamientos, planes de acción, actividades a desarrollar por el Comité de Contingencia. |
| Coordinador de la UFINF | Coordinador de Contingencia Informática | Planificar, actualizar y supervisar la actualización y ejecución del Plan de Contingencia Informática. |
| Representante de la UFINF (Analista o Especialista vinculado a la Gestión del Centro de Cómputo) | Líder de Equipo de Recuperación (Centro de Cómputo) | Brindar apoyo en la formulación, revisión y actualización de la normatividad y a los procedimientos referentes a la continuidad de TI. |
| Representante de la UFINF (Analista o Especialista de la UFINF) | Miembro del Comité | Supervisar y dar la conformidad de la recuperación de los Sistemas de Información en el ámbito del Plan de Contingencia. |
| Representante de la UFINF (Analista o Especialista vinculado a la Gestión de Redes y Comunicaciones) | Líder de Equipo de Recuperación (Redes y Comunicaciones) | Aprobar y supervisar las operaciones técnicas de contingencia relacionadas a la infraestructura informática. |
| Representante de la UFINF (Analista o Especialista de la UFINF) | Miembro del Comité | Coordinar y supervisar el cumplimiento de los aspectos de seguridad de la información en la gestión de la continuidad de TI. |
| Representante de la UFINF (Analista o Especialista vinculado al Desarrollo de Aplicaciones) | Líder de Equipo de Recuperación (Desarrollo) | Brindar apoyo en la revisión y actualización de los sistemas, procedimientos referentes a la continuidad de los sistemas de información de la entidad |

| | | |
|---|---|---|
| Representante de la UFINF (Analista o Especialista de la UFINF) | Miembro del Comité | Brindar apoyo en la configuración, revisión y verificación de los sistemas, procedimientos referentes a la continuidad de los sistemas de información de la entidad |

## Anexo 2: Integrantes de los Equipos de Recuperación de TI

A continuación, se detalla la lista de integrantes que conforman los diferentes Equipos de Recuperación de TI: Centro de Cómputo, Redes y Comunicación, Desarrollo y Base de Datos.

### Líder de Equipos de Recuperación de TI

| Apellidos | Nombres | Unidad de Organización | Rol | Sede | Piso | Anexo | Correo electrónico |
|---|---|---|---|---|---|---|---|
| Benites Sernaque | José Manuel | OGPMP -UFINF | Líder de Equipos de Recuperación | Lampa | 4 | 3520 | jbenites@invermet.gob.pe |

### Equipo de Recuperación del Centro de Cómputo

| Ít. | Apellidos | Nombres | Unidad de Organización | Rol | Sede | Piso | Anexo | Correo electrónico |
|---|---|---|---|---|---|---|---|---|
| **Líder del Equipo** | | | | | | | | |
| 1 | Santa Cruz | Antonio | OGPMP -UFINF | Líder Equipo de Recuperación | Lampa | 4 | 3520 | osinf04@invermet.gob.pe |
| **Integrantes** | | | | | | | | |
| 2 | Sevillano Peralta | Edinson | OGPMP -UFINF | Miembro del Comité | Lampa | 4 | 3520 | osinf11@invermet.gob.pe |
| 3 | Enrique Morales | David | OGPMP -UFINF | Miembro del Comité | Lampa | 4 | 3550 | osinf15@invermet.gob.pe |

### Equipo de Recuperación de Redes, Comunicaciones y Base de Datos

| Ít. | Apellidos | Nombres | Unidad de Organización | Rol | Sede | Piso | Anexo | Correo electrónico |
|---|---|---|---|---|---|---|---|---|
| **Líder del Equipo** | | | | | | | | |
| 1 | Morocho Maldonado | Vicente | OGPMP -UFINF | Líder Equipo Recuperación | Lampa | 4 | 3520 | osinf10@invermet.gob.pe |
| **Integrantes** | | | | | | | | |
| 2 | Luna Mori | Alvaro | OGPMP -UFINF | Miembro del Comité | Lampa | 4 | 3550 | osinf13@invermet.gob.pe |

### Equipo de Recuperación de Desarrollo

| Ít. | Apellidos | Nombres | Unidad de Organización | Rol | Sede | Piso | Anexo | Correo electrónico |
|---|---|---|---|---|---|---|---|---|
| **Líder del Equipo** | | | | | | | | |
| 1 | Azañero Elguera | Manuel | OGPMP -UFINF | Líder Equipo Recuperación | Lampa | 4 | 3520 | jazanero@invermet.gob.pe |
| **Integrantes** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | Durand Missari | Jose Maria | OGPMP -UFINF | Miembro del Comité | Lampa | 4 | 3550 | osinf16@invermet.gob.pe |

## Anexo 3: Directorio del personal de TI

| Ít. | Apellidos | Nombres | Unidad de Organización | Rol | Teléfono |
|---|---|---|---|---|---|
| 1 | Vivanco Yovera | Rocío | OGPMP -UFINF | Coordinadora del Comité de Contingencia | 987729042 |
| 2 | Azañero Elguera | Manuel | OGPMP -UFINF | Líder Equipo Recuperación (Desarrollo) | 960223129 |
| 3 | Benites Sernaque | José | OGPMP -UFINF | Líder Equipos Recuperación | 942478802 |
| 4 | Santa Cruz | Antonio | OGPMP -UFINF | Líder Equipo Recuperación (Redes) | 997889378 |
| 5 | Sevillano Peralta | Edinson | OGPMP -UFINF | Miembro del Comité | 943060150 |
| 6 | Enrique Morales | David | OGPMP -UFINF | Miembro del Comité | 926330684 |
| 7 | Morocho Maldonado | Vicente | OGPMP -UFINF | Líder Equipo Recuperación (Desarrollo) | 993497845 |
| 8 | Luna Mori | Alvaro | OGPMP -UFINF | Miembro del Comité | 948885859 |
| 9 | Durand Missari | Jose Maria | OGPMP -UFINF | Miembro del Comité | 939260375 |

# Anexo 4: Directorio de proveedores

**PROVEEDORES INFORMÁTICA - 2023**

| Nº | SERVICIO | PROVEEDOR | TELEFONO | CORREO ELECTRONICO | CONTACTO |
|---|---|---|---|---|---|
| 1 | TRASLADO DEL CENTRO DE DATOS | JKM REDES Y SERVICIOS E.I.R.L. | 981158164 | EVARGAS@JKM.PE | EDUARDO VARGAS |
| 2 | ACONDICIONAMIENTO Y TRASLADO | ACR SOLUCIONES Y SERVICIOS E.I.R.L | 991766982 | - | - |
| 3 | 22 LAPTOPS LENOVO | LEVEL TECH PERU S.A.C. | 992504402 | SOPORTE@LEVELTECHPERU.COM | CRISTHIAN CORDOV |
| 4 | 21 LAPTOPS TIPO I | PROYECTEC E.I.R.L. | 994731463 -985681289 | SOPORTE@PROYECTEC.COM.PE | CESAR ARI |
| 5 | 21 LAPTOPS TIPO II | LA CASA DEL SUMINISTRO S.C.R.L. | 988316177 | ADMINISTRADOR@SUMINISTROS.COM.I | ADMINISTRADOR |
| 6 | 105 COMPUTADORAS TIPO I | PROTECNOLOGIA E.I.R.L. | 990160403 | SOPORTE@PROTECNOLOGIA.PE | SOPORTE |
| 7 | 18 COMPUTADORAS TIPO II | CANTEC CORPORATION S.A.C | 965446600 | WI_33@HOTMAIL.COM | SOPORTE |
| 8 | IMPRESORA DE FOTOCHECK | MURDOCH SISTEMAS S.A. | 14282233 | MURDOCHVENTAS@GMAIL.COM | SOPORTE |
| 9 | SERVIDOR NAS VASTEC | PARTNERS TECHNOLOGY S.A.C. | 997547072 - (01) 221-0970 / | CONTACTO@PARTECH.COM.PE | SOPORTE |
| 10 | PROYECTORES | COMPUTER AND PRINTING SOLUTIONS S.A.C. | 933774728 | VENTAS@CYPSOLUTIONS.NET HTTPS://( | SOPORTE |
| 11 | INSTALACION DE PROYECTORES | SIRCOMCE EIRL | 987939747 - 987939744 | FSALCEDO@SIRCOMCE.COM | SR. ALCEDO |
| 12 | CABLEADO ESTRUCTURADO DE OAF | SIRCOMCE EIRL | 987939747 - - 987939744 | FSALCEDO@SIRCOMCE.COM | SR. ALCEDO |
| 13 | CABLEADO ESTRUCTURADO DE OCI | H. REA SERVICE E.I.R.L. | 993243635 - 999041718 | HREASERVICE@HOTMAIL.COM | HAIDEE E REA ARGANDONA |
| 14 | SERVICIO DE CUSTODIA DE CINTAS | DOCUMENT SECURITY MW ENTERPRISE SAC | 955 170 110 -924-308995 | ANDREINA.MATA@DOCUMENT.PE CONSULTAS@DOCUMENT.PE, A.CASTRO@DOCUMENT.PE | ANDREINA MATA, EDUARDO CESAR COLCHAO AGUIRRE |
| 15 | INTERNET Y SERVICIO DE TELEFONIA IP | COLINANET | 988217591 988198488 968968992 988217977 | DGUERRERO@COLINANET.COM, WRAM | DORA GUERRERO FREDDY COHELO VIVIANA SALINAS |
| 16 | S10 | SISTEMA 10 S.A.C. | 225-0167 - -(511) 2249014 | VENTAS@S10PERU.COM | ANDREA AREAS C |
| 17 | WINDOWS SERVER 2022 4LIC Y WINDOWS SERVER REMOTE DESKTOP SERVICES- 1 USER CAL 30LIC | DAILY TECHNOLOGY S.A.C. | 739-2405 - 932442563 | MARJORIE.TORRES@DAYLOG.COM.PE | MARJORIE TORRES |
| 18 | ORACLE | SISTEMAS ORACLE DEL PERU S.R.L. | +57 3124573379 | MASAMI.YAMAGUCHI@ORACLE.COM / | SOPORTE |
| 19 | MICROSOFT OFFICE 165 LICENCIAS | INET PERU S.A.C.– | 421-5347 | EDWIN.VASQUEZ@I-NET.PE | EDWIN VASQUEZ |
| 20 | MANTENIMIENTO AIRE ACONDICIONADO | FGO MANTENIMIENTOS INDUSTRIALES S.A.C. | 955-773-251 | AGONZALES@FGOMANTENIMIENTOS.C( | ALVARO GONZALES |
| 21 | MANTENIMIENTO DE UPS | GST INGENIEROS SAC | 676-7889 -942-899 430 | JTICONA@GST-INGENIEROS.COM | JORGE ARMANDO TICONA HUAMÁN |
| 22 | DISCOS PARA AMPLIACIÓN DE CAPACIDAD DE ALMACENAMIENTO PARA SERVIDOR SIAF | JM INVERSIONES HUALLPA S.A.C. | 997 016 093 – 989 013 193 | M.HUALLPA.SAC@GMAIL.COM | MARIA YSABEL CAMACHO HUALLPA |
| 23 | FILE SERVER S/N 2M221100WL | JL BUSINESS AND SERVICE S.A.C. | 961 780 122 / 431-7836 | CURIARTE@JLBUSINESS.COM | CARLOS URIARTE |
| 24 | CERTIFICADOS SSL MULTIDOMINIO | ABC IDENTIDAD DIGITAL S.A.C. | 958 154 406 -992588647 | VENTAS1@ABCID.PESOPORTE1@BIGPRI | ALDAIR CALERO WILBERT CABEZAS BALDEÓN |
| 25 | ENLACE ENTRE SEDES | OPTICAL TECHNOLOGIES | 955479730 - 955458881 | OPERADORES@OPTICAL.PEJSANDOVAL@ | JESUS SANDOVAL |
| 26 | SOPORTE DE LA LICENCIA DE BACKUP | INSPIRA SECURE TECHNOLOGY SAC | 945530223 - (+511) 433 90 22 902757030 | MIGUEL.ARIAS@INSPIRATEC.COM.PEMA | MIGUEL AREAS MANUEL HUAMANÍ |
| 27 | ANTIVIRUS | INNOVA TC | 998767964 932421495 | CESAR.PASTOR@INNOVATC.COM.PE SOPORTE@INNOVATC.COM.PE AMMI.OBREGON@INNOVATC.COM.PE | AMMI OBREGON |
| 28 | COMPONENTE DE FIRMA 4IDENTITY | FIRMUX DIGITAL S.A.C | 955106363 | SOPORTE@FIRMUXDIGITAL.COMMARCI | MARCIA NIQUÉN MIGUEL |
| 29 | LICENCIAS DE CORREO EN NUBE | DAILY TECHNOLOGY S.A.C. | 7392405 | MARJORIE.TORRES@DAYLOG.COM.PE | MARJORIE TORRES |
| 30 | LICENCIA DE DISEÑO GRAFICO | VINIMAX S.A.C | 13308769 (+51) 926 573 028 | CAT@HOSTINGLINUS.COM | OSCAR GONZALES VIVIAN ALFARO |
| 31 | EQUIPO DE SEGURIDAD PERIMETRAL | REDES Y SERVICIOS SAC | 998099129 7390803 Anexo 207 | BRETESI@RED.NET.PE | BRUCE RETES IQUISE |
| 32 | SERVIDOR DE BASE DE DATOS | D.I. CONSULTING SOLUTION INTEGRATOR E.I.R.L. | 941941159 | DAVID.DELGADO@CONSULTIGDI.COM | DAVID DELGADO SANDOVAL |
| 33 | GESTOR DOCUMENTAL - OPEN KM | DOMAIN CONSULTING SAC | 914348617 - 985471897 | AROSADO@DOMAIN.COM.PE | ANGELA ROSADO |
| 34 | CABLEADO ESTRUCTURADO INVERMET | PRIME | 991333148 | MAVILONCCANTO@GMAIL.COM | ARQUITECTO MAVILON |
| 35 | SOPORTE A LA SUSCRIPCIÓN DE RED HAT | INSPIRA SECURE TECHNOLOGY SAC | 945530223 - (+511) 433 90 22 902757030 | MIGUEL.ARIAS@INSPIRATEC.COM.PEMA | MIGUEL AREAS MANUEL HUAMANÍ |
| 36 | ACCESS POINT | BIGSECURE SAC | (+511) 7084143 988963695 | APUICON@BIGSECURE.NET | ANGGIE PUICÓN |
| 37 | PDU | GST INGENIEROS SAC | 676-7889 -942-899 430 | JTICONA@GST-INGENIEROS.COM | JORGE ARMANDO TICONA HUAMÁN |
| 38 | SOPORTE JBOSS | D.I. CONSULTING SOLUTION INTEGRATOR E.I.R.L. | 941941159 | DAVID.DELGADO@CONSULTIGDI.COM | DAVID DELGADO SANDOVAL |
| 39 | TELEFONOS IP | BESTSOL | 970304029 | KARINA.PURIZACA@BESTSOLPERU.COM | HOLA KARINA |
| 40 | DISCOS DUROS PCS | GLOBAL TOOLS | 951479225 | GLOBALTOOLS@INFONEGOCIO.NET.PE | TUESTA GONZALES |

## Anexo 5: Fichas descriptivas de los sistemas informáticos

### *1.- Sistema Integrado de Administración Financiera (SIAF)*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Analista de Sistemas | Sede: Lampa |

**Descripción**

El SIAF es un sistema informático que tiene por finalidad permitir gestionar en todas las entidades públicas de los tres niveles de gobierno (gobierno nacional, gobierno regional y gobiernos locales - municipalidades) los tres procesos básicos de la administración financiera del estadoperuano, siendo estos los siguientes:

- Programación del uso de los recursos en función de las políticas públicas;
- Ejecución de la programación mediante la gestión de ingresos, gastos y financiamiento;
- Rendición de cuentas sobre el uso de los recursos vinculando los aspectos financieros con los resultados obtenidos; asimismo, cuenta con información de seguimiento y evaluación de la gestión, haciendo posible la retroalimentación del proceso de planeamiento y programación.

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| El backup de la data del sistema está programado 3 veces al día. La misma que es resguardada en los servidores de la entidad y en cintas que lleva el proveedor de resguardo cada mes.<br><br>De ocurrir un siniestro existe la necesidad de contar con el apoyo del sectorista asignado por el Ministerio de Economía y Finanzas (MEF).<br><br>La plataforma tecnológica del sistema SIAF se encuentra respaldada en un servidor físico ubicado en Centro de Datos de INVERMET. | Tiempo de recuperación promedio: 4 hora |

**Observaciones**

## *2.- Sistema Integrado de Gestión Administrativa (SIGA)*

**Responsable(s):**

Coordinador de la UFINF

Analista de Sistemas

**Ubicación Física**

Sede: Lampa

**Descripción**

El SIGA es un sistema integral de gestión administrativa que está diseñado para contribuir al ordenamiento y simplificación de los procesos de la gestión administrativa. Apoya a la mejora de la eficiencia en la gestión de los procesos de Abastecimiento, Control Patrimonial de Bienes e Inmuebles, Control de Bienes no patrimoniales, Tesorería y Presupuesto por Resultados.

Características del SIGA

- Sistema de registro único.
- Catálogo unificado, estandarizado y que se relaciona con los clasificadores presupuestales, el Plan Contable y la Clasificación de los Bienes Patrimoniales.
- Programación del Cuadro de Necesidades de Bienes, Servicios, Obras (CN) y la generación del Plan Anual de Adquisiciones y Contrataciones (PAC).
- Registro de Procesos de Selección en sus distintas etapas.
- Seguimiento de la ejecución del Contrato.
- Generación de las Órdenes de Compra y de Servicios.
- Atención de los Pedidos de Bienes y Servicios provenientes de las distintas dependencias de la Entidad.
- Registro y Contabilización de los Movimientos en el Almacén.
- Registro y Control de los Bienes e Inmuebles.
- Registro de ingresos de caja general.
- Registro de ingresos, comprobante de pago, planilla de movilidad de caja chica.
- Seguimiento a través de consultas y reportes.
- Utiliza tecnología cliente / servidor.
- Cuenta con interfaz al SIAF.

**Estrategia de Recuperación**

Se cuenta con el backup de la información del sistema el cual tiene una programación de 3 veces al día. La misma que se resguardada en los servidores de la entidad y en cintas que lleva el proveedor de resguardo cada mes.

De ocurrir un siniestro existe la necesidad de contar con el apoyo del sectorista asignado por el Ministerio de Economía y Finanzas (MEF).

**Tiempo de Recuperación**

Tiempo de recuperación promedio: 4 horas

| | |
|---|---|
| La plataforma tecnológica del sistema SIGA se encuentra respaldada en un servidor físico ubicado en Centro de Datos de INVERMET.<br><br>En caso de una pérdida del servidor en nuestra entidad, se prepara un nuevo servidor, se instala la base de datos, se realiza la coordinación con el MEF para que habiliten los parámetros de conexión de la base de datos, se realiza las configuraciones y pruebas. | |
| **Observaciones** | |

## *3.- Sistema de Valores en Custodia*

| | |
|---|---|
| **Responsable(s):**<br>Coordinador de la UFINF<br>Especialista en Sistemas de Información | **Ubicación Física**<br>Sede: Lampa |

**Descripción**

Permite registrar, controlar y brindar seguimiento a los valores en custodia - Carta Fianza, producto de los contratos firmados en la Oficina de Abastecimiento, Servicios Generales y Control Patrimonial; asimismo, permite la apertura, control y seguimiento de la Caja Chica otorgada a la Oficina de Tesorería y Gerencia General, así como también, permite registrar la rendición correspondiente.

| | |
|---|---|
| **Estrategia de Recuperación**<br><br>Se guardan las fuentes en un repositorio free en nube BUT BUCKET, en la entidad se realiza snapshot de los servidores virtualízales.<br><br>En cuanto a la base de datos, de ocurrir un problema en el motor de base de datos, se procederá a realizar la restauración y recuperación de la base de datos a partir del último backup realizado.<br><br>En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia de un mes. | **Tiempo de Recuperación**<br><br>Dependiendo de la complejidad de la recuperación, el tiempo es de 30 minutos a 3 horas aproximadamente.<br><br>Para este problema se tendría un tiempo aproximado de 5 días de recuperación adicionando infraestructura. |
| **Observaciones** | |

## *4.- Sistema de Boletas de Pago en Línea*

| **Responsable(s):**<br>Coordinador de la UFINF<br>Especialista en Sistemas de Información | **Ubicación Física**<br>Sede: Lampa |
|---|---|

**Descripción**

- Optimizar los procesos de registro, entrega, almacenaje y custodia de las boletas de pago de los servidores públicos.
- Mejorar la experiencia de los servidores públicos a través de la consulta y obtención de sus boletas de pago mediante la plataforma.

| **Estrategia de Recuperación**<br>Se guardan las fuentes en un repositorio free en nube BUT BUCKET, en la entidad se realiza snapshot de los servidores virtuales.<br>En cuanto a la base de datos, de ocurrir un problema en el motor de base de datos se procederá a realizar la restauración y recuperación de la base de datos a partir del último backup realizado.<br>En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia de un mes. | **Tiempo de Recuperación**<br>Dependiendo de la complejidad de la recuperación, el tiempo es de 30 minutos a 3 horas aproximadamente. |
|---|---|

**Observaciones**

## *5.- Sistema de Valorizaciones*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Especialista en Sistemas de Información | Sede: Lampa. |

**Descripción**

Permite la automatización del proceso de control y pago de valorizaciones y la digitalización de la información para reducir tiempos y optimizar las operaciones de pago de las valorizaciones.

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| Se guardan las fuentes en un repositorio free en nube BUT BUCKET, en la entidad se realiza snapshot de los servidores virtualízales<br>En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia. | Dependiendo de la complejidad de la recuperación, el tiempo es de 30 minutos a 3horas aproximadamente |

**Observaciones**

## *6.- Sistema de Trámite Documentario*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Especialista en Sistemas de Información | Sede: Lampa. |

**Descripción**

El propósito principal del sistema de trámite documentario, es brindar soporte a los procesos misionales, gerenciales y de apoyo INVERMET, gestionando todo el ciclo de vida de los trámites.

El sistema brinda el soporte en todas las fases de los expedientes, desde el ingreso por la mesa de partes o de la creación en una unidad orgánica hasta el archivado en una de las plataformas de archivo.

Los objetivos principales de este sistema son:

- Llevar un registro actualizado de los trámites, anexos e informativos que ingresan o se generan en INVERMET.
- Establecer un control efectivo de la recepción de documentos en INVERMET, con el propósito de localizar en forma inmediata los diferentes trámites, anexos e informativos que ingresan o se generan en la institución.

| Estrategia de Recuperación | Tiempo de Recuperación |
|---|---|
| • Si ocurriese un problema en el servidor de físico de base de datos de producción (Oracle), la entidad cuenta con un servidor virtual de contingencia en la misma sede.<br>• En cuanto a la base de datos, de ocurrir un problema en el motor de base de datos se procederá a realizar la restauración y recuperación de la base de datos a partir del último backup realizado.<br>• En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia de un mes.<br>• Si ocurriese un problema en el servidor de base de datos digital (open km) se tiene previsto implementar un servidor virtual de contingencia para la solución de open km que involucra los archivos de configuración y licenciamiento.<br>• Si ocurriese un problema en el servidor de base de datos digital (open km) (Servidor de almacenamiento de la información) se restauraría el sistema en otro servidor de almacenamiento. | El tiempo de recuperación promedio debería ser de 1 hora |
| **Observaciones** | |

## *7.- Portal Web Institucional*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Especialista en Sistemas de Información | Sede: Lampa |

**Descripción**

El Portal Web Institucional de INVERMET es una plataforma estructurada de acceso público, con información del acontecer económico nacional, útil para las unidades ejecutoras, profesionales,estudiantes y al público en general.

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia. | Dependiendo de la complejidad de la recuperación, el tiempo es de 30 minutos a 3 horas aproximadamente |

**Observaciones**

## *8.- Sistema de Fedatarios*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Especialista en Sistemas de Información | Sede: Lampa |

**Descripción**

Es una herramienta que permite automatizar el proceso que realiza el fedatario. Dicha herramienta permitirá, mediante el uso de la firma digital, comprobar y autenticar/certificar digitalmente un documento para su empleo en los procedimientos de la entidad o para el uso que requiera darle el administrado,

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| En el caso de ocurrir un siniestro mayor con pérdida de los servidores físicos de la entidad, se tiene un backup de la base de datos de producción con el servicio de veritas de vigencia. | Dependiendo de la complejidad de la recuperación, el tiempo es de 30 minutos a 3 horas aproximadamente |

**Observaciones**

## *9.- Servicio de Directorio Activo (MS Active Directory)*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Analista de Sistemas | Sedes: Lampa |

**Descripción**

El Servicio de Directorio Activo de INVERMET tiene implementado a nivel funcional de dominio y de bosque: INVERMET.GOB. PE sobre Windows Server 2008 R2.

Se cuenta con unidades organizativas estructuradas y políticas de grupos configuradas que restringen o brindan acceso a los recursos de red. INVERMET.

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| Los controladores de dominio cuentan con contingencia local de alta disponibilidad (en el Centros de Cómputo de INVERMET). | Dependiendo del escenario, esta recuperación puede demorar 1 hora en promedio. |

**Observaciones**

## *10.- Servicio de Almacenamiento*

| **Responsable(s):** | **Ubicación Física** |
|---|---|
| Coordinador de la UFINF<br>Analista de Sistemas | Sede: Lampa. |

**Descripción**

El servicio de almacenamiento de datos dedicados de INVERMET permite compartir la capacidad de almacenamiento del servidor principal para todas las aplicaciones y servicios de TI críticos y sensibles de INVERMET.

| **Estrategia de Recuperación** | **Tiempo de Recuperación** |
|---|---|
| Se tiene una contingencia local que cubriría el 70 % del servicio aproximadamente. | Aproximadamente cuatro (4) horas, dependiendo del escenario en que se suscita el incidente. |

**Observaciones**

## Anexo 6: Lista de tareas para reinicio de los sistemas informáticos

En el siguiente cuadro se muestran las tareas a ejecutar sobre las plataformas de TI necesarias para volver a poner en funcionamiento cada uno de los sistemas informáticos.

| Ít. | Sistema informático | Descripción de la tarea | Responsable |
|---|---|---|---|
| 1 | Sistema Integrado de Administración Financiera (SIAF) | 1. Levantar servidor de base de datos.<br>2. Levantar servidor de aplicaciones. | Analista de Sistemas |
| 2 | Sistema Integrado de Gestión Administrativa (SIGA) | 1. Levantar servidor de base de datos.<br>2. Levantar servidor de aplicaciones. | Analista de Sistemas |
| 3 | Sistema de Valores en Custodia | 1. Levantar servidor de base de datos.<br>2. Levantar servidor de aplicaciones. | Especialista en Sistemas de Información |
| 4 | Sistema de Boletas de Pago en Línea | 1. Levantar servidor de base de datos.<br>2. Levantar servidor de aplicaciones. | Especialista en Sistemas de Información |
| 5 | Sistema de Valorizaciones | 1. Levantar servidor de base de datos.<br>2. Levantar servidor de aplicaciones. | Especialista en Sistemas de Información |
| 6 | Sistema de Trámite Documentario | 1. Levantar servidor de base de datos.<br>2. Levantar servidores de aplicaciones JBOSS.<br>3. Levantar servidor de aplicaciones SISCOMEF. | Especialista en Sistemas de Información |
| 7 | Portal Web Institucional | 4. Levantar servidores de base de datos.<br>5. Levantar servidores de aplicaciones.<br>6. Levantar servidor de aplicaciones | Especialista en Sistemas de Información |
| 8 | Sistema de Fedatarios | 7. Levantar servidores de aplicaciones JBOSS.<br>Levantar servidor de aplicaciones | Especialista en Sistemas de Información |

| | | | |
|---|---|---|---|
| 09 | Servicio de directorio (MS Active Directory) | 1. Levantar servidor AD.<br>2. Levantar nodo 1 de Exchange.<br>3. Levantar nodo 2 de Exchange. | Analista de Sistemas |
| 10 | Servicios de almacenamiento, respaldo y recuperación de datos | 1. Levantar sistema de almacenamiento<br>2. Levantar servidor Vbackup.<br>3. Levantar servidor de reportes.<br>4. Activar las unidades de cinta. | Analista de Sistemas |
| 11 | Servicios de red y comunicaciones | 1. Levantar conmutadores centrales (*core switch*).<br>2. Levantar conmutadores de borde (*border switch*).<br>3. Levantar equipos de seguridad perimetral: antispam, firewall, controlador de enlaces.<br>4. Levantar enrutadores (*routers*) de enlaces WAN. | Analista de Sistemas |

## Anexo 7: Prioridad de recuperación de las plataformas tecnológicas

En casos de eventos que afecten simultáneamente a la disponibilidad de varias de las plataformas tecnológicas que brindan soporte a los sistemas informáticos considerados en la contingencia, para la recuperación respectiva se deberá tomar en cuenta el orden de prioridad que se muestra a continuación, entendiéndose como tal, la secuencia de encendido de dichas plataformas:

- Equipos de red (*networking*): conmutador central (*core switch*), conmutador de borde (*border switch*), antispam, cortafuegos (*firewall*), controlador de enlaces (*link controller*), redes LAN, SAN y WAN.
- Sistema de Almacenamiento.
- Servidores Active Directory.
- Plataforma de VCenter
- Servidor de base de datos.
- Servidor de Trámite Documentario

## Anexo 8: Lista de tareas para verificación del retorno a condiciones normales

A continuación, se presenta la relación de tareas que el personal de la UFINF de INVERMET, debe realizar para verificar que la provisión de los sistemas informáticos ha retornado desde el Centro de Procesamiento de Datos de Contingencia (servicio de *hosting*) al Centro de Cómputo de INVERMET.

| N° | Componente | Descripción de la tarea | Responsable |
|---|---|---|---|
| 1 | Configuración del enlace de Internet | 1. Validación de servicios por IP pública.<br>2. Prueba de acceso al Portal de INVERMET.<br>3. Prueba de envío y recepción de correoelectrónico.<br>4. Prueba de navegación por internet.<br>5. Verificación de registros en los servidores.<br>6. Validación de las aplicaciones externas. | - Coordinadora de la UFINF.<br>- Analista de Sistemas |
| 2 | Servicios de seguridad perimetral | 1. Realizar un ataque de *SQL Injection* a alguna página web publicada para probar el funcionamiento del IPS.<br>2. Probar navegación a página web restringidapara probar filtro de contenido.<br>3. Revisar la cabecera de un correo electrónico recibido y enviado para probar su paso por el *antispam*. | - Coordinadora de la UFINF.<br>- Analista de Sistemas |
| 3 | Servicios en plataforma Windows/Linux | 1. Probar la conectividad.<br>2. Validar servicios de aplicaciones y bases de datos por cada una de las máquinas virtuales que se encuentran en contingencia<br>3. Validar conectividad de aplicaciones con labase de datos. | - Coordinadora de la UFINF.<br>- Analista de Sistemas de Información |