FONCODES
Firma Digital
Firmado digitalmente por VILA HIDALGO Hugo Priscilio FAU 20509139700 hard
Motivo: Soy el autor del documento
Fecha: 24.08.2020 11:48:11 -05:00

Resolución de Dirección Ejecutiva

Nº 000070-2020-FONCODES/DE

Lima, 24 de agosto de 2020.

VISTO:

El Memorando N° 000159-2020-MIDIS-FONCODES/UTI de la Unidad de Tecnologías de la Información, el Informe N° 000304-2020-MIDIS/FONCODES/UPPM de la Unidad de Planeamiento, Presupuesto y Modernización, el Informe Nº 000122-2020-MIDIS-FONCODES/UAJ de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, a través de la Ley N° 29792, se crea el Ministerio de Desarrollo e Inclusión Social, determinándose su ámbito, competencias, funciones y estructura orgánica básica; señalando además en su Tercera Disposición Complementaria Final, la adscripción a dicho Ministerio, entre otros programas, la del Fondo de Cooperación para el Desarrollo Social (en adelante, Foncodes);

Que, el Manual de Operaciones de Foncodes, aprobado mediante la Resolución Ministerial N° 228-2017-MIDIS, establece en los literales h) e i) del artículo 9 que la Dirección Ejecutiva tiene la facultad de aprobar, modificar y derogar directivas, reglamentos y otras normas técnico-operativas o administrativas internas que requiera el programa para su funcionamiento, así como emitir Resoluciones de Dirección Ejecutiva en asuntos de su competencia;

FONCODES
V°B° Digital
Firmado digitalmente por GONZALES INGA Ruth Janen FAU 20509139700 soft
Motivo: Doy V° B°
Fecha: 24.08.2020 09:30:16 -05:00

Que, el citado Manual de Operaciones, establece en los literales a) y g) del artículo 21 como funciones de la Unidad de Tecnologías de la Información, la de elaborar, proponer, ejecutar, monitorear y evaluar los planes estratégicos, de gestión y operativos para el desarrollo de las tecnologías de la información en el Programa Social, alineándolos a los objetivos, políticas y lineamientos dictados por la alta dirección, el sector y los órganos de Gobierno rectores en Tecnologías de la Información, y aplicar las recomendaciones y levantar las observaciones realizadas por el Órgano de Control Interno y auditoría externa, como resultado de las acciones de control realizadas al Programa Social en materia de tecnologías de la información;

Que, mediante la Resolución de Dirección Ejecutiva N° 150-2018-FONCODES/DE, se aprobó el Procedimiento N° 86-2018-FONCODES/UPPM-CROM “Control de Documentos Normativos”, que tiene como objetivo, establecer las disposiciones para la elaboración, actualización y control de los documentos normativos en sus etapas de acciones previas, elaboración, revisión, aprobación, distribución, registro e implementación;

FONCODES
Firma Digital
Firmado digitalmente por RENGIFO NAKAMA Rocio Marisol FAU 20509139700 hard
Motivo: Doy V° B°
Fecha: 24.08.2020 08:20:26 -05:00

Que, mediante la Ley N° 28716, Ley de Control Interno de las entidades del Estado se establecen las normas para regular la elaboración, aprobación, implantación funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos con acciones y actividades de control previo, simultáneo y posterior, contra los actos y prácticas indebidas o de corrupción, promoviendo al debido y transparente logro de los fines, objetivos y metas institucionales;

Que, mediante la Resolución de Contraloría General N° 320-2006-CG se aprobaron las "Normas de Control Interno", de aplicación a las entidades del Estado conforme a lo establecido por la citada Ley N° 28716, Ley de Control Interno de las entidades del Estado, con la finalidad de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública, en relación a la protección del patrimonio público y al logro de los objetivos y metas institucionales;

FONCODES
V°B° Digital
Firmado digitalmente por CALMET WILLIAMS Jean Pierre FAU 20509139700 hard
Motivo: Doy V° B°
Fecha: 23.08.2020 14:25:49 -05:00

Que, en el séptimo comentario del acápite 3.10, inciso 3 del numeral III, de las Normas Básicas para las Actividades de Control Gerencial, denominado “Controles para las Tecnologías de la Información y Comunicaciones”, se establece que el adecuado ambiente de control en los sistemas informáticos, requiere que éstos sean preparados y programados con anticipación para

FONCODES
Fondo de Cooperación para el Desarrollo Social
Firma Digital
Firmado digitalmente por VILA HIDALGO Hugo Priscilio FAU 20509139700 hard
Motivo: Soy el autor del documento
Fecha: 24.08.2020 11:48:11 -05:00

mantener la continuidad del servicio, para lo cual se debe elaborar, mantener y actualizar periódicamente un plan de contingencia, debidamente autorizado y aprobado por el titular o funcionario designado, donde se estipule procedimientos previstos para la recuperación de datos, con el fin de afrontar situaciones de emergencia;

Que, la Norma Técnica Peruana "NTP-ISO/EC 27001:2014 Tecnologías de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2ª Edición, aprobada mediante la Resolución Ministerial N° 004-2016-PCM, en el acápite a.17.1 del Anexo A denominado "Aspectos de seguridad de la información en la gestión de continuidad del negocio", señala que la organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información, durante una situación adversa;

Que, con la Resolución de la Dirección Ejecutiva N° 100-2013-FONCODES/DE, se aprobó el "Plan de Contingencia de la Coordinación de Sistemas de Información (CSI) 2013", que tiene como finalidad establecer los procedimientos que permitan reducir el riesgo de siniestro de cualquier índole, y afrontar eventos que amenazan la continuidad de operaciones informáticas de Foncodes;

Que, mediante la Memorando N° 000159-2020-MIDIS/FONCODES/UTI, la Unidad de Tecnologías de la Información remite a la Unidad de Planeamiento, Presupuesto y Modernización la propuesta del "Plan de Contingencias de Tecnologías de la Información 2020-2021", de acuerdo a la Recomendación N° 12 del Informe de Auditoría Financiera al Ejercicio 2018- Foncodes, elaborado por la SOA Consorcio Urbano Toledo y Asociados S.C., Ventosilla, Vásquez y Asociados S.C.R.L., Camac Morales S.C. y Víctor Piscoya y Asociados Contadores Públicos, que tiene como objetivo mostrar y adiestrar al personal de la Unidad de Tecnologías de la Información (UTI), en un plan que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de Tecnologías de la Información en Foncodes, ante eventos previsibles que amenazan a la institución, reduciendo los riesgos y mitigando los efectos adversos, asimismo logra un manejo operativo eficiente ante una eventual emergencia producida en Foncodes que permita reducir los riesgos para el personal, visitante y activos, proteger las instalaciones, evitar o limitar la propagación del siniestro, evitar o reducir los riesgos a los ambientes vecinos y evitar la contaminación del medio ambiente;

Que, con el Informe N° 000304-2019-MIDIS/FONCODES/UPPM, la Unidad de Planeamiento, Presupuesto y Modernización a través del Coordinador de Racionalización, Organización y Métodos, emite la conformidad al Plan N° 27-2020-FONCODES/UTI "Plan de Contingencias de Tecnologías de la Información, respecto a los criterios de consistencia y coherencia que todo documento normativo debe cumplir, precisando que el citado proyecto normativo cumple con las disposiciones establecidas en el Procedimiento N° 86-2018-FONCODES/UPPM-CROM "Control de Documentos Normativos", aprobado mediante la Resolución de Dirección Ejecutiva N° 150-2018-FONCODES/DE, y recomienda proseguir con el trámite para su respectiva aprobación;

Que, mediante el Informe N° 000122-2020-MIDIS/FONCODES/UAJ, la Unidad de Asesoría Jurídica, de acuerdo a los antecedentes y normativa aplicable, considera procedente en sus aspectos legales y formales, la emisión de la Resolución de Dirección Ejecutiva mediante la cual se apruebe el Plan N° 27-2020-FONCODES/UTI "Plan de Contingencias de Tecnologías de la Información 2021-2021", propuesto por la Unidad de Tecnologías de la Información, que cuenta con la conformidad de la Unidad de Planeamiento, Presupuesto y Modernización;

Que, estando a los considerandos precedentes resulta necesario emitir el acto administrativo que apruebe el Plan N° 27-2020-FONCODES/UTI "Plan de Contingencias de Tecnologías de la Información 2020-2021" y se deje sin efecto el Plan de Contingencia de la Coordinación de Sistemas de Información (CSI) 2013, aprobado por la Resolución de la Dirección Ejecutiva N° 100-2013-FONCODES/DE, de fecha 13 de agosto de 2013;

Con el visado de conformidad, de acuerdo a sus competencias, de la Unidad de Tecnologías de la Información, la Unidad de Planeamiento, Presupuesto y Modernización y, la Unidad de Asesoría Jurídica;

FONCODES
Fondo de Cooperación para el Desarrollo Social
Firma Digital
Firmado digitalmente por VILA HIDALGO Hugo Priscilio FAU 20509139700 hard
Motivo: Soy el autor del documento
Fecha: 24.08.2020 11:48:11 -05:00

De conformidad con el Decreto Ley N° 26157, Ley del Fondo de Nacional de Compensación y Desarrollo Social - Foncodes, la Ley N° 29792, Ley de creación, organización y funciones del Ministerio de Desarrollo e Inclusión Social, y de acuerdo a las facultades contenidas en el Manual de Operaciones de Foncodes, aprobado mediante la Resolución Ministerial N° 228-2017-MIDIS;

SE RESUELVE:

ARTÍCULO 1.- Aprobación del Plan

Aprobar el Plan N° 27-2020-FONCODES/UTI "Plan de Contingencias de Tecnologías de la Información 2020-2021", que forma parte integrante de la presente Resolución.

ARTÍCULO 2.- **Dejar sin efecto**

Déjese sin efecto el "Plan de Contingencia de la Coordinación de Sistemas de Información (CSI) 2013", aprobado por la Resolución de la Dirección Ejecutiva N° 100-2013-FONCODES/DE de fecha 13 de agosto de 2013.

ARTÍCULO 3.- Disposición

Disponer que la Unidad de Tecnologías de la Información, adopte las acciones necesarias para el debido cumplimiento de la presente Resolución.

ARTÍCULO 4.- Notificación

Encargar a la Unidad de Administración que disponga las acciones necesarias para la debida y oportuna notificación de la presente Resolución a las Unidades Orgánicas y Unidades Territoriales.

ARTÍCULO 5.- Publicación

Disponer la publicación de la presente Resolución en el portal institucional de Foncodes (www.foncodes.gob.pe).

REGÍSTRESE Y COMUNÍQUESE.

Documento firmado digitalmente

……..

HUGO P. VILA HIDALGO
DIRECTOR EJECUTIVO
FONDO DE COOPERACIÓN PARA EL DESARROLLO SOCIAL

PLAN N.° 27-2020-FONCODES/UTI

PLAN DE CONTINGENCIAS DE TECNOLOGÍAS DE LA INFORMACIÓN 2020-2021

RUBRO	CARGO / UNIDAD ORGÁNICA	FIRMA
Elaborado por:	Oficial de Seguridad de la Información Juan Carlos Reátegui Morales	FONCODES Firma Digital Firmado digitalmente por REATEGUI MORALES Juan Carlos FAU 20509139700 soft Motivo: Soy el autor del documento Fecha: 22.08.2020 21:36:54 -05:00
Revisado por:	Jefe de Unidad de Tecnologías de la Información Jean Pierre Calmet Williams	FONCODES Firma Digital Firmado digitalmente por CALMET WILLIAMS Jean Pierre FAU 20509139700 hard Motivo: Soy el autor del documento Fecha: 22.08.2020 21:42:07 -05:00
	Coordinador de Racionalización y Organización y Métodos Martín Vidalón Sirlupu	FONCODES Firma Digital Firmado digitalmente por VIDALON SIRLUPU Martin Harold FAU 20509139700 hard Motivo: Soy el autor del documento Fecha: 22.08.2020 22:05:17 -05:00
Aprobado por:	Director Ejecutivo Hugo Vila Hidalgo	FONCODES Firma Digital Firmado digitalmente por VILA HIDALGO Hugo Priscilo FAU 20509139700 hard Motivo: Soy el autor del documento Fecha: 23.08.2020 13:46:46 -05:00

ÍNDICE

I. Introducción 3
II. Finalidad 4
III. Objetivo....4
IV. Alcance 5
V. Base Legal....5
VI. Política 5
VII. Definiciones 5
VIII. Responsables 6
IX. Aspectos Básicos a Considerar 6
X. Gestión del Plan de Contingencias.....6
XI. Plan de Respaldo (Medidas de Prevención, Protección y Mitigación). 8
XII. Plan de Ejecución (Emergencia)....14
XIII. Plan de Recuperación 20
XIV. Activación del Plan de Contingencias....26
XV. Disposiciones Complementarias....28
XVI. Referencias Bibliográficas 29
XVII. Anexos....29
Anexo 1.- Lista de Contactos....30
Anexo 2.- Teléfonos de Emergencia....31
Anexo 3.- Términos y Definiciones 31

I. Introducción

El Fondo de Cooperación para el Desarrollo Social (Foncodes) es un programa nacional del Ministerio de Desarrollo e Inclusión Social (MIDIS) que trabaja en la generación de mayores oportunidades económicas sostenibles de los hogares rurales pobres extremos, facilitando la articulación entre los actores privados del lado de la demanda y de la oferta de los bienes y servicios que se requieren para fortalecer los emprendimientos de estos hogares, contribuyendo a la reducción de los procesos de exclusión que determinan que estos hogares no puedan articularse a dichos mercados.

La estrategia de desarrollo de capacidades para la generación de ingresos autónomos toma en cuenta lo siguiente:

- El desarrollo de capacidades para el fortalecimiento de los sistemas de producción familiar y la gestión de emprendimientos como ejes de inserción en los mercados, que posibiliten el aprendizaje, la apropiación y la innovación de tecnologías como vehículos para la generación de oportunidades.

- El acceso de los hogares a los servicios de infraestructura económica productiva para mejorar su productividad y viabilizar procesos de inserción.

- La mejora de las capacidades de gestión de los gobiernos locales, la participación y concertación ciudadana, orientada a la promoción de alternativas sostenibles de generación de oportunidades económicas para los hogares rurales en situación de extrema pobreza y a la mejora de la inversión pública en infraestructura necesaria para sustentar y potenciar los emprendimientos de los hogares rurales.

A través del tiempo las Tecnologías de la Información (TI) se han establecido como un elemento fundamental de las operaciones del Foncodes. Actualmente los servicios como acceso a Internet, correo electrónico, intranet, bases de datos, impresión y almacenamiento de archivos, comunicaciones y los aplicativos que dan soporte al "core[1]" del negocio de Foncodes, son críticos para el cumplimiento de su misión institucional.

El plan de contingencia de sistemas de información se encuentra diseñado en el marco de la política de seguridad del Foncodes[2] y continuidad operativa, en consecuencia, se toman las previsiones necesarias para modificar los procedimientos establecidos en el presente plan.

[1] "Core" es sinónimo de núcleo o esencia.
[2] Conforme los lineamientos de Seguridad de la Información del MIDIS (Resolución Ministerial N.° 028-2019-MIDIS).

Los cambios que ocurran en la infraestructura de Tecnología de Información y los procesos de la Institución, deberán reflejarse en el Plan de Contingencias y debe actualizarse en base al proceso siguiente:

- Conducir el análisis de riesgo en las operaciones
- Identificar controles preventivos
- Desarrollar estrategias de recuperación
- Revisar y formular la política del plan de contingencia
- Conducir pruebas, entrenamiento y ejercicios

Este documento será revisado y actualizado periódicamente, la versión actual es al 27 de julio del 2020.

II. Finalidad

Reducir el riesgo de siniestro de cualquier índole y afrontar eventos que amenazan la continuidad de operaciones informáticas que apoyen el cumplimiento de la misión del Fondo de Cooperación para el Desarrollo Social - Foncodes.

III. Objetivo.

Establecer normas y procedimientos para afrontar situaciones adversas que se presenten en los sistemas de información, equipos de cómputo y de comunicación de Foncodes, que permita garantizar la continuidad de las operaciones de Tecnologías de Información (TI), reduciendo sus riesgos y mitigando los efectos adversos.

Este plan de contingencias sigue el ciclo de vida iterativo PHVA[3] y nace de un análisis de riesgo donde se identifica aquellas amenazas que afectan a la continuidad del negocio.

Asimismo, lograr un manejo operativo eficiente ante una eventual emergencia producida en Foncodes que permita:

- Reducir los riesgos para el personal, visitante y activos.
- Proteger las instalaciones.
- Evitar o limitar la propagación del siniestro.
- Evitar o reducir los riesgos a los ambientes vecinos.
- Evitar la contaminación del medio ambiente.

Volver las operaciones rápidamente, al estado inicial antes de suceder el siniestro.

[3] PHVA: Planificar - Hacer - Verificar - Actuar.

IV. Alcance

Las operaciones informáticas de Foncodes Sede Central, Anexos de la Sede Central y Unidades Territoriales.

V. Base Legal

- Ley N.° 29664, Ley que Crea el Sistema Nacional de Gestión de Desastres (SINAGERD).
- Ley N.° 29733, Ley de Protección de Datos Personales y su reglamento, aprobado por Decreto Supremo N.° 003-2013-JUS.
- Decreto Supremo Nº 013-2003-PCM, Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.
- Resolución de Contraloría General N.° 320-2006-CG, Aprobar las Normas de Control Interno.
- Resolución Ministerial N.° 028-2015-PCM, Aprueba los lineamientos para la Gestión de Continuidad Operativa en las entidades públicas en los tres niveles de Gobierno, específicamente respecto al Plan de Recuperación de los Servicios de Tecnología de Información.
- Resolución Ministerial N.° 004-2016-PCM, Apruébese 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 Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N.° 028-2019-MIDIS, Aprobar los Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social.
- Resolución de Dirección Ejecutiva Nº 179-2019-FONCODES/DE, "Procedimiento de Gestión del Riesgo".
- Resolución de Dirección Ejecutiva Nº 19-2020-FONCODES/DE, "Procedimiento de Detección de anomalías e incidencias en los servicios de tecnologías de información que afecten la seguridad informática".

VI. Política

En caso de interrupción de todo o parte de los servicios información se utilizarán las medidas disponibles para restituir la operatividad en el menor plazo posible, el cual se dará prioridad a la Dirección Ejecutiva, Unidad de Administración, Unidades de Línea y Sistemas a Nivel Nacional.

VII. Definiciones

Ver Anexo 3. Términos y Definiciones.

VIII. Responsables

El jefe de la Unidad de Tecnologías de la Información, es el responsable del cumplimiento del presente plan, de delegar en el personal de su unidad los detalles pertinentes, y de validar el presente documento con el Comité de Gobierno Digital.

El jefe de la Unidad Territorial el responsable de cumplir el presente plan en las Unidades Territoriales.

IX. Aspectos Básicos a Considerar

La efectividad en la ejecución de este documento, ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente que afecte la plataforma tecnológica, se fundamenta en los siguientes supuestos:

- Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- Los funcionarios y profesionales que ejecutan esta guía, y sus equipos, se encuentran disponibles y no han sido afectados por el desastre.
- El desastre no afectó simultáneamente el Data Center principal y el Data Center Alterno.
- El Data Center Alterno estará habilitado para cuando menos, un promedio de 15 usuarios concurrentes.
- Tener operativo las computadoras en Sede Central y Unidad Territorial, para que los servidores realicen trabajo remoto hasta que termine la emergencia.
- Solo el funcionario responsable activará el Plan de Contingencias.
- Se han realizado las pruebas de las estrategias y procedimientos al menos una vez al año, y han funcionado.
- Los funcionarios y profesionales responsables del Plan, han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

X. Gestión del Plan de Contingencias.

Se conoce como contingencia a un evento que es probable que ocurra, pero del cual no se tiene la certeza de que vaya a ocurrir. Una contingencia es por lo tanto un suceso posible con mayores o menores probabilidades de ocurrir.

Por esta razón, se dice que las contingencias como acontecimientos que pueden ser tanto espontáneos como provocados, ya que no están previstos.

Un plan de contingencia es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

Asimismo, se define como contingencia a la alteración de la continuidad operativa, que impacta en forma relevante en el desarrollo de un servicio considerado crítico, teniendo su origen en una falla de uno o varios componentes o de la interrupción de una tarea, sin estar necesariamente prevista.

El Plan de Contingencias, consta de tres planes:

- Plan de Respaldo.
- Plan de Emergencia.
- Plan de Recuperación.

El enfoque del presente Plan de Contingencias, es por escenarios tal como se muestra en la Tabla N.° 01 Escenarios considerados como contingencias.

Tabla N.° 01 Escenarios considerados como contingencias:

Escenario	Causas	
No Disponibilidad del Datacenter. **1**	Terremoto de Grado mayor a 8 de escala Richter.	
	Incendio de Local San Isidro	
	Aniego por daño en el servicio de agua y/o desagüe.	
	Atentado terrorista	
	Ciberataque	
Caída de la Infraestructura de Comunicaciones. **2**	Falla en el Switch Core	
	Falla en conexión de cableado	
	Falla en señal de comunicaciones	
	Falla en energía eléctrica.	
	Ciberataque	
Caída de Infraestructura de Servidores o Caída de Bases de Datos. **3**	No disponibilidad de servidor de Dominio	
	No disponibilidad de energía o aire acondicionado	
	Ciberataque	
Condiciones inseguras para el personal (Pandemias, epidemias, etc.) **4**	Atentado terrorista	
	Pandemia	
	Epidemia	
	Otras condiciones	

Fuente: Propia

XI. Plan de Respaldo (Medidas de Prevención, Protección y Mitigación).

Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

Contempla el desarrollo de un análisis de riesgo y acciones como:

- Revisión permanente de extintores.
- Simulacros de Sismo e Incendio.
- Realización, custodia y revisión de copias de respaldo (backup).
- Mantenimiento permanente del Data Center y los servidores de las Unidades Territoriales.
- Mantenimiento permanente de las comunicaciones (redes LAN y WAN) a los equipos informáticos y de los servidores de la Sede Central, la Molina y las Unidades Territoriales.
- Contar con computadoras operativas adicionales para utilizarlas ante un evento.

11.1. Objetivos

- Tener un Plan anticipado para que, llegado el momento de un siniestro, se pueda saber qué acciones tomar.
- Fortalecer la imagen de un Foncodes, seguro y resiliente.
- Coadyuvar a formar una cultura de seguridad y proactividad.
- Asegurar que las operaciones críticas de Tecnologías de Información que presta la UTI, no se interrumpan.

11.2. Alcance

El Plan de Respaldo trata de cómo se llevarán a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de sistemas, proyectos, y usuarios, tendrán sus propios Planes de Respaldo.

En términos generales se considera a la función de respaldo como una responsabilidad del usuario del servicio, la razón de esta asignación de responsabilidad es que, al producirse una emergencia, la principal actividad o responsabilidad del usuario es la de recuperación del bien o servicio de TI, ya que se considera, que tiene más opciones y flexibilidad que el proveedor del servicio.

En el Plan se considera a la UTI como proveedor de los servicios de Tecnologías de la Información (TI) y quien tiene como principal función la recuperación del servicio al menor tiempo posible. Si se logra esto, por definición no habrá desastre alguno.
En la Tabla N.° 02 Responsabilidades definidas para cada rol, se definen las tareas y los responsables.

Tabla N.° 02: Responsabilidades definidas para cada rol

ROL	ANTES DEL EVENTO (Respaldo)	DURANTE EL EVENTO (Emergencia)	DESPUES DEL EVENTO (Recuperación)
Líder de Contingencia	Velar por la actualización del Plan y recursos requeridos. Organizar y capacitar el Equipo de Contingencia.	Evaluar y activar el Plan y las estrategias de recuperación y contingencia. Liderar al Equipo de Contingencias.	Velar por la actualización del Plan acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción.
	Velar por el conocimiento y pruebas del Plan	Comunicar a la alta dirección sobre el estado de la operación y contingencia.	
	Gestionar para conseguir los recursos necesarios para el Plan.	Informar el momento en que opera en contingencia y que puede suceder con la prestación de servicio.	Informar a la alta dirección sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
	Comunicación a las personas que corresponda sobre la situación de contingencia.	• Liderar la operación bajo contingencia. • Comunicar a la dirección el desastre, interrupción o evento contingente. • Liderar el retorno a la normalidad.	
Líder de Infraestructura Líder de Redes y Comunicaciones y Líder de Atención al Usuario	Comunicar necesidades de ajustes.	Evaluar el desastre, interrupción o evento contingente.	Reportar los inconvenientes y oportunidades de mejora del Plan. Lecciones aprendidas. Evaluación de todas las contingencias que se tuvieron y se solucionaron para la mejora del plan.
	Participar en la ejecución de las pruebas de Plan.	En caso de no contar con un contrato de mantenimiento del equipo de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución.	
		Comunicar el evento al Líder del Plan.	
		• Verificar disponibilidad y notificar al personal requerido para atender el evento. • Ejecutar las guías de contingencia y recuperación. • Comunicar a los proveedores la activación de Plan. • Solicitar la corrección del componente afectado y realizar seguimiento de la solución. • Estar atentos para dar una correcta información a las personas que lo requieran. • Mantener informado al Líder del Plan.	
Líder de Seguridad	Coordinar actividades de entrenamiento, documentación y actualización del Plan.	• Proveer soporte a los profesionales especializados. • Notificar al proveedor del Centro	Actualizar el Plan de acuerdo con los inconvenientes y oportunidades de mejora

ROL	ANTES DEL EVENTO (Respaldo)	DURANTE EL EVENTO (Emergencia)	DESPUES DEL EVENTO (Recuperación)
	Coordinar las actividades de pruebas del Plan. Identificar los recursos requeridos para la operación del Plan.	de Cómputo Alterno (Si Aplica). • Gestionar el alistamiento y disponibilidad del Centro de Computo Alterno. • Coordinar con los responsables el desplazamiento al centro de Cómputo Alterno, de las personas que activaran la infraestructura. • Mantener informado al Líder del Plan.	encontrados.
Apoyo Logístico	Participar en la ejecución de las pruebas del Plan de Contingencia.	Participación permanente del apoyo logístico durante el evento	Reportar los inconvenientes y oportunidades de mejora del Plan.

Fuente: Propia.

11.3. Estrategias de respaldo

El Plan de Respaldo tiene las siguientes características:

11.3.1. Público

Todos los usuarios están debidamente informados de sus responsabilidades respecto al respaldo. El Oficial de Seguridad de Información es responsable de informarles periódicamente.

La frecuencia, el alcance de los bienes a respaldar (cuáles son los equipos informáticos y archivos electrónicos) y las tareas a realizar deben estar debidamente normados[4].

11.3.2. Respaldo de los trabajos individualizados y capacidad instalada medida

El Plan ha sido elaborado considerando respaldos por aplicativos y por trabajos, y está implícito en la responsabilidad individual de cada empleado. El Plan pone énfasis en la determinación de la capacidad de Respaldo para conocer los recursos necesarios para realizarlo. La capacidad calculada ha sido obtenida de diferentes fuentes informativas (usuarios, proveedores, librerías y directorios existentes).

El Plan ha sido elaborado considerando respaldos por aplicativos y por trabajos y cada trabajador es responsable de considerar los respaldos respectivos de su trabajo.

El Plan pone énfasis en la determinación de la capacidad de respaldo para conocer los recursos necesarios para realizarlo, considerando los respaldos de uso comunitario y los respaldos del uso de los trabajadores.

[4] Actualmente es a través de lo establecido en la Resolución de Dirección Ejecutiva N.° 030-2015-FONCODES-DE en donde se aprueba el Procedimiento para el Uso de Activos y Servicios Informáticos y Seguridad de la Información.

La capacidad calculada ha sido obtenida de diferentes fuentes informativas (usuarios, proveedores, librerías y directorios existentes).

11.3.3. Puntos importantes a considerar:

11.3.3.1. Identificar trabajos críticos.

Las tareas críticas son aquellas que deben realizarse en un determinado momento en particular y se necesitan para tomar decisiones vitales a nivel gerencial. Cada empleado es responsable de determinar cuáles son sus trabajos críticos y los momentos en que deben realizarlos.

11.3.3.2. Identifica la configuración crítica requerida.

Para cada tarea crítica el Plan de Contingencia identifica la configuración y entorno del sistema de respaldo requerido para su procesamiento. Este requerimiento incluye software, comunicaciones, datos y personal.

11.3.3.3. Identifica trabajos no relevantes.

En algunos casos particulares identificar trabajos no críticos o no relevantes, para poner su capacidad o recursos remanentes al servicio de las tareas críticas.

La Estrategia de Respaldo adoptada ha permitido identificar un sistema con una configuración adecuada y con suficiente capacidad para procesar las tareas críticas. El Plan de Contingencias, prevé recurrir a varias instalaciones similares en capacidad. (Sede La Molina, Unidades Territoriales con local propio).

11.3.3.4. Portabilidad

Será posible trasladar el procesamiento de tareas críticas y no críticas a las instalaciones de respaldo. Para ello se emplearán herramientas estándar y de uso común en el medio. (servidores, estaciones, medios de almacenamiento, equipos de comunicaciones, entre otros).
Contar con un soporte técnico permanente cuando los servidores tengan que realizar tareas críticas a través de trabajo remoto.

11.3.3.5. Procedimientos Manuales

Opcionalmente se considera a las operaciones manuales como una alternativa de respaldo para el procesamiento. No se descarta recurrir a ellas en caso de emergencia.

11.3.3.6. Otras Instalaciones por Convenio.

El Plan contempla la firma de convenio de asistencia recíproca con otras entidades que pertenecen al sector MIDIS. Ante la eventualidad de un desastre se dispondrá de instalaciones externas que permitirán restablecer el servicio.

11.3.3.7. Servicio de Procesamiento de Datos.

Opcionalmente se han identificado empresas del medio que brindan servicio de procesamiento de datos como una segunda alternativa a la recuperación.

11.3.3.8. Transmisión de comunicación por diferentes medios.

No se ha concentrado la transmisión de datos en un sólo proveedor o en un solo medio. Se cuenta con otros medios que pueden emplearse alternativamente como línea celular, WhatsApp, teléfono fijo, correo, entre otros.

11.3.3.9. Correspondencia a través de mensajería

Este medio de comunicación, como respaldo, continuará siendo útil y no se descarta en ningún momento su empleo.

11.3.3.10. Respaldo de datos vitales

En esta estrategia se incluyen todos los programas y datos que implican de una u otra manera algún riesgo para la normal operación de Foncodes, los planes y presupuestos, especificaciones de servicios, registros de sueldos, y aquellos que particularmente cada Unidad lo indique.

Todas las copias se obtendrán en formato estándar aplicable a cada Sistema Operativo. Por ninguna circunstancia se empleará software fuera del estándar. Todas las copias de respaldo se almacenarán en UTI o los locales que UTI disponga.

Dentro de las estrategias de respaldo, se incluyen los sistemas de información institucionales.

Todos los datos de los sistemas indicados se protegen y recuperan de acuerdo a los procedimientos de Respaldo y Recuperación.

En todos los sistemas se consideran los siguientes tipos de respaldo de los Datos Almacenados:

- **Respaldos Diarios.** - Se realizan diariamente al concluir cada jornada de labor. Se efectúan sobre todos los archivos vitales de cada aplicación.

- **Respaldos Semanales.** -Se realizan semanalmente al concluir cada semana de labor, el día viernes o sábado. Se efectúan sobre todos los archivos vitales de cada aplicación.

- **Respaldo Mensuales.** - Se realizan mensualmente al concluir cada mes de labor, el último día del mes. Se efectúan sobre todo en los discos de los Servidores.

- **Respaldo Especial**. -Se realizan eventualmente antes de realizar alguna operación especial de mantenimiento en previsión a posibles fallas durante la ejecución de procesos particulares.

11.3.3.11. Procedimientos:

Procedimientos de Respaldo y Recuperación. (RUA Nº 004-2016-MIDIS-FONCODES/UA.
Registro de las copias de Respaldo, almacenadas en las oficinas y en la instalación.

11.3.3.11.1. Servidores de las Unidades Territoriales: Generan un backup de manera diaria de su base de datos y de sus archivos de trabajo importantes y cada quince días lo remiten a la Sede Central para su verificación.

11.3.3.11.2. Servidores en entorno Web: los servidores Web generan archivos que concentran su información interna y que luego son respaldados, para cada aplicación se tiene un procedimiento especial para su restauración ante una contingencia requerida.

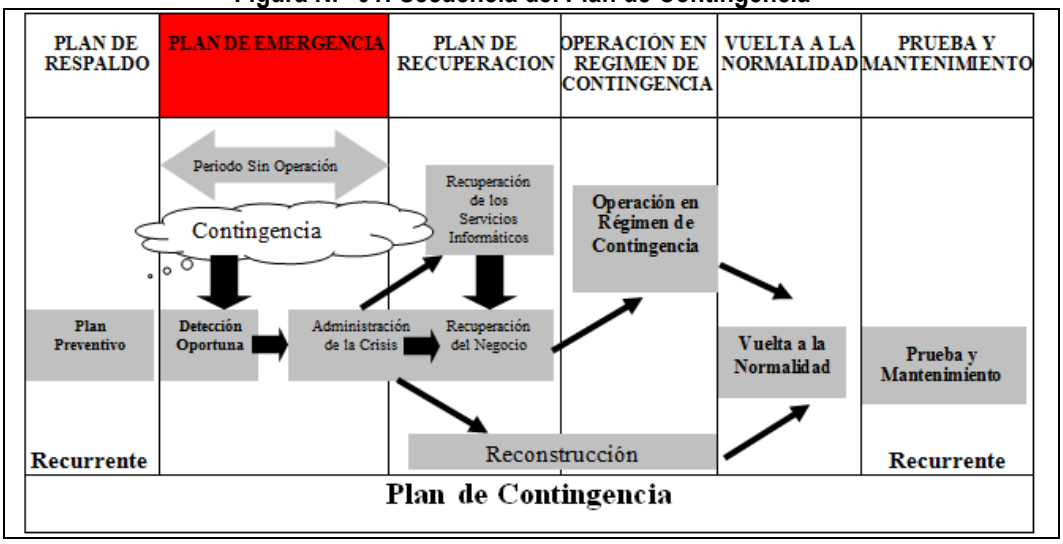
11.3.3.11.3. Servidores de correo electrónico: se generan respaldos semanales a las bases de datos que contienen los buzones de correo de electrónico.

11.3.3.11.4. Servidores de archivos: Se respalda diariamente (de lunes a viernes) la información de trabajo que las diferentes áreas han colocado en los servidores de archivos de la Sede Central.

11.3.3.11.5. Computadoras personales. las computadoras asignadas al personal, tienen carpetas en los servidores de Foncodes, lo cual es responsabilidad de los usuarios, a estos servidores se les hace backup periódicamente.

11.3.3.11.6. Documentación de los Sistemas. Toda la documentación digital de trabajo, se encuentra en los espacios de los servidores de archivos que se han definido para ello y es respaldada diariamente.

Figura N.° 01: Secuencia del Plan de Contingencia



Fuente: Propia.

XII. Plan de Ejecución (Emergencia).

12.1. Objetivos.

Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después.

Su finalidad es paliar los efectos adversos de la amenaza.

Contempla acciones como:

- Activación o pre contratos de alquiler de equipos informáticos.
- Apoyo de proveedores de servicios (Internet, energía eléctrica, custodia de backups, etc.).
- Restauración de copias de respaldo.
- Trabajos de usuarios a distancia (trabajo remoto).
- Reanudación de la actividad.

12.2. Alcance

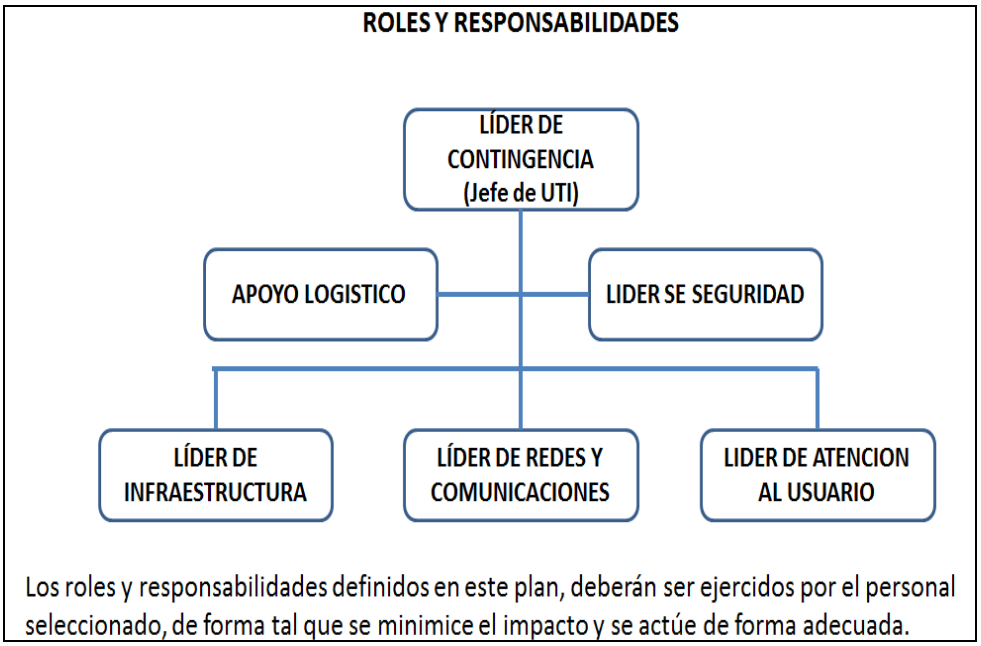
El Plan de emergencia de Foncodes, se ha desarrollado para afrontar las amenazas de acuerdo a la priorización que se ha asignado en cada caso.

12.3. Estrategias

Las estrategias adoptadas son:

- Contar con un Plan que contemple razonablemente las amenazas más relevantes que afectan a la institución en general y a la información en particular.
- Protección de recursos en un orden de importancias para proporcionar los servicios.
- Aprovechar toda la información disponible proveniente de los organismos de defensa gubernamentales y privados (INDECI, IMARPE, IGP, etc.).
- Asignación clara de roles y responsabilidades. (Ver Tabla N.° 02: Responsabilidades definidas para cada rol), considerando la estructura de la UTI, ver Figura N.° 02: Estructura jerárquica en el Plan de Contingencias.
- Tener un efectivo árbol de llamadas. (Ver Figura N.° 03: Árbol de llamadas en el Plan de Contingencias).
- Uso de medios preventivos automáticos de tecnología probada.
- Observación directa de las amenazas y su seguimiento de las mismas.
- Difusión de los Planes entre los trabajadores y su entrenamiento, mediante capacitaciones y simulacros.
- Asignar trabajos de manera remota, sin sobrecargar los equipos.

Figura N.° 02: Estructura jerárquica en el Plan de Contingencias



Fuente: Propia.

12.4. **Actividades de notificación, evaluación y activación de Plan de Contingencias**

Los usuarios deben reportar el incidente a la UTI cuando:

- No se puedan utilizar los sistemas de información
- No hay red de comunicaciones.
- No hay servicio de correo electrónico.
- No hay acceso a los archivos contenidos en los servidores.
- Cualquier otro evento de tecnología que afecte a la prestación del servicio.

12.5. **Criterios para declarar Contingencia y Notificación**

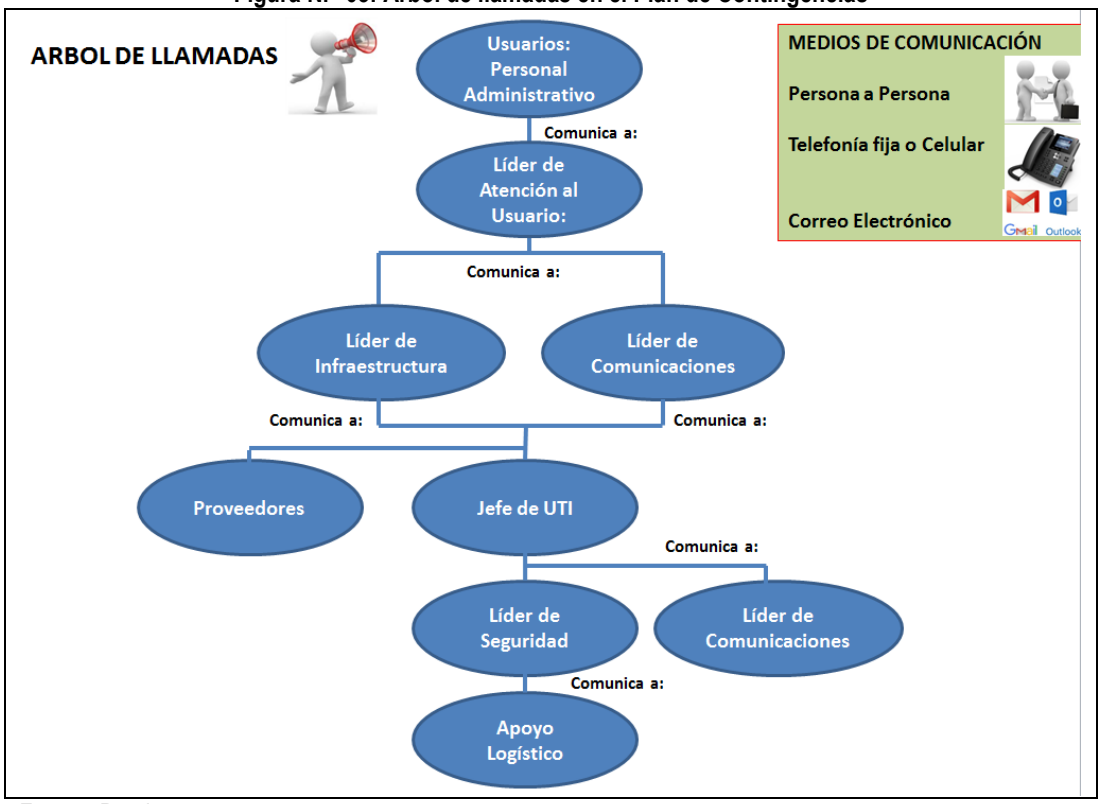
Los criterios para declarar la contingencia están condicionados a la ocurrencia de los siguientes escenarios:

a) No Disponibilidad del Datacenter
b) Caída de la Infraestructura de Comunicaciones
c) Caída de Infraestructura de Servidores o de Base de Datos.
d) Condiciones inseguras para el personal (Pandemias, epidemias, entre otras.).

El personal administrativo (vigilancia, servicios generales) debe reportar el incidente a UTI cuando:

- Suena la alarma del edificio de la Sede Central o Unidades Territoriales.
- Hay inundación en cualquier piso.
- Hay un conato de incendio en el piso cinco (5) donde está ubicado en Data Center.
- Cualquier otro evento que afecte o pueda afectar a los equipos informáticos.

Figura N.° 03: Árbol de llamadas en el Plan de Contingencias



Fuente: Propia.

El personal de la UTI encargado del monitoreo de la plataforma (infraestructura de técnica, infraestructura de comunicaciones, infraestructura de datos) deben reportar el incidente al jefe de la UTI o al Oficial de Seguridad de la Información.

- Se detecta caída de servicios.
- Se detecta mal funcionamiento de infraestructura critica (servidores, dispositivos de comunicaciones, bases de datos).
- Se disparen alarmas ambientales y otras contingencias que se coordinaría con la Dirección Ejecutiva, de quien depende la UTI jerárquicamente.

La UTI debe atender el incidente y se continúa con la ejecución de esta guía si:

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados. En cualquiera de los casos, debe escalarlo a los funcionarios responsables.

12.5.1. Evaluación de la magnitud e impacto del incidente:

El profesional especializado de la plataforma afectada, debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el Plan de Contingencias aplicables u otras soluciones potenciales.
- Tiempo estimado de solución del incidente.

Finalmente, comunicarse con el jefe de la Unidad de Tecnología de la Información (UTI) para informar los resultados del diagnóstico.

12.5.2. Activación del centro de cómputo alterno.

El jefe de la UTI, define si se activa o no el Centro de Cómputo Alterno, teniendo en cuenta los siguientes aspectos:

- Si el evento afectó considerablemente al Data Center Principal.
- Si la solución en el sitio dura más del tiempo definido en el punto de tolerancia.

En caso de que se active, el líder de infraestructura debe comunicar la activación al proveedor (de ser pertinente), teniendo en cuenta:

- Fecha y hora a partir de la cual se da inicio a la activación.
- Funcionarios de la entidad que estarían en el proceso de activación, para que se tramiten los permisos de acceso correspondientes.

El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Data Center Alterno, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones hacia el Data Center Alterno.
- Detención de la replicación de datos.
- Verificación de la disponibilidad de información en el Data Center Alterno.
- Activación servicio de controladores de dominio y sistema operativo en servidores.
- Activación servicio de bases de datos y aplicaciones.

El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el Data Center Alterno, teniendo en cuenta:

- Acceder a los sistemas de información.
- Realizar pruebas sobre los sistemas de información.

El jefe de la UTI, comunica el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.

12.5.3. Actividades paralelas.

El Líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:

Si es un evento que afectó las comunicaciones.

- Verificar el Switch de contingencia, en caso de falla en el Switch de core.
- Contactar al proveedor de comunicaciones, en caso de falla en router de conexión.

- Utilizar el switch del piso (u otro similar) como contingencia ante falla de un switch en un centro de cableado.
- Configurar el firewall de contingencia, en caso de falla del equipo principal.

Si es un evento que afectó la infraestructura de servidores:
- Activar el servidor de contingencia, anta falla del servidor de dominio.

Si es un evento que afectó la infraestructura de Bases de datos, Almacenamiento y Respaldo:
- Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de la base de datos, y borrado o pérdida de datos.

En caso que la falla afecte un equipo que no se encuentra en garantía o mantenimiento correctivo, el Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.

El jefe de UTI realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.

La Unidad de Administración realiza la contratación o compra de los servicios y equipos para la operatividad de Foncodes.

El Líder responsable de la plataforma afectada coordina la solución con el proveedor contratado.

12.5.4. Retorno a la normalidad

El jefe de la UTI comunica la solución del incidente a la entidad y en conjunto con los profesionales especializados, definen la estrategia de retorno a la normalidad, teniendo en cuenta:
- Fecha del retorno a operación normal.
- Consideraciones especiales a aplicar en el proceso de retorno.
- Consideraciones especiales con respectos a la recuperación de la información y mantener la integridad de los datos, cuando aplique.
- Sincronización entre los centros de cómputo, cuando se operó en el Data Center Alterno, si aplica.

El Oficial de Seguridad de Información, en conjunto con los funcionarios que participaron en la atención del incidente, documenta el incidente e identifican oportunidades de mejora para fortalecer el Plan de Contingencias.

Se realiza el cierre del incidente, interrupción mayor o evento contingente, y se continúa con la ejecución del procedimiento de acciones preventivas y correctivas del Sistema de Gestión de la Seguridad de la Información (SGSI).

12.6. Actividades de manejo de crisis

Una crisis, según la ISO 22301 es “una situación con un alto nivel de incertidumbre que afecta las actividades básicas y/o la credibilidad de la organización y requiere medidas urgentes”.

Las crisis están generadas por todos aquellos eventos inesperados e/o inevitables de carácter catastrófico que pueden afectar a los activos críticos, la estructura financiera, las personas e incluso la reputación, poniendo en peligro la propia supervivencia de la compañía, y que, siendo verdaderas, no siempre suponen la activación de un plan de continuidad operativa.

Las crisis no siempre implican interrupción de la actividad empresarial o amenazas directas a la vida, a la propiedad o a los activos, pero, sin embargo, casi siempre suponen un peligro para la reputación de una organización y su marca, incluso si es sólo a través de la necesidad de demostrar una fortaleza y liderazgo efectivo.

A continuación, se listan las actividades y consideraciones necesarias para el manejo de una crisis que afecte o pueda afectar la reputación, imagen u operación de Foncodes.

a) El jefe de la UTI comunica al Comité de Gobierno Digital y a la Alta Dirección, teniendo en cuenta los siguientes aspectos:
   - Sistemas y servicios afectados y operativos
   - Resultados del diagnóstico
   - Acciones realizadas antes, durante el evento
   - Tiempo estimado para normalización, teniendo en cuenta los protocolos
   - Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles durante la crisis y el retorno a la normalidad
   - Decisiones que debe tomar la alta dirección.

b) La Alta Dirección y el Comité de Gobierno Digital se establecen como un Equipo de Manejo de Crisis, quienes evalúan la crisis y el impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontar la crisis.

c) La Alta Dirección, a través de los voceros o funcionarios delegados, comunicará la crisis a nivel interno y externo, en caso de ser requerido, teniendo en cuenta los siguientes aspectos:
   - ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
   - ¿Qué información está en proceso de verificación e investigación?
   - ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
   - ¿Qué información se debe manejar al interior de la entidad?
   - ¿Quiénes fueron afectados por la crisis (audiencia)?
   - ¿Qué otras audiencias deberían saber sobre la crisis?
   - ¿Cómo se comunicará la información a los interesados o afectados (medio)?

   La comunicación de la crisis deberá considerar los siguientes principios:
   - Informar rápida y periódicamente: Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.
   - Decir la verdad: Ser honestos en los comunicados, sin embargo, no significa transmitir toda la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia.

Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.

- Emitir reportes lo más exactos posible: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

Las audiencias a considerar en la comunicación de la crisis son:

- Áreas o Unidades Territoriales inspeccionadas, vigiladas y/o controladas.
- Usuarios externos de los productos y/o servicios de la entidad.
- Funcionarios
- Opinión Pública
- Gobierno y Autoridades
- Líderes de Opinión
- Contratistas y Proveedores

d) La Alta Dirección, o los funcionarios designados por ésta, deberá realizar monitoreo permanente de la crisis y tomar las decisiones que correspondan para continuar con la mitigación del mismo. Se debe tener en cuenta:

- ¿Qué información circula en los medios de comunicación?
- ¿Qué información circula a nivel interno?
- ¿Qué impacto sobre la crisis tiene la información que está circulando en los medios?
- ¿Se requerirá realizar nuevos comunicados?

XIII. Plan de Recuperación

Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Contempla acciones como:

- Evaluación de daños.
- Traslado de las operaciones al Datacenter alterno.
- Traslado del Datacenter alterno al lugar habitual.
- Reanudación de la actividad.
- Desactivación de contratos de alquiler.
- Reclamos a la compañía de seguros.

13.1. Objetivos

El Objetivo del Plan de Recuperación es el de restablecer en el menor tiempo posible el nivel de producción normal de la Unidad de Tecnologías de Información (UTI).

Asimismo, son Objetivos del Plan de Recuperación los siguientes:

1) Determinación de las políticas y procedimientos para respaldar una o todas las Aplicaciones.
2) Intentar reactivar dentro de las 72 horas de producido un desastre, todos los Sistemas de Información y sus funciones inherentes.
3) Conseguir el completo respaldo de las comunicaciones con las Unidades Territoriales.

4) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
5) Apoyo permanente a los usuarios del Sistema.
6) Proveer un paquete de acciones a ejecutar para garantizar y asegurar una rápida, eficiente y oportuna respuesta a los desastres.

13.2. **Alcance**

El Plan de Recuperación se basa en los planes de emergencia y de respaldo y como ellos, existen en todas las funciones de la UTI, y en todos los niveles. La responsabilidad de la recuperación es de quien presta el servicio, en este caso de la UTI. Se considera en todo momento que la capacidad de procesamiento de datos de Foncodes, está compuesta de una combinación de personal, equipos, datos, programas, procedimientos, comunicaciones, suministros y estrategias de recuperación.

13.3. **Estrategias**

El Plan de Recuperación identifica específicamente los elementos listados en el párrafo anterior y destaca la forma en que cada uno de ellos debe restablecerse. En general, las estrategias escogidas identifican las fuentes alternativas de los recursos, los lista y los describe.

a) Personal

El personal es el recurso más crítico, ya que es difícil de reemplazar y entrenar. Su experiencia, entrenamiento y conocimiento lo hace único para la instalación.

El personal de Foncodes se encuentra distribuida en 26 Unidades Territoriales, de presentarse el evento afectaría a un grupo, por lo que el Plan basa su estrategia en el Programa de Seguridad y el Plan de Emergencia de la institución que, a su vez, basa su estrategia en la supervivencia y seguridad del personal.

Adicionalmente, se identifica al personal clave en la tarea de restablecimiento del servicio,

De contar con una crisis nacional se designarán personas claves en las Unidades Territoriales, para que reporten las incidencias periódicamente.

b) Instalación

El Datacenter o Centro de Datos tiene la función de consolidar en él los recursos, servicios y sistemas de información de Foncodes, y requiere básicamente de equipos y el personal de que los opera. La acción de recuperación, por lo tanto, implica únicamente el traslado de algunos servidores, adaptar instalaciones de comunicaciones, de personal, documentación, datos y programas de respaldo a las instalaciones de respaldo:

A finales del año 2015 debido a un incendio ocurrido en el edificio de la Sede Central, se utilizó el local de La Molina como lugar alterno para el procesamiento de la información, lográndose habilitar temporalmente los servicios y sistemas de información principales. A la fecha se cuenta con espacio al cual se podría volver a desarrollar una situación similar.

c) Facilidades de Comunicación

En el Plan de Contingencias se considera a la mayor parte de las facilidades de comunicación como propias, aun cuando son servicios proporcionados por terceros. La razón de esta consideración es

que en la medida que los servicios deseados sean ajenos, mayor será el tiempo que se necesitará para restablecerlos en caso de emergencia; por esta razón también se considera a este rubro por separado.

El restablecimiento de las facilidades de comunicación queda bajo la responsabilidad de las empresas proveedoras de estos servicios. Mientras dure la situación de emergencia el procesamiento de datos quedará circunscrito en las instalaciones de respaldo, probablemente sin medios de transmisión de datos. La comunicación entre las instalaciones de respaldo y la oficina principal se realizará por telefonía celular, correo u otro medio de comunicación existente.

d) Equipo de Procesamiento de Datos

Todos los equipos de Foncodes son transportables lo que facilitará su traslado a las instalaciones de respaldo.

Para lograr esta transportabilidad, y como se indicó anteriormente, todo el software y componentes adquiridos son estándar y de uso común en el mercado.

Los proveedores de equipos y servicios de respaldo para los procesos de recuperación de equipos tienen una descripción técnica de detalle del hardware y software instalado.

13.4. **Supuestos**

En esta sección se describe la probable magnitud y alcance de las contingencias que ha de afrontarse y el entorno en el cual ha de funcionar el Plan, que se abordó en sus aspectos generales en el capítulo IX. “Aspectos Básicos a Considerar”. Sin embargo, a raíz de las lecciones aprendidas en la reciente pandemia, podemos ser más específicos en algunos aspectos, tal como:

- Los usuarios se comunicarán con sus equipos de casa a sus equipos de la Sede Central, de ser necesario.
- Se tiene procedimientos para el manejo de los riesgos más comunes.
- Hay experiencias en el manejo de los recursos logísticos y humanos, entre otros.

Los supuestos tratan el riesgo inherente al Plan en sí mismo, esto es, que podría suceder si el Plan no funciona como se ha escrito o que, funcionando tal como está escrito, no alcanzara sus Objetivos.

También trata los riesgos residuales que podrían existir al estar en vigor el presente Plan de Contingencias de TI. Este Riesgo se considera como la suma del Plan más todos los riesgos que el Plan no atiende.

13.5. **Sub-Planes de Apoyo**

13.5.1. Sub-Plan de Comunicaciones

Se debe llevar un registro documentado de las capacitaciones y comunicaciones desarrolladas.

La UTI determinará la necesidad de comunicaciones y capacitaciones pertinentes, en cada caso, incluyendo:

a) Contenido de la comunicación.
b) Cuando comunicar.

c) A quien comunicar.

En la Tabla N.° 03: Cronograma de Comunicaciones, se detalla los objetivos e interesados para efectos de desarrollar las comunicaciones.

Tabla N.° 03: Cronograma de Comunicaciones

Nombre de Evento	Objetivo	Interesados	Tipo de Evento	Fecha
Difusión de Plan de Contingencia	Dar a conocer Plan de Contingencia	Todo Foncodes	Comunicación vía correo	Octubre 2020
Difusión de Gestión de Riesgos	Sensibilizar al personal sobre los riesgos en TI	Personal UTI	Comunicación vía correo	Noviembre 2020
Difusión y preparación para Simulacro Shake Out	Crear conciencia sobre el riesgo de sismo	Todo Foncodes	Comunicación vía correo. Spot Virtuales	Noviembre a Diciembre 2020
Seguridad Digital	Crear conciencia de la importancia de protegerse contra los ciberataques	Todo Foncodes	Comunicación vía correo. Exposición Virtual	Noviembre a Diciembre 2020

Fuente: Propia.

Algunos aspectos a considerar en las comunicaciones:

- **Transparencia**: Hacer que todos los procesos, procedimientos, métodos, fuentes de datos y supuestos utilizados en la comunicación estén disponibles para las partes interesadas, teniendo en cuenta la confidencialidad de la información según se requiera.
- **Idoneidad**: Hacer que la información proporcionada en la comunicación a las partes interesadas sea pertinente, utilizando formatos, el idioma y los medios que cumplan con sus intereses y necesidades, para que puedan participar plenamente.
- **Credibilidad**: Comunicar con una conducta honesta y justa, y proporcionar información que se veraz, exacta y sustantiva. Desarrollar la información y datos con métodos e indicadores reconocidos y reproducibles.
- **Respuesta**: Responder a las preguntas y preocupaciones de las partes interesadas de forma plena y oportuna. Hacer conscientes a las partes interesadas de cómo se han abordado sus preguntas e inquietudes.
- **Claridad**: Asegurar que los métodos de comunicación y el lenguaje son comprensibles para las partes interesadas para minimizar la ambigüedad.

En la Figura N.° 04 se evidencia a las áreas u entidades a las cuales se debe priorizar las comunicaciones.

Figura N.° 04: Segmentación de los interesados para las comunicaciones

Fuente: Propia. (En base a Manual de ISO 22301 New Horizons, 2019)

13.5.2. Sub-Plan de Capacitaciones

La capacitación, es un proceso educacional de carácter estratégico aplicado de manera organizada y sistémica, mediante el cual el personal adquiere o desarrolla conocimientos y habilidades específicas relativas al trabajo, y modifica sus actitudes frente a aspectos de la organización, el puesto o el ambiente laboral. Más aun estando en el área TIC, donde la tecnología cambia rápidamente, es necesario mantenerse en constante proceso de capacitación.

Alcance: Personal de la UTI, extendiéndose a los usuarios

Fines: Generar conductas positivas, mejorar la productividad y disminuir riesgos.

Generar una cultura de prevención de riesgos.

Mantener al trabajador de la UTI al día en los avances tecnológicos, lo que alienta la iniciativa y creatividad, previniendo la obsolescencia de la fuerza de trabajo.

En la Tabla N.° 04: Plan de Capacitación, se detalla sobre las actividades de capacitación a desarrollar.

Tabla N.° 04: Plan de Capacitación

AREA	TEMA	FRECUENCIA
Desarrollo	Testing a software. Mejores prácticas en seguridad (OWASP)	Permanente
Soporte	Análisis de Riesgo en ambientes de TI Manejo de Contingencias de TI	Permanente
Infraestructura	Análisis de Riesgo en ambientes de TI Manejo de Contingencias de TI	Permanente
Calidad	Análisis de Riesgo en ambientes de TI Manejo de Contingencias de TI	Permanente
Fuente: Propia.		

Se coordinará con la Unidad de Recursos Humanos (URH), para brindar las capacitaciones a los usuarios por parte de especialistas de la UTI o algún proveedor especialista en la materia.

13.5.3. Sub-Plan de Pruebas y Validaciones

El Sub-Plan de Pruebas y validaciones, es el proceso para asegurarse que los datos o bases de datos se han recuperado completamente, además de otros aspectos de funcionalidad, funcionan correctamente y con normalidad.

Se debe llevar un registro documentado de las pruebas efectuadas.

En la Tabla N.° 05: Cronograma de Pruebas, se detalla las pruebas que debe desarrollarse para implementar el presente Plan.

Tabla N.° 05: Cronograma de Pruebas

Nombre de Evento	Objetivo	Interesados	Tipo de Evento	Fecha
Simulacro	Probar la eficacia del Plan	Personal UTI	Simulacro con caída de sistemas.	Enero 2021
	Restauración de backup de SGP	Personal UTI	Simulacro con caída de sistemas.	2021
	Restauración de backup de SGA	Personal UTI	Simulacro con caída de sistemas.	2021
	Restauración de backup de SGD	Personal UTI	Simulacro con caída de sistemas.	2021
	Restauración de Documentos (Alfresco)	Personal UTI	Simulacro con caída de sistemas.	2021
Simulación	Probar la eficacia del Plan	Personal UTI	Simulación con caída de sistemas	30/07/2021

Fuente: Propia.

13.5.4. Sub-Plan de Mantenimiento del Plan de Contingencias

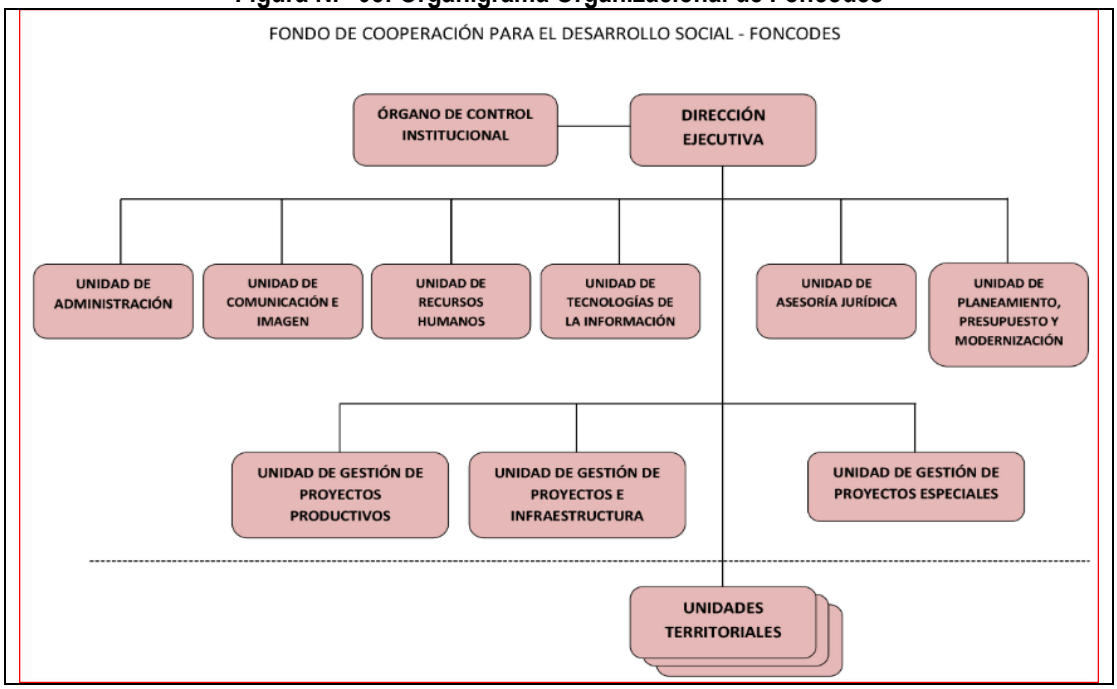
Cada primer mes del año se reunirá el jefe de la UTI, el Oficial de Seguridad de la Información, y otros profesionales y/o técnicos que el jefe de la UTI determine, para evaluar si ha habido cambios en el hardware, software o procesos, que ameriten una actualización del Plan de Contingencias, se dejara constancia de la reunión con acta firmada, sobre la decisión, sea positiva o negativa.

XIV. Activación del Plan de Contingencias

14.1. Decisión

Queda a juicio del Director Ejecutivo y del jefe de la UTI el determinar, en primer lugar, si ha de activarse el Plan de Contingencias y, en segundo lugar, si el procesamiento ha de trasladarse a las instalaciones Datacenter alterno. Para ello se basarán en las recomendaciones de la Jefatura de la UTI. Ver Figura N.° 05: Organigrama Organizacional de Foncodes.

Figura N.° 05: Organigrama Organizacional de Foncodes



Fuente: Página web de Foncodes

14.2. Duración estimada

El jefe de la UTI, será responsable de determinar la duración estimada de la interrupción del servicio durante su traslado de ser necesario. Dado que este es un factor clave, será discutido y analizado antes de darse la orden de traslado.

14.3. Responsabilidades

- Orden de Ejecución del Plan: Director Ejecutivo.
- Supervisión General del Plan: jefe de la UTI.
- Tareas de recuperación: Equipo de Contingencias.
- Aplicación del Plan: Se aplicará el Plan siempre que se prevea una pérdida del servicio por un periodo mayor a 48 horas.

14.4. Procedimientos de contingencia

Especificación de los procedimientos que se deberán llevar a cabo en caso de que, aún pese a las normas establecidas, se produzca un evento de riesgo.

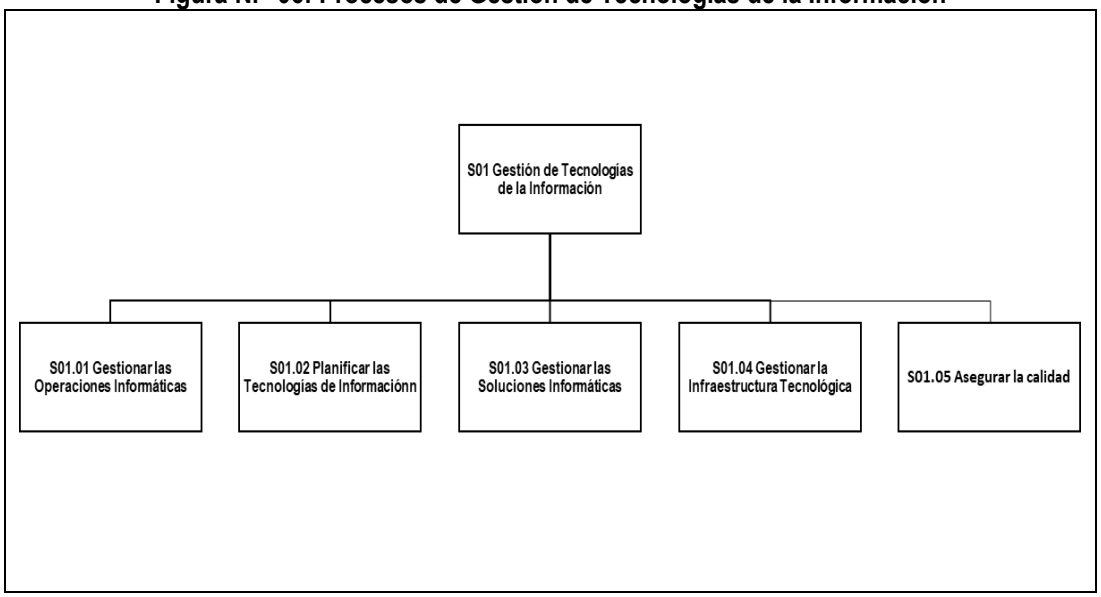
Criterios para declarar la contingencia. - Los criterios para declarar la contingencia están definidos por los siguientes criterios:

- Sistemas y servicios afectados.
- Resultados del diagnóstico.
- Acciones realizadas.
- Tiempo estimado para normalización.
- Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
- Decisiones que debe tomar la alta dirección.

14.5. **Organización y Administración para el Plan de Contingencias**

La organización y administración del Plan de Contingencias de Tecnologías de la Información está definido por los procesos que la Unidad de Tecnologías de la Información (UTI) tiene definidos conforme lo aprobado a través de la Resolución de la Dirección Ejecutiva N.° 140-2018-FONCODES/DE y cuyos procesos principales se muestran a continuación (Figura N.° 06).

Figura N.° 06: Procesos de Gestión de Tecnologías de la Información



Fuente: Manual N.° 14-2018-FONCODES/UTI: Manual de procesos y procedimientos de gestión de tecnologías de la información (aprobado con RDE N.° 140-2018-FONCODES/DE)

14.5.1. Roles y responsabilidades

Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada.

En la tabla N.° 02 Responsabilidades definidas para cada rol, se muestran los roles y responsabilidades para cada actor del Plan de Contingencias

14.5.2. Organización del trabajo para la ejecución del plan

El presente plan de contingencias detalla claramente los niveles de toma de decisiones y acciones de respuesta ante cualquier situación que requiere la ejecución de un procedimiento de contingencia; de tal manera que las decisiones a tomar no dependan de consultas adicionales o que generen dudas para su inmediata ejecución.

Asimismo, queda definido un comité de trabajo para el cumplimiento y actualización del Plan de Contingencia ante problemas informáticos, que participaran al momento de tomar decisiones ante eventualidades que impacten en el funcionamiento de los servicios informáticos de a UTI.

El Comité designado, es el responsable del Plan de Contingencias. Sus funciones básicas son; Programar, dirigir, ejecutar y evaluar el desarrollo del plan, organizando asimismo los equipos.

El Comité de Seguridad está constituido por:

- Jefe de la Unidad de Tecnologías de Información (UTI).
- El Oficial de Seguridad de la Información.
- Responsable(s) que se definan y/o encarguen para cada uno de los procesos principales de la gestión de tecnologías de la información.

El jefe de la Unidad de TI tiene como funciones básicas programar y evaluar el desarrollo del plan de contingencias.

Los responsables de los diferentes procesos de la Gestión de Tecnologías de la Información y el oficial de seguridad tienen como funciones básicas dirigir y ejecutar el desarrollo del plan de Contingencias en los puntos de su competencia, organizando asimismo equipos de trabajo para hacer frente antes, durante y después de materializada y controlada la amenaza.

XV. Disposiciones Complementarias

15.1. El presente Plan de Contingencia cubre razonablemente los casos más probables de interrupción del servicio, sin embargo este debe ser actualizado periódicamente, cuando cambia alguno de los factores relevantes del entorno, como algún nuevo dispositivo crítico, un cambio de tecnologías, o de normatividad que afecte el alcance del Plan de Contingencias, ya que este es un documento en evolución, en tal sentido, su revisión será anual y su actualización permanente; en correspondencia con los cambios que se registren en la infraestructura de Tecnologías de Información de Foncodes, asimismo este debe ser coordinado con el Plan de Continuidad Operativa.

15.2. Es indispensable contar con un Datacenter Alterno, para asegurar la continuidad de operaciones ante problemas graves que afecten la infraestructura de la Sede Principal, se debe evaluar los locales propios que tienen Foncodes a nivel nacional, realizar convenios de cooperación con entidades del Sector, u otras del estado e inclusive explorar la alternativa de protección en la nube. Es necesario precisar que en las Unidades Territoriales no se tienen espacios acondicionados para los equipos centrales y ello puede poner en riesgo la continuidad de sus operaciones.

15.3. Se deberá contar con un Plan de Capacitación a los usuarios sobre seguridad de información y continuidad operativa, con el fin de prevenir incidentes de seguridad informática, de seguridad física ante siniestros, además de simulacros de evacuación.

15.4. Se debe mantener coordinaciones estrechas con los responsables de TI y seguridad de información del MIDIS y los programas sociales adscritos al Sector, para efectos de trabajos y colaboraciones conjuntas ante casos de riesgos; asimismo, con las autoridades, como serenazgo, bomberos, hospitales y clínicas, para caso de emergencia.

15.5. Foncodes debe desarrollar una cultura de prevención de riesgos, entre todos sus integrantes, a fin de disminuir las vulnerabilidades y gestionar las amenazas, minimizando los impactos, y formando un equipo resiliente y preparado ante circunstancias adversas.

XVI. Referencias Bibliográficas

- ISO 27001:2014 Seguridad de Información
- ISO 31001:2017 Gestión de Riesgos
- ISO 22301:2013 Gestión de la Continuidad del Negocio.
- ISO 22320:2013 Plan de Emergencias.
- Manual de ISO 22301:2013 New Horizons 2019.

XVII. Anexos

17.1. Anexo 1.- Lista de Contactos
17.2. Anexo 2.- Teléfonos de emergencia
17.3. Anexo 3.- Definiciones

XVIII. Hoja de control de cambios

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1.0	13.08.2013	Versión original
2.0	27.07.2020	Actualización del documento

Anexo 1.- Lista de Contactos

Personal

Cargo	Nombre	Teléfono
Jefe de Unidad de Tecnologías de la Información	Jean Pierre Calmet	947454944
Especialistas en Redes	Jean Pierre Calmet Luis Tullume	947454944 972665892
Administrador de Base de Datos	Romaín Loayza	996475353
Oficial de Seguridad de la Información	Juan Carlos Reátegui	980929404
Especialistas de Sistemas	Victor Quispe	987183134

Proveedores y Servicio

Institución/ Equipo	Proveedor	Contacto	Correo	Teléfono
Servicio Internet	GTD Perú S.A.	Plataforma Atención Cliente	Clientes.GtdPeru@grupogtd.com	743-0911 0800-7-0202
Solución Antivirus	ESET Perú S.A.	Victor Gutierrez	vgutierrez@eset.pe	992214073
Custodia de Backup	Iron Mountain Perú S.A.	César Monigote Vega	cesar.monigote@ironmountain.com.pe	998318464 981077937 7114000 Anexo 355
Telefonía Móvil	Telefónica del Perú S.A.A.	Violeta Alvarado	violeta.alvarado@telefonica.com	996166521
PECERT	SEGDI-PCM (Centro de Incidentes de Seguridad)	Plataforma PECERT	pecert@pcm.gob.pe	2197000 Anexo 5116

Anexo 2.- Teléfonos de Emergencia

TELEFONOS DE EMERGENCIA (San Isidro)	
DEFENSA NACIONAL (MIDIS) (Percy Rudy Montes Rueda)	6318000 anexo 1586 949519228
Coordinador de Seguridad del MIDIS (Alejandro Clecke Camargo)	6318000 Anexo 1610 973589598
Supervisor de Seguridad del MIDIS (Alfonso de La Quintana Cámero)	957421446
Supervisor Residente FONCODES (Victor Cárdenas Giron)	940027408
COE - MIDIS	6318000 -Anexo 1611 994431862
Serenazgo San Isidro	3190450
Emergencia Policial	105
Comisaria San Isidro (Calle Antequera # 162)	4410222
Cuerpo General de Bomberos	116
SAMU (Sistema de Atención Medica Urgencia)	106
Bomberos San Isidro 100	2640339
Coordinador de Brigadas (Juan Carlos Reátegui)	#966935208
Luz del Sur	617-5000
Sedapal	317-8000
Central de FONCODES	3118900

Cultura Preventiva: Es el conjunto de actitudes y creencias positivas, compartidas por todos los miembros de una empresa sobre salud, riesgos, accidentes, enfermedades y medidas preventivas. También podemos definirla como la actitud proactiva, de todos y todas los integrantes de las familias, escuelas, empresas y comunidades, para emprender acciones de prevención, independientemente de que exista o no un desastre inminente.

Anexo 3.- Términos y Definiciones

Para los fines de aclarar los conceptos en el presente documento se utilizarán las definiciones de la Norma Técnica Peruana ISO 27002:2014.EDI. Código de buenas prácticas para la gestión de la seguridad de la Información.

Activo: Algo que tenga valor para lo organización.

Activo Informático: Conjunto de bienes de una organización que se encuentran relacionados directa o indirectamente con la actividad informática. Entre ellos se encuentran:

- La información mecanizada.
- Los medios de comunicación que se utilizan para la transmisión de datos mecanizados
- (computadoras, redes de computadoras, correo electrónico, etc.).
- Los medios magnéticos y ópticos de almacenamiento de la información (cintas, cartuchos,
- discos, etc.).

- Los programas y las aplicaciones de la institución, ya sea desarrollados por esta, adquiridos o alquilados a terceros.
- Los manuales, procedimientos y reglamentaciones afines al área de la informática (Plan de Contingencia, Procedimientos de Seguridad, etc.).

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

Análisis del riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Control: Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. Control es también usado como sinónimo de salvaguardia o contramedida.

Desastre: Para efectos de establecer los alcances del plan de contingencias partiremos de la definición de un desastre: "algún tipo de evento que causa una reducción significativa en la capacidad de procesamiento de los sistemas de información o en la infraestructura de apoyo que mantiene la funcionalidad del mismo; por lo que la ocurrencia del desastre implica necesariamente un impacto o reducción en las capacidades de operación y del servicio que la Organización brinda a sus clientes y usuarios internos".

La manifestación del desastre implica un impacto en la ejecución de los procesos críticos de la Organización. Situación que limitará la capacidad de ésta para satisfacer la demanda normal del servicio.

La naturaleza del desastre puede ser muy variada, desde causas naturales, hasta daños intencionales del usuario interno.

Las consecuencias de un desastre dentro de la Organización son variadas, y pueden ir desde lapsos cortos de suspensión de los servicios hasta suspensión indefinida de los servicios elementales de la Organización, lo que demandará de medidas de operación limitadas y procesos de recuperación complejos.

Evento de seguridad de información: Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

Evaluación del riesgo: Proceso general de análisis y evaluación del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

Incidente de seguridad de información: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

Instalaciones de proceso de información: Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

Pauta: Descripción que aclara que es lo que se debe hacer y como se hace, con el fin de alcanzar los objetivos planteados en las políticas.

Política: Dirección general y formal expresada por la gerencia.
Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden son consideradas.

Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

UPS.- Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados. Otra función que se puede añadir a estos equipos es mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en caso de usar corriente alterna.

UTI.- Unidad de Tecnología de la Información.

Valoración del riesgo: Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.

Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.