MEF

Firmado Digitalmente por ALARCON ALVIZURI Bertha Patricia FAU 20131370645 soft
Fecha: 27/06/2023 15:45:18 COT
Motivo: Doy V° B°

REPUBLICA DEL PERU

MINISTERIO DE ECONOMÍA Y FINANZAS
SECRETARÍA GENERAL
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
11 JUL. 2023
JUAN RAÚL LÓPEZ TORRES
FEDATARIO

MEF

Firmado Digitalmente por TRINIDAD GUERRERO Kitty Elisa FAU 20131370645 soft
Fecha: 11/07/2023 12:12:04 COT
Motivo: Doy V° B°

Resolución Ministerial

Lima, 11 de julio del 2023 No. 257-2023-EF/47

MEF

Firmado Digitalmente por ELGAREJO CASTILLO Juan Carlos FAU 20131370645 soft
Fecha: 10/07/2023 19:41:16 COT
Motivo: Doy V° B°

CONSIDERANDO:

Que, mediante la Ley N° 29664, se crea el Sistema de Nacional de Gestión del Riesgo de Desastres (SINAGERD), como sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres;

Que, mediante Resolución Ministerial N° 028-2015-PCM, se aprueban los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno y en dicho contexto, mediante la Resolución Ministerial Nº 362-2021-EF/47 se aprueba el Plan de Continuidad Operativa del Ministerio de Economía y Finanzas, cuyo objeto es establecer los parámetros que permitan garantizar, ante un desastre de gran magnitud o cualquier evento que interrumpa las actividades críticas del MEF, una respuesta adecuada para minimizar el impacto del riesgo de disrupción que pueda afectar el normal desarrollo de las actividades del Ministerio;

MEF

Firmado Digitalmente por VARGAS MEDRANO Carlos Alberto FAU 20131370645 hard
Fecha: 04/07/2023 10:34:02 COT
Motivo: Doy V° B°

Que, mediante la Resolución Ministerial Nº 320-2021-PCM, se aprueban nuevos Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno y se deroga la Resolución Ministerial Nº 028-2015-PCM;

Que, los citados Lineamientos tienen como objetivo establecer los procedimientos para la implementación de la Gestión de Continuidad Operativa y la formulación de los Planes de Continuidad Operativa en las Entidades Públicas de los tres niveles de Gobierno, con el fin de continuar funcionando ante un desastre o cualquier evento que interrumpa prolongadamente sus operaciones;

Que, adicionalmente, el numeral 6.3.2 de los referidos Lineamientos precisa que para la aprobación del Plan de Continuidad Operativa, el Grupo de Comando para la Gestión de la Continuidad Operativa presenta el proyecto del Plan de Continuidad Operativa al titular de la entidad o Alta Dirección para su revisión y aprobación respectiva, a través de resolución o norma de mayor jerarquía de la entidad;

Que, acorde con el nuevo marco normativo para la gestión de continuidad operativa, a través de la Resolución Ministerial N° 150-2022-EF/47, se aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa del Ministerio de Economía y Finanzas;

MEF

Firmado Digitalmente por ALARCON ALVIZURI Bertha Patricia FAU 20131370645 soft
Fecha: 27/06/2023 15:45:26 COT
Motivo: Doy V° B°

MINISTERIO DE ECONOMÍA Y FINANZAS
SECRETARÍA GENERAL
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
11 JUL. 2023
JUAN RAÚL LÓPEZ TORRES
FEDATARIO

MEF

Firmado Digitalmente por TRINIDAD GUERRERO Kitty Elisa FAU 20131370645 soft
Fecha: 11/07/2023 12:12:12 COT
Motivo: Doy V° B°

Que, a través del Acta de Reunión Nº 002-2023-GRUPO DE COMANDO-MEF, correspondiente a la sesión del Grupo de Comando de fecha 19 de junio de 2023, se acordó aprobar el proyecto del Plan de Continuidad Operativa del Ministerio de Economía y Finanzas y encargar a la Oficina de Gestión de Riesgos Operativos de la Oficina General de Integridad Institucional y Riesgos Operativos, en su calidad de Presidente del Grupo de Comando, realizar las acciones correspondientes para la aprobación de la propuesta de Plan de Continuidad Operativo, en correspondencia con el marco normativo vigente;

MEF

Firmado Digitalmente por MELGAREJO CASTILLO Juan Carlos FAU 20131370645 soft
Fecha: 10/07/2023 19:41:19 COT
Motivo: Doy V° B°

Que, el literal b) del artículo 62 del Texto Integrado Actualizado del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con la Resolución Ministerial Nº 213-2020-EF/41, establece como función de la Oficina General de Integridad Institucional y Riesgos Operativos el conducir la formulación de propuestas de metodologías, lineamientos u otros documentos que permitan la adecuada gestión de riesgos operativos y de continuidad operativa del Ministerio de Economía y Finanzas, lo cual se gestiona a través de la Oficina de Gestión de Riesgos Operativos; y;

MEF

Firmado Digitalmente por VARGAS MEDRANO Carlos Alberto FAU 20131370645 hard
Fecha: 04/07/2023 20:34:07 COT
Motivo: Doy V° B°

Que, de conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; en la Ley N° 29664, Ley que crea el Sistema de Gestión del Riesgo de Desastres (SINAGERD); en la Resolución Ministerial Nº 320-2021-PCM, que aprueban los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno; en la Resolución Ministerial N° 150-2022-EF/47, que aprueba la conformación del Grupo Comando para la Gestión de la Continuidad Operativa del Ministerio de Economía y Finanzas; y en la Resolución Ministerial N° 213-2020-EF/41, que aprueba el Texto Integrado Actualizado del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas.

SE RESUELVE:

Artículo 1. Objeto

Aprobar el "Plan de Continuidad Operativa del Ministerio de Economía y Finanzas", que como Anexo forma parte de la presente Resolución Ministerial.

Artículo 2. Derogación

Derogar los siguientes dispositivos legales:

- Resolución Ministerial Nº 362-2021-EF/47 que aprueba el Plan de Continuidad Operativa del Ministerio de Economía y Finanzas.
- Resolución Ministerial N° 089-2020-EF/47 que aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa del Ministerio de Economía y Finanzas.
- Resolución Ministerial N° 385-2020-EF/47 que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa en el Ministerio de Economía y Finanzas".

MEF

Firmado Digitalmente por ALARCON ALVIZURI Bertha Patricia FAU 20131370645 soft
Fecha: 27/06/2023 15:45:36 COT
Motivo: Doy V° B°

REPUBLICA DEL PERU

MINISTERIO DE ECONOMÍA Y FINANZAS
SECRETARÍA GENERAL
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
11 JUL. 2023
JUAN RAÚL LÓPEZ TORRES
FEDATARIO

MEF

Firmado Digitalmente por TRINIDAD GUERRERO Kitty Elisa FAU 20131370645 soft
Fecha: 11/07/2023 12:12:19 COT
Motivo: Doy V° B°

Resolución Ministerial

MEF

Firmado Digitalmente por VARGAS MEDRANO Carlos Alberto FAU 20131370645 hard
Fecha: 04/07/2023 20:34:15 COT
Motivo: Doy V° B°

Artículo 3. Publicación

Publicar la presente Resolución Ministerial y su Anexo en la sede digital del Ministerio de Economía y Finanzas (www.gob.pe/mef); así como en la Intranet del Ministerio y disponer su difusión a todo el personal del Ministerio mediante correo electrónico.

Regístrese y comuníquese.

MEF

Firmado Digitalmente por ELGAREJO CASTILLO Juan Carlos FAU 20131370645 soft
Fecha: 10/07/2023 19:41:27 COT
Motivo: Doy V° B°

ALEX ALONSO CONTRERAS MIRANDA
Ministro de Economía y Finanzas

MEF

Firmado Digitalmente por
ALARCON ALVIZURI
Bertha Patricia FAU
20131370645 soft
Fecha: 27/06/2023
15:10:32 COT
Motivo: Doy V° B°

PERÚ Ministerio de Economía y Finanzas

MEF

Firmado Digitalmente por
SANTILLAN RAMIREZ
Segundo Marcos FAU
20131370645 soft
Fecha: 27/06/2023
14:58:05 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por
JARA HUALLPATUERO
Maria Ysabel FAU
20131370645 soft
Fecha: 04/07/2023
18:23:35 COT
Motivo: Doy V° B°

PLAN DE CONTINUIDAD OPERATIVA DEL MINISTERIO DE ECONOMÍA Y FINANZAS

Oficina General de Integridad Institucional y Riesgos Operativos
Oficina de Gestión de Riesgos Operativos

ÍNDICE

I. INFORMACIÓN GENERAL

Mediante la Ley N° 29664 se crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) como sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, evitar la generación de nuevos riesgos, y preparar la atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de gestión.

La Política Nacional de Gestión del Riesgo de Desastres al 2050, ha identificado como problema público la débil gobernanza de la Gestión del Riesgo de Desastres, y en atención de dicho problema, la citada política ha establecido en su Objetivo Prioritario 3 "Mejorar la implementación articulada de la gestión del riesgo de desastres en el territorio", el Lineamiento L3.1. "Implementar medidas para la optimización de la gestión del riesgo de desastres en los tres niveles de gobierno", en el cual se ha determinado como un servicio a la población, la elaboración de un programa de continuidad operativo del Estado, a cargo de las todas las entidades de los tres niveles de gobierno.

Asimismo, el Plan Nacional de Gestión del Riesgo de Desastres 2022-2030 (aprobado por Decreto Supremo Nº 115-2022-PCM) contempla como Acción Estratégica Multisectorial - AEM 3.2 "Fortalecer capacidades de las entidades del Sistema Nacional de Gestión del Riesgo de Desastres para la gestión de la continuidad operativa del Estado" y define como Actividad Operativa Multisectorial - AOM 3.2.1 "Planes de continuidad Operativa implementados en las entidades del Sistema Nacional de Gestión del Riesgo de Desastres"; por lo que, corresponde elaborar y aprobar e implementar el Plan de Continuidad Operativa en el Ministerio de Economía y Finanzas.

Mediante Resolución Ministerial N° 320-2021-PCM se aprueban los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación del Plan de Continuidad de las Entidades Públicas en los tres niveles de gobierno y se deroga la Resolución Ministerial N° 028-2015-PCM, con lo cual se establece un nuevo marco normativo para la gestión de la continuidad operativa.

De conformidad con los lineamientos vigentes, la gestión de la continuidad operativa se desarrolla a través de los siguientes componentes:

a. Identificación de Riesgos y Recursos
b. Desarrollo e implementación de la gestión de la continuidad operativa.
c. Pruebas y actualización de los planes de continuidad operativa.
d. Integración de la gestión de la continuidad operativa a la cultura organizacional.

La Identificación de Riesgos y Recursos comprende la identificación de peligros y riesgos, el análisis de impacto, la determinación de las actividades críticas, la determinación de recursos humanos, recursos informáticos e información crítica, recursos físicos críticos, así como los recursos financieros.

El desarrollo e implementación de la gestión de la continuidad operativa incluye la gestión de crisis, así como del Plan de Continuidad Operativa.

Los ejercicios o pruebas se realizan para validar el Plan de Continuidad Operativa, para lo cual se establecen objetivos definidos, reporte de resultados alcanzados y recomendaciones. Asimismo, el Plan de Continuidad Operativa se actualiza ante cualquier cambio interno o externo que afecte al Ministerio.

La integración de la gestión de la continuidad operativa a la cultura organizacional comprende la evaluación del grado de conocimiento sobre la gestión de la continuidad operativa, diseño e implementación de planes de capacitación y entrenamiento respectivo, monitoreo permanente del nivel de entendimiento de la gestión de la continuidad operativa

y supervisión de la implementación de la Gestión de la Continuidad Operativa e informar a la Alta Dirección.

Al amparo de la normativa vigente, se requiere establecer un conjunto de acciones para que la institución se anticipe y responda de manera efectiva ante un evento disruptivo que implique un riesgo de interrupción en sus operaciones. Estas acciones constituyen la implementación de los componentes en la gestión de continuidad operativa en el MEF.

En este contexto, la Oficina de Gestión de Riesgos Operativos, en su calidad de presidente del Grupo de Comando, junto a los miembros de este colegiado y en sesiones participativas, ha conducido la elaboración del Plan de Continuidad Operativa, en concordancia con lo descrito en el numeral 6.2 “De la estructura de los Planes de Continuidad Operativa” de los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de Gobierno, aprobado por la Resolución Ministerial Nº 320-2021-PCM.

Glosario

Actividades críticas: Están constituidas por las actividades que la entidad haya identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias señaladas en las normas vigentes sobre la materia. (Fuente: Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno, numeral 5.1)

Amenaza: Fenómeno, sustancia, actividad humana o condición peligrosa que pueden ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales (Fuente: Naciones Unidas; https://www.un-spider.org/es/riesgos-y-desastres/gestion-del-riesgo-de-desastres)

Aplicaciones críticas: Aplicaciones de TI identificados en el análisis de impacto que son indispensable para el desarrollo de las actividades críticas del MEF.

Centro de procesamiento de datos principal: Lugar de los sistemas físicos (hardware) o lógicos (software), sistemas y/o aplicaciones, redes y cualquier otro mecanismo de distribución de la información que resulten necesarias para la ejecución de procesos operacionales por parte del Ministerio (Fuente: Plan de Recuperación de Desastres – OGTI, MEF).

Centro de procesamiento de datos de contingencia: Réplica del ambiente de producción del Centro de Procesamiento de Datos Principal (Fuente: Plan de Recuperación de Desastres – OGTI, MEF).

Desastre de gran magnitud: Conjunto de daños y pérdidas, en la salud, fuentes de sustento, habitad físico, infraestructura, actividad económica y medio ambiente, que ocurre a consecuencia del impacto de un peligro o amenaza, cuya intensidad genera graves alteraciones en el funcionamiento de las unidades sociales que afectan la vida de la nación y supera o pueda superar la capacidad de respuesta del país, y en casos excepcionales, puede demandar la ayuda internacional. (Fuente: Decreto Supremo N° 074-2014-PCM, norma complementaria sobre declaratorias de estado de emergencia por desastre o peligro Inminente).

Emergencia: Estado de daños sobre la vida, el patrimonio, y el medio ambiente ocasionados por la ocurrencia de un fenómeno natural o inducido por la acción humana que altera el normal desenvolvimiento de las actividades de la zona afectada. (Fuente: Decreto Supremo N° 048-2011-PCM, Reglamento de la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastre).

Evento disruptivo: Ocurrencia o cambio que interrumpe las actividades planificadas, operaciones o funciones, ya sean anticipadas o no anticipadas (Fuente: ISO 22301).

Gestión de la continuidad operativa: Es el proceso continuo que debe formar parte de las operaciones habituales de la entidad pública con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones. (Fuente: Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno, numeral 5.1).

Grupo de comando: Es el conjunto de profesionales que se encarga de la elaboración del Plan de Continuidad Operativa de la entidad y de la toma de sesiones respecto a la implementación de dicho plan (Fuente: Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno, numeral 5.1).

Peligro: Probabilidad de que un fenómeno físico, potencialmente dañino, de origen natural o inducido por la acción humana, se presente en un lugar específico, con una cierta intensidad y en un periodo de tiempo y frecuencia definido. (Fuente: Decreto Supremo N° 048-2011-PCM, Reglamento de la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastre).

Plan de continuidad operativa (PCO): Instrumento a través del cual se implementa la continuidad operativa, tiene como objetivo garantizar que la entidad ejecute las actividades críticas identificadas previamente. Contiene la identificación de riesgos y recursos, acciones para la continuidad operativa y el cronograma de ejercicios (Fuente: Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno, numeral 5.1)

Plan de recuperación de los servicios informáticos: Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnologías de la información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas su ocurrencia. Para su desarrollo toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 2007:2014 **(**Fuente: Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno, numeral 5.1)

Tiempo máximo tolerable de interrupción (MTPD): Tiempo que podría a llegar a ser inaceptable, en el cual habría impactos adversos como consecuencia de no proporcionar un servicio o llevar a cabo una actividad. (Fuente: ISO 22301)

Vulnerabilidad: Es la susceptibilidad de la población, la estructura física o las actividades socioeconómicas, de sufrir daños por acción de un peligro o amenaza. (Fuente: Decreto Supremo N° 048-2011-PCM, Reglamento de la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastre).

II. BASE LEGAL

2.1 Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
2.2 Decreto Supremo N° 048-2011-PCM, que aprueba el Reglamento de la Ley del Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
2.3 Decreto Supremo Nº 115-2022-PCM que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022 – 2030
2.4 Decreto Supremo N° 038-2021-PCM que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
2.5 Resolución Ministerial N° 213-2020-EF/41, que aprueba el Texto Integrado Actualizado del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas.
2.6 Resolución Ministerial N° 320-2021-PCM, aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación del Plan de Continuidad de las Entidades Públicas en los tres niveles de gobierno.
2.7 Resolución de Secretaria General que aprueba el Manual de Procedimientos del Macroproceso E04 Gestión de la Prevención e Integridad Institucional

Las normas antes mencionadas incluyen sus normas modificatorias, complementarias y conexas.

III. OBJETIVOS

3.1 Objetivo General

Garantizar la continuidad operativa del Ministerio de Economía y Finanzas (MEF), ante la ocurrencia de un evento disruptivo que interrumpa sus procesos, ejecutando las actividades críticas seleccionadas, hasta lograr su recuperación en el menor plazo posible.

3.2 Objetivos Específicos

a. Identificar las actividades críticas que requieren ser ejecutadas de manera ininterrumpida.

b. Determinar los recursos humanos, equipos e infraestructura, así como los servicios informáticos necesarios para ejecutar las actividades críticas seleccionadas según su nivel de criticidad.

c. Lograr un nivel de preparación que permita al MEF cumplir con funciones mínimas en un escenario de desastre de gran magnitud.

IV. IDENTIFICACIÓN DE RIESGOS Y RECURSOS

4.1 Matriz de Riesgos

La Oficina de Gestión de Riesgos Operativos (OGRO) en coordinación con diferentes órganos del MEF, ha elaborado la Matriz de Riesgos donde se identifican los riesgos que pueden interrumpir el desarrollo de las actividades y operaciones (riesgos de disrupción) del MEF. Asimismo, ha evaluado los niveles de riesgo, como resultado de la valoración efectuada por cada órgano o unidad orgánica interviniente, en función de los peligros y la vulnerabilidad relacionada con la afectación a la infraestructura física y a las personas.

El Plan de Prevención y Reducción del Riesgo de Desastres del MEF (PPRRD- MEF), aprobado con Resolución Ministerial N° 186-2021-EF/47, identifica los siguientes peligros:

Cuadro 1: Peligros según su origen

Origen natural	Definición
Sismo	Se define como sismo al proceso de generación y liberación de energía para posteriormente propagarse en forma de ondas por el interior de la tierra; al llegar a la superficie, estas ondas son registradas por las estaciones sísmicas y percibidas por la población y por las estructuras.
Tsunami	Se define como una ola de grandes dimensiones originada cerca de la costa por un sismo de gran magnitud o erupción volcánica submarina, que puede desplazarse a una velocidad de hasta 50 km/h en cualquier dirección, que puede traer como consecuencia la destrucción y muerte de seres humanos al arrastrar grandes masas de agua.
Movimiento en masa	Del conjunto de eventos que implican los movimientos en masa, se considera, a las zonas de mayor susceptibilidad a la ocurrencia de estos eventos. Es así que vemos que los huaycos periódicos (flujos de lodo y piedra) se presentan con mayor frecuencia y se producen durante la temporada de lluvias, entre diciembre y abril.
Inundaciones	Las inundaciones son un desbordamiento de agua en distintos tipos de suelo y pueden ocurrir durante lluvias de gran intensidad, por olas del océano que llegan a la costa, cuando la nieve se derrite demasiado rápido, o en el momento en el que se rompen presas o diques.
Heladas y friaje	Las Heladas son fenómenos que se presentan en la sierra en períodos de otoño e invierno, cuando la temperatura desciende por debajo de los cero grados y ocurre en zonas localizadas por encima de los 2,500 metros de altitud.
Fenómeno del Niño	Es un fenómeno o evento de origen climático relacionado con el calentamiento del Océano Pacífico oriental ecuatorial, el cual se manifiesta de manera más intensa, provocando estragos en la zona intertropical y ecuatorial debido a las fuertes lluvias, afectando principalmente a la región costera del Pacífico de América del Sur.
Origen Antrópico o Humano	**Definición**
Contaminación Ambiental - Deforestación	Se denomina contaminación ambiental a la presencia de componentes nocivos (ya sean químicos, físicos o biológicos) en el medio ambiente (entorno natural y artificial), que supongan un perjuicio para los seres vivos que lo habitan, incluyendo a los seres humanos.
Incendios urbanos	Los incendios urbanos son fuegos no controlados de grandes proporciones que ocasionan lesiones, pérdidas de vidas humanas, daños materiales y deterioran el ambiente.
Incendios forestales	Un incendio forestal es un fuego que se propaga sin control en terrenos rurales o áreas de cultivo cualquiera que sea su origen, que puede causar daño a las personas, la propiedad o al medio ambiente, a través de vegetación leñosa, arbustiva o herbácea, viva o muerta.
Emergencias sanitarias	La Emergencia Sanitaria es un evento extraordinario que constituye un riesgo para la salud pública, afectando a los conciudadanos y ciudadanos de otros Estados, a través de la propagación de la enfermedad y que potencialmente requiere una respuesta inmediata y coordinada

Fuente: Resolución Ministerial N° 186-2021-EF/47

Tomando en consideración los peligros descritos anteriormente, y otros peligros que amenazan la continuidad de las operaciones del MEF, identificadas en las sesiones

participativas con los órganos del MEF, se presenta en el cuadro 2 la valoración del peligro y la vulnerabilidad[1], en función de la afectación al personal y a la infraestructura física.

Cuadro 2: Evaluación de los peligros

Peligros	Valoración del Peligro	Valoración de la Vulnerabilidad		
		Personal	Infraestructura Física	Promedio
1. Sismo de gran magnitud	Alto	Muy Alto	Muy Alto	Muy Alto
2. Inundación y Aniego	Medio	Bajo	Medio	Medio
3. Incendio	Alto	Muy Alto	Muy Alto	Muy Alto
4. Falla Eléctrica	Medio	Medio	Medio	Medio
5. Pandemia o Epidemia	Medio	Medio	Bajo	Medio
6. Ataque Terrorista	Bajo	Alto	Alto	Alto
7. Disturbios sociales	Medio	Medio	Medio	Medio
8. Actividad Criminal	Medio	Alto	Bajo	Medio
9. Delitos informáticos	Alto	Alto	Bajo	Medio
10. Caída de internet	Alto	Medio	Medio	Medio
11. Debilidad Estructural	Alto	Muy Alto	Muy Alto	Muy Alto
12. Lluvias	Bajo	Bajo	Bajo	Bajo
13. Movimiento en masa	Bajo	Bajo	Bajo	Bajo
14. Tsunami	Bajo	Bajo	Bajo	Bajo
15. Helada y friaje	Bajo	Bajo	Bajo	Bajo
16. Fenómeno del niño	Bajo	Bajo	Bajo	Bajo
17. Deforestación	Bajo	Bajo	Bajo	Bajo
18. Incendios Forestales	Bajo	Bajo	Bajo	Bajo

Fuente: Sesiones BIA. Elaboración de la OGRO

En base a los resultados descritos en el cuadro 2, se obtiene la matriz de riesgos con los 18 peligros identificados, la cual se muestra en el cuadro 3:

Cuadro 3: Matriz de riesgos del PCO

Peligros	Nivel de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
1. Sismo de gran magnitud					x
2. Inundación y Aniego			x		
3. Incendio					x
4. Falla Eléctrica			x		
5. Pandemia o Epidemia			x		
6. Ataque Terrorista			x		
7. Disturbios sociales			x		
8. Actividad Criminal			x		
9. Delitos informáticos				x	
10. Caída de internet				x	
11. Debilidad Estructural					x
12. Lluvias		x			
13. Movimiento en masa		x			
14. Tsunami		x			
15. Helada y friaje		x			
16. Fenómeno del niño		x			
17. Deforestación		x			
18. Incendios Forestales		x			

Fuente: Sesiones BIA. Elaboración de la OGRO

4.2 Determinación del nivel de impacto

En base a los peligros identificados en el cuadro 3 que tengan un nivel de riesgo mayor al nivel "medio", se procede a evaluar en qué medida se ve afectado los procesos que permiten el cumplimiento de la misión y funciones del MEF.

[1] En base a lo estipulado en el "anexo 2 de los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación del Plan de Continuidad de las Entidades Públicas en los tres niveles de gobierno"

Para tal efecto, en base a la evaluación del impacto en los procesos del MEF, realizada con los órganos involucrados en la continuidad operativa, se obtuvo como resultado un indicador del periodo máximo tolerable de interrupción (MTPD) de 72 horas post evento[2].

En el cuadro 4 se muestra las amenazas consideradas en la evaluación, así como su nivel de impacto:

Cuadro 4: Amenazas que impactan la continuidad del MEF

Ministerio de Economía y Finanzas	Impacto de suceder un peligro										
	Sismo	Inundación y Aniego	Incendio	Falla eléctrica	Pandemia o epidemia	Ataque terrorista	Disturbios sociales	Actividad criminal	Delitos informáticos	Caída internet	Debilidad estructural
Procesos que soportan el cumplimiento de la misión del MEF.	Muy Alto	Medio	Muy Alto	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Muy Alto

Fuente: Elaboración de la OGRO

4.3 Identificación de Recursos

4.3.1 Determinación de recursos humanos

El personal determinado para el desarrollo de las actividades en un escenario de continuidad operativa (denominado "**Personal Titular**") lo conforman **101 personas** (41 en modalidad presencial y 60 en modalidad teletrabajo total).

Asimismo, se ha identificado a 99 personas que no intervienen directamente en la ejecución de las actividades relacionadas de la continuidad operativa, pero si participan en la toma de decisiones estratégicas (directores de órganos y miembros del Grupo de Comando) o como apoyo en el escenario de interrupción de operaciones (OSDN, OGRO y OGTI). De estas 99 personas, 98 son considerados como teletrabajo total, y **1 persona** en labores presenciales.

En tal sentido, se ha definido un **total de 200 personas** para la gestión de la continuidad operativa del MEF. Los datos como nombres, teléfono, correo del personal identificado para la continuidad operativa, es administrado en un repositorio de datos compartidos de actualización constante, el cual es administrado por la OGRO y cuyo link es el siguiente \\ws2012-fs.mef.gob.pe\pco

La distribución del personal se resume en el siguiente cuadro.

Cuadro 5: Distribución de personal para la gestión de la continuidad operativa

ÓRGANO	Teletrabajo Total	Trabajo Presencial (Sede Alterna)
▪ **DVMH**	**26**	**25**
DGPP	5	12
DGTP	5	11
DGCP	2	0
DGA	6	2
DGGFRH	8	0

[2] Resultado obtenido en el Análisis de Impacto (BIA) e Incluye el tiempo de respuesta del Plan de Operaciones de Emergencia del Sector Economía y Finanzas (POESEF) y del Plan de Contingencia ante Sismo de Gran Magnitud Seguido de Tsunami frente a la costa central del Perú, del Sector Economía y Finanzas ambos planes en el marco de la Gestión del Riesgo de Desastres (GRD)

ÓRGANO	Teletrabajo Total	Trabajo Presencial (Sede Alterna)
▪ **DVME**	**24**	**11**
DGPMI	2	6
DGPMDF	7	0
DGPIP	4	5
DGPPIP	4	0
DGMFPP	4	0
DGAEICP	3	0
▪ **SG**	**10**	**5**
OGAJ	1	0
OGA	7	3
OGPP	1	0
OGSU	1	2
SUB-TOTAL (Personal Titular)	**60**	**41**
▪ **Alta Dirección**	20	0
▪ **Grupo de Comando**	19	0
▪ **Directivos**	18	0
▪ **OGRO**	0	1
▪ **OGTI**	41	0
SUB-TOTAL (Personal decisiones estratégicas y de apoyo)	**98**	**1**
TOTAL	**158**	**42**

Fuente: Sesiones BIA. Elaboración de la OGRO

4.3.2. Determinación de los recursos físicos críticos

Para el desarrollo de la continuidad operativa, se ha determinado, según el cuadro 5, que 158 personas (entre titulares y de apoyo) realizarán teletrabajo total; no obstante, hay órganos o unidades orgánicas que por la naturaleza de sus actividades críticas necesitan que al menos un personal titular realice trabajo presencial en la Sede Alterna, siendo 42 personas las que podrían desarrollar dichas acciones en la sede alterna.

Para dicho fin, se ha identificado el material y equipo necesario para el desarrollo de sus actividades, los mismos que se muestran en el cuadro 6:

Cuadro 6: Identificación de recursos físicos críticos

Órgano o Unidad Orgánica	Disco duro	Impresora	Credenza melamina	Gabinete metal	Central Telefónica	Switch de red	Teléfonos
DGPP	1	1	1		1	1	6
DGTP	1						5
DGPMI	-	1	1				2
DGPIP	-						1
DGA	-	1		1		1	1
ORH	-						1
Total	**2**	**3**	**2**	**1**	**1**	**1**	**16**

Fuente: Sesiones BIA. Elaboración de la OGRO

4.3.3. Determinación de recursos informáticos e información crítica

a) Equipos informáticos

Se cuenta con setenta y ocho (78) equipos informáticos para el desarrollo de las actividades críticas consideradas en la continuidad operativa; asimismo, se cuenta con cincuenta y seis (56) equipos informáticos para las actividades que no intervienen directamente en la continuidad operativa (Alta Dirección, Grupo de Comando, directivos que no pertenecen al grupo de Comando).

En el cuadro 7 se muestra la distribución de los 134 equipos informáticos:

Cuadro 7: Identificación de recursos informáticos críticos

Órgano	Equipos para Teletrabajo Total	Equipos para trabajo Presencial (Sede Alterna)
▪ **DVMH**	**20**	**25**
DGPP	5	12
DGTP	5	11
DGCP	1	0
DGA	5	2
DGGFRH	4	0
▪ **DVME**	**10**	**11**
DGPMI	1	6
DGPMDF	2	0
DGPIP	3	5
DGPPIP	2	0
DGMFPP	1	0
DGAEICP	1	0
▪ **SG**	**7**	**5**
OGAJ	1	0
OGA	4	3
OGPP	1	0
OGSU	1	2
SUB-TOTAL (Personal Titular)	**37**	**41**
▪ **Alta Dirección**	16	0
▪ **Grupo de Comando**	8	0
▪ **Directivos**	18	0
▪ **OGRO**	0	1
▪ **OGTI**	13	0
SUB-TOTAL (Personal decisiones estratégicas y de apoyo)	**55**	**1**
TOTAL	**92**	**42**

Fuente: Sesiones BIA. Elaboración de la OGRO

b) Servicios informáticos (Aplicativos)

Los servicios informáticos identificados para el desarrollo de las actividades, en un escenario de continuidad operativa, se clasifican en dos grupos: (i) Servicios informáticos administrativos (5 aplicativos); y (ii) Servicio informáticos especiales (20 aplicativos y acceso a link específico al portal MEF). El detalle de cada aplicativo y link específico por usuario se muestra en la siguiente ruta: \\ws2012-fs.mef.gob.pe\pco

Servicios informáticos administrativos:

Cuadro 8: Identificación de servicios informáticos administrativos

PERSONAL	Office	Internet	Correo MEF	STD	Acrobat
Alta Dirección	Todo el personal involucrado en la continuidad operativa				
Grupo de Comando					
Directivos					
Personal involucrado directamente en la GCO					
Apoyo y asesoramiento					

Fuente: Sesiones BIA. Elaboración de la OGRO

Servicios informáticos especiales:

Cuadro 9: Identificación de servicios informáticos especiales

Órgano	SPIJ[3]	SIAF	SIGA	SGP	BI	SISPER	AIRHSP	SIAD	PDT Plame[4]	SINABIP	MIF
DGTP	x	x		x				x			x

[3] No es administrado por la OGTI dado que el servicio es brindado por el Ministerio de Justicia
[4] No es administrado por la OGTI dado que el servicio es brindado por la SUNAT

Órgano	SPIJ[3]	SIAF	SIGA	SGP	BI	SISPER	AIRHSP	SIAD	PDT Plame[4]	SINABIP	MIF
DGPP	x	x	x	x	x		x				
DGA	x	x	x							x	
DGCP	x	x									
DGPMI	x	x	x		x						
DGGFRH	x		x			x	x				
DGPMDF	x				x						
DGPIP	x		x								
DGMFPP	x										
DGAEICP	x										
DGPPIP	x		x								
OGAJ	x										
OGPP	x	x		x			x				
OGSU											
OGA	x	x	x			x	x		x		x

Órgano	Ev. Presup	SICAL	Convenios	CMEF	Carga info	SIMGF	SIGESCO	Vent. Elec.	Cont. APP
DGTP									
DGPP	x	x	x	x	x				
DGA									
DGCP									
DGPMI									
DGGFRH									
DGPMDF						x			
DGPIP									
DGMFPP									
DGAEICP									
DGPPIP									x
OGAJ									
OGPP									
OGSU							x	x	
OGA									

Fuente: Sesiones BIA. Elaboración de la OGRO

c) <u>Información crítica (registros vitales)</u>

La información crítica está relacionada la información depositada en las carpetas compartidas y cuya accesibilidad debe estar disponibles en un escenario de continuidad operativa. Para este fin, se ha identificado 17 órganos y unidades orgánicas que tienen acceso a 52 carpetas compartidas, cuya distribución se muestra en el cuadro 10:

Cuadro 10: Identificación de servicios informáticos especiales

Nro	Órgano	Cantidad de Carpetas compartidas
1	DGTP	7
2	DGPP	5
3	DGA	4
4	DGCP	1
5	DGPMI	1
6	DGGFRH	1
7	DGPMDF	5
8	DGPIP	4
9	DGMFPP	1
10	DGAEICP	1
11	DGPPIP	1
12	OGAJ	2
13	OGPP	1
14	OGSU	3
15	OGA	9

Nro	Órgano	Cantidad de Carpetas compartidas
16	ORH	4
17	OGRO	2
	Total	**52**

Fuente: Sesiones BIA. Elaboración de la OGRO

El detalle de cada ruta de las carpetas compartidas por usuario se muestra en la siguiente ruta: \\ws2012-fs.mef.gob.pe\pco

4.3.4. Determinación de los recursos financieros

Para el desarrollo de las actividades de la continuidad operativa, la Unidad Ejecutora 001-46: MEF – Administración General del pliego Ministerio de Economía y Finanzas cuenta con una asignación presupuestal para la reducción de vulnerabilidades relacionadas con la infraestructura y para la adquisición de recursos tecnológicos.

Como pliego o unidad ejecutora, tiene la posibilidad de ejecutar algunas modificaciones presupuestales, a fin de orientar recursos para las acciones de implementación de la Continuidad Operativa, como ya lo viene ejecutando.

V. ACCIONES PARA LA CONTINUIDAD OPERATIVA

5.1 Determinación de las actividades críticas

Las actividades críticas son las que no pueden interrumpirse porque afectaría el cumplimiento de la misión institucional. Su determinación incluye la identificación de los servicios y proveedores internos y externos críticos para su ejecución, de ser el caso. El detalle de las personas de contacto, teléfonos y correos se encuentran en el siguiente link \\ws2012-fs.mef.gob.pe\pco

Se ha identificado nueve (09) actividades críticas, las mismas que son vinculadas a los macroprocesos del MEF. A continuación, en el cuadro 11 se detalla los órganos que participan por cada actividad, macroproceso así como el periodo máximo tolerable de interrupción (MTPD).

Cuadro 11: Recursos financieros - PIA y PIM del MEF

Nro	Actividad crítica	Macroproceso vinculado	Órgano Involucrado	MTPD
1	Implementar y mantener las capacidades tecnológicas que aseguren la Continuidad Operativa	S03 Gestión de Tecnología de la Información	OGTI	12
2	Brindar asesoría y opinión legal, así como, coordinar requerimientos de opinión a instrumentos normativos propuestos por diversos Sectores	S01 Asesoramiento Jurídico y Defensa Jurídica	OGAJ	24
3	Brindar orientación especializada, así como, de emisión, asistencia y capacitación técnica especializada a entidades públicas	M03 Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	DGTP DGPP DGA DGGFRH DGPIP DGPMI DGAEICP DGPPIP	48
4	Mantener las capacidades para la Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01 Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	DGTP DGPP DGCP DGA DGGFRH DGPMDF DGPIP DGPMI	48

			DGMFPP DGAEICP DGPPIP	
5	Atender las consultas y administrar la gestión documental y archivo, brindando un servicio de calidad al ciudadano y al usuario interno.	S04 Gestión Documental y de Atención al Usuario	OGSU	48
6	Asegurar la programación y asignación de recursos para la provisión de bienes y servicios requeridos en un escenario de continuidad operativa.	S05 Gestión de Recursos Institucionales	OGA-OAB	48
7	Gestión de prensa para difusión en medios de comunicación.	E02 Gestión de la Comunicación e Imagen Institucional	OC	72
8	Gestionar derechos y obligaciones económicas financieras, mediante la programación, gestión y evaluación de los recursos públicos	M02 Administración Financiera del Sector Público	DGTP DGPP DGGFRH DGPMI	72
9	Gestionar el talento humano para asegurar la continuidad operativa del MEF	S02 Gestión del Talento Humano	OGA- ORH	72

Fuente: Sesiones BIA. Elaboración de la OGRO

5.2 Aseguramiento del acervo documentario

Corresponde a la disponibilidad y capacidad de poder contar con la documentación, para lo cual se realiza la correspondiente digitalización, asegurando su valor legal y conservación adecuada.

La Oficina General de Servicios al Usuario (OGSU) cuenta con el Plan Anual de Trabajo Archivístico[5] que se actualiza cada año; este plan contempla actividades de digitalización de documentos con valor legal y valor informativo a cargo del Archivo Central, como medida de contingencia ante cualquier eventualidad y con el objetivo de garantizar la integridad y disponibilidad de dichos documentos.

Asimismo, la Resolución Ministerial N° 348-2020-EF/45 que aprueba la Directiva N° 003-2020-EF/45.01 “Disposiciones para la prevención, conservación y recuperación del acervo documental del Ministerio de Economía y Finanzas en caso de siniestros”, establece medidas preventivas y acciones a fin de evitar la pérdida o deterioro del patrimonio documental en los escenarios de sismo, incendio, inundación y sabotaje.

5.3 Aseguramiento de la Base de Datos mediante la ejecución del Plan de Recuperación de los recursos informáticos

El MEF, para garantizar la continuidad operativa de las diferentes aplicaciones y servicios informáticos, tiene un Centro de Procesamiento de Datos Principal (CPD Principal), un Centro de Procesamiento de Datos de Contingencia (CPD de Contingencia) y un tercer Centro de Procesamiento de Datos del sitio de recuperación de desastres (CPD-DRS).

El Centro de Procesamiento de Datos de Contingencia es una réplica del ambiente de producción del Centro de Procesamiento de Datos Principal, de tal forma que cuando un servicio o aplicación informática presenta algún incidente y no funciona, se puede habilitar el Centro de Procesamiento de Datos de Contingencia para restablecer el servicio o aplicación informática.

El CPD-DRS forma parte de la continuidad operativa, este se habilita cuando el CPD Principal como el CPD de Contingencia ha sufrido un incidente grave que imposibilita

[5] Para el año 2023 se aprobó el plan con Resolución Ministerial N° 274-2022-EF/45 de fecha 03.12.2023

su funcionamiento. En el CPD-DRS sólo se habilitan las aplicaciones críticas para permitir que el MEF pueda realizar sus actividades críticas.

Asimismo, la OGTI ha presentado como estrategia de infraestructura tecnológica alterna la ubicación del CPD-DRS fuera de la ciudad de Lima, ubicándose en la ciudad de Trujillo, departamento La Libertad.

Los CPD Principal y Contingencia están integrados a través de multiplexores interconectados por medio de una fibra óptica dedicada (fibra oscura), cuentan con un sistema de replicación, accesos a Internet con diferentes ISP y una red de datos IP-MPLS para la interconexión con Entidades. Asimismo, albergan la capacidad de procesamiento y almacenamiento de la Institución en operación continúa las 24 horas del día, los 7 días de la semana.

5.4 Roles y Responsabilidades para el desarrollo de las actividades críticas

De conformidad con la normativa vigente, se tienen las siguientes instancias involucradas en la gestión de la continuidad operativa:

- Titular de la Entidad
- Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa
- Grupo de Comando

Las responsabilidades de cada instancia están descritas en el numeral 6.1 de la Resolución Ministerial N° 320-2021-PCM que aprueba los *"Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres Niveles de Gobierno".*

Además de las responsabilidades señaladas en el citado lineamiento, es pertinente el establecimiento de los siguientes roles específicos que asumen los representantes designados por cada órgano o unidad orgánica, como miembros del Grupo de Comando. En el cuadro 12 se muestra los roles.

Cuadro 12: Rol de los órganos y U.O. para la continuidad operativa

N°	Órganos /UO	Roles
1	Secretaría General	o Activar el Plan de Continuidad Operativa a propuesta del el Grupo de Comando. o Disponer la implementación de las decisiones adoptadas por el Grupo de Comando durante el desarrollo de la continuidad operativa.
2	OGRO quien preside el Grupo de Comando	o Asumir la coordinación general de la continuidad operativa. o Convocar a sesión a los miembros del Grupo de Comando. o Adoptar acciones como coordinador para el acceso a la Sede Alterna del MEF, así como la seguridad necesaria para su funcionamiento. o Garantizar que las instancias administrativas del MEF brinden el apoyo administrativo y logístico durante el desarrollo de la continuidad operativa. o Consolidar la información remitida por los órganos miembros del Grupo de Comando. o Reportar a los miembros del Grupo de Comando el cumplimiento de acciones previstas, así como cualquier situación no contemplada que repercuta en el éxito de la continuidad operativa. o Propone a Secretaría General la activación, desactivación del PCO y vuelta a la normalidad previa aprobación en sesión de Grupo de Comando.
3	OSDN	o Adoptar las acciones como director de la emergencia en comité de seguridad, en el marco del plan de seguridad o Adoptar las acciones como coordinador del COES-EF durante y después del evento disruptivo en el marco del plan de contingencia.
4	OGA	o Reportar al jefe (a) de la OGRO el estado de los servicios básicos (luz y Agua) de la Sede Central del MEF y estado de seguridad de la sede central. o Adoptar las acciones como coordinador para la movilización de personal a la Sede Alterna.

		o Realizar las coordinaciones correspondientes con la Policía Nacional -PNP, para garantizar la seguridad externa de la zona afectada
5	OGTI	o Reportar al jefe (a) de la OGRO el estado del Centro de Procesamiento de Datos Principal, Centro de Procesamiento de Datos de Contingencia y Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres luego de un evento disruptivo. o Asumir la activación del Plan de Recuperación de Desastres (DRP) desde la activación del PCO.
6	OC	o Adoptar acciones para la difusión de comunicados internos y externos durante el desarrollo de la continuidad operativa.
7	ORH	o Reportar al Jefe (a) de la OGRO la disponibilidad del personal suplente y alterno involucrado en la continuidad operativa. o Evaluar las interrupciones que afecten o puedan afectar las actividades críticas del órgano o unidad orgánica al que pertenecen y comunicar al Jefe (a) de la OGRO. o Ejecutar el plan de continuidad operativa en el momento que se comunique su activación. o Mantener comunicación constante durante la gestión de crisis y la ejecución del plan de continuidad operativa. o Reportar al Jefe (a) de la OGRO el estado de recuperación de las actividades críticas de los órganos y unidades orgánicas a los que pertenecen. o Participar en la realización de las pruebas de continuidad operativa.
8	DGTP	
9	DGPP	
10	DGA	
11	DGGFRH	
12	DGGPMDF	
13	DGPIP	
14	DGPMI	
15	DGMFPP	
16	DGAEICP	
17	DGPPIP	
18	DGCP	
19	OGAJ	
20	OGPP	
21	OGSU	

Fuente: Sesiones BIA. Elaboración de la OGRO

5.4.1. Cadena de mando

Para el óptimo desarrollo de las actividades relacionadas a la continuidad operativa en el MEF y considerando la participación directa en la toma de decisiones de acuerdo al ROF, se ha determinado la sucesión o Cadena de Mando, la misma que se describe en el cuadro 13 siguiente:

Cuadro 13: Cadena de mando en la continuidad operativa

N°	Instancias	Titular	Alterno
1	Despacho Ministerial	Ministro (a)	Jefe(a) Gabinete de Asesores
2	Despacho Viceministerial de Hacienda	Viceministro (a) de Hacienda	Secretario (a) Ejecutivo(a)
3	Despacho Viceministerial de Economía	Viceministro (e) de Economía	Secretario (a) Ejecutivo(a)
4	Secretaría General	Secretario (a) General	Asesor(a)
5	Directores Generales o Jefes	Director (a) General o Jefe de cada Órgano	Director (a) o Jefe de cada unidad orgánica
6	Directores de Línea o Jefes	Director (a) de Línea o Jefe de cada Unidad Orgánica	Coordinador/Especialistas
7	Grupo de Comando	Representantes designados	Representante alterno

Fuente: Sesiones BIA. Elaboración de la OGRO

Corresponde al Jefe (a) de la OGRO convocar a sesión de Grupo de Comando cuando suceda un evento disruptivo que pueda interrumpir el cumplimiento de la misión y funciones del MEF o cuando amerite una sesión.

5.5 Requerimientos

5.5.1 Requerimiento de Personal

Conforme a lo descrito en el numeral 4.3.1 del presente documento, se ha determinado que para el desarrollo de las actividades en un escenario de continuidad operativa se requiere de 200 personas, de los cuales, 101 personas son titulares (41 en modalidad presencial y 60 en modalidad teletrabajo total) y 99 personas que corresponden a directivos y/o no participan directamente de la continuidad operativa

pero que dan soporte (98 en modalidad teletrabajo total y 1 en presencial). En el cuadro 14 se muestra el resumen del requerimiento de personal.

Cuadro 14: Requerimiento de personal

Requerimiento de personal	Tipo de trabajo		Total Requerido
	Presencial	Teletrabajo Total	
Alta Dirección	0	20	20
Grupo de comando	0	19	19
Directivos que no forman parte del Grupo de Comando	0	18	18
Personal involucrado directamente en la GCO	41	60	101
Apoyo y asesoramiento	1	41	42
Total	**42**	**158**	**200**

Fuente: Sesiones BIA. Elaboración de la OGRO

5.5.2 Requerimiento de Material y Equipo

El numeral 4.3.2 detalla el requerimiento de material y equipo que serán empleados por el personal que realiza trabajo presencial en la sede alterna, en un escenario de continuidad operativa. El cuadro 15 muestra el resumen del requerimiento de material y equipo.

Cuadro 15: Requerimiento de material y equipo

Órgano o Unidad Orgánica	Material y equipo con que se cuenta para la GCO						
	Disco duro	Impresora	Credenza melamina	Gabinete metal	Central Telefónica	Switch de red	Teléfonos
DGPP	1	1	1	0	1	1	6
DGTP	1						5
DGPMI	-	1	1	0			2
DGPIP	-						1
DGA	-	1	0	1		1	1
ORH	-						1
Total	**2**	**3**	**2**	**1**	**1**	**1**	**16**

Fuente: Sesiones BIA. Elaboración de la OGRO

Por otro lado, el cuadro 16 muestra las brechas de material y equipo.

Cuadro 16: Brechas de material y equipo

Órgano o Unidad orgánica	Brechas de materiales y equipos (Requerido)	
	Kit de útiles	USB
DGPP	16	16
DGTP	14	14
DGPMI	6	6
DGPIP	3	3
DGA	2	2
ORH	1	1
Total	**42**	**42**

Fuente: Sesiones BIA. Elaboración de la OGRO

5.5.3 Requerimiento de Recursos Informáticos

El requerimiento de los recursos informáticos incluye los equipos informáticos, los servicios informáticos (aplicativos) y la información crítica (registros vitales) necesarios para el desarrollo de las actividades críticas.

Equipos Informáticos

En base a lo descrito en el numeral 4.3.3, se ha identificado las brechas por equipo informático, el mismo que se muestra en el cuadro 17.

Cuadro 17: Brechas de equipos informáticos

Órgano	Equipos con que se cuenta para GCO		Brecha de equipo informáticos		Total Requerido
	Teletrabajo Total	Presencial (Sede Alterna)	Teletrabajo Total	Presencial (Sede Alterna)	
▪ **DVMH**	**20**	**25**	**6**	**0**	**51**
DGPP	5	12	0	0	17
DGTP	5	11	0	0	16
DGCP	1	0	1	0	2
DGA	5	2	1	0	8
DGGFRH	4	0	4	0	8
▪ **DVME**	**10**	**11**	**14**	**0**	**35**
DGPMI	1	6	1	0	8
DGPMDF	2	0	5	0	7
DGPIP	3	5	1	0	9
DGPPIP	2	0	2	0	4
DGMFPP	1	0	3	0	4
DGAEICP	1	0	2	0	3
▪ **SG**	**7**	**5**	**3**	**0**	**15**
OGAJ	1	0	0	0	1
OGA	4	3	3	0	10
OGPP	1	0	0	0	1
OGSU	1	2	0	0	3
SUB-TOTAL (Personal Titular)	**37**	**41**	**23**	**0**	**101**
▪ **Alta Dirección**	16	0	4	0	20
▪ **Grupo de Comando**	8	0	11	0	19
▪ **Directivos**	18	0	0	0	18
▪ **OGRO**	0	1	0	0	1
▪ **OGTI**	13	0	28	0	41
SUB-TOTAL (Personal decisiones estratégicas y de apoyo)	**55**	**1**	**43**	**0**	**99**
TOTAL	**92**	**42**	**66**	**0**	**200**

Fuente: OGTI. Elaboración de la OGRO

El plan de acción para el cierre de brechas relacionados a equipos informáticos es elaborado por la OGTI y se detalla en el **Anexo 1,** numeral 1.1

a) Servicios informáticos (Aplicativos)

El numeral 4.3.3 del presente documento detalla el requerimiento de los servicios informáticos (aplicativos), los mismos que, luego de la evaluación respectiva con los órganos y unidades orgánicas involucradas en la continuidad operativa, no se requiere recursos informáticos administrativos.

En cuanto los recursos informáticos especiales, a partir del análisis de brechas elaborado por la OGTI en su oportunidad, los cuadros 18 y 19 muestran el estado de las aplicaciones y/o servicios requeridos.

Cuadro 18: Aplicaciones y/o servicios incluidos en el Plan de Recuperación de Desastres -DRP:

Órgano	SPIJ[6]	SIAF	SIGA	SISPER	AIRHSP	SIAD	PDT Plame[7]
DGTP	x	x				x	
DGPP	x	x	x		x		
DGA	x	x	x				
DGCP	x	x					

[6] El MEF accede al aplicativo a tres de internet. La disponibilidad del aplicativo dependerá de Ministerio de Justicia.
[7] El MEF accede al aplicativo a tres de internet. La disponibilidad del aplicativo dependerá de Ministerio de Justicia.

DGPMI	x	x	x				
DGGFRH	x		x	x	x		
DGPMDF	x						
DGPIP	x		x				
DGMFPP	x						
DGAEICP	x						
DGPPIP	x		x				
OGAJ	x						
OGPP	x	x			x		
OGSU							
OGA	x	x	x	x	x		x

Fuente: OGTI. Elaboración de la OGRO

Cuadro19: Aplicativos y/o servicios a incluir en el Plan de Recuperación de Desastres -DRP

Órgano	Ev. Presup	SICAL	Convenios	CMEF	Carga info	SIMGF	SIGESCO	Vent. Elec.	Cont. APP	SGP	BI	SINABIP	MIF
DGTP										x			x
DGPP	x	x	x	x	x					x	x		
DGA												x	
DGCP													
DGPMI											x		
DGGFRH													
DGPMDF						x					x		
DGPIP													
DGMFPP													
DGAEICP													
DGPPIP									x				
OGAJ													
OGPP										x			
OGSU							x	x					
OGA													x

Fuente: OGTI. Elaboración de la OGRO

El plan de acción para el cierre de brechas relacionados a tecnologías de la información es elaborado por la OGTI y se detalla en el **Anexo 1,** numeral 1.1.

b) <u>Información crítica</u>

La información crítica es guardada en las carpetas compartidas por cada órgano o unidad orgánica involucrados en la continuidad operativa. A partir del análisis de brechas elaborado por la OGTI en su oportunidad, se requiere un total de 52 carpetas compartidas distribuidos. El plan de acción para el cierre de brechas relacionados a las carpetas compartidas es elaborado por la OGTI y se detalla en el **Anexo 1,** numeral 1.1. En el cuadro 20 se muestra la brecha de carpetas compartidas.

Cuadro 20: Brecha de carpetas compartidas

Órgano	No cubierto	cubierto	Total de carpetas compartidas requerida
DGTP	6	1	7
DGPP	4	1	5
DGA	4	0	4
DGCP	1	0	1
DGPMI	1	0	1
DGGFRH	1	0	1
DGPMDF	5	0	5
DGPIP	4	0	4
DGMFPP	1	0	1
DGAEICP	1	0	1
DGPPIP	1	0	1

OGAJ	0	2	2
OGPP	1	0	1
OGSU	3	0	3
OGA	9	0	9
ORH	4	0	4
OGRO	2	0	2
Total	**48**	**4**	**52**

Fuente: OGTI. Elaboración de la OGRO

El detalle de equipos informáticos, de aplicativos, información crítica por cada personal y órgano se encuentra en el siguiente link \\ws2012-fs.mef.gob.pe\pco

5.5.4 Requerimiento Presupuestal

En función de las brechas identificadas para el caso de recursos informáticos y recursos de información crítica (registros vitales), la OGTI, en coordinación con la OGA, realizan las acciones para estimar los recursos presupuestales necesarios para cubrir dichas brechas tecnológicas, luego de establecer los criterios para la progresividad de su habilitación.

5.6 Determinación de la Sede Alterna de trabajo

El MEF cuenta con una Sede Alterna que está ubicada en Jr. Elizalde N° 495, Cercado de Lima. Este local pertenece al Banco de la Nación (BN), el cual mediante un Convenio de Colaboración Interinstitucional comparte el espacio físico para el funcionamiento de la Sede Alterna para la implementación del PCO del MEF, el mismo que tiene un periodo de renovación cada dos años, siendo la vigencia de la última renovación hasta el 15.12.2024

La Sede Alterna cuenta con módulos de trabajo de uso compartido, equipado con laptops, impresoras multifuncionales, teléfonos IP y analógico, mini central telefónica y 2 switch para red, con conectividad independiente.

5.7 Activación del Plan de Continuidad Operativa

La activación del Plan de Continuidad Operativa es propuesta por el Grupo Comando al titular de la entidad. Para la activación del citado PCO, el Grupo de Comando gestiona la realización de las acciones de preparación, antes del evento disruptivo, así como las acciones de evaluación, durante y después del evento disruptivo, de acuerdo a lo siguiente:

Antes.

- Realizar campañas de comunicación para difundir el PCO entre todo el personal de la organización.
- Preparar, disponer y verificar los recursos y medios, necesarios para utilizarlos en el momento en que se active el PCO.
- Implementar programas de capacitaciones para el personal involucrado en el PCO.
- Remitir el PCO al INDECI en concordancia de la normativa vigente en coordinación con la secretaria general.
- Realizar ejercicios de simulacros y simulación, como parte de la verificación de la aplicación del PCO.

Durante.

- Al ocurrir un evento disruptivo el Grupo de Comando evalúa la necesidad de activar el PCO.
- Toma conocimiento del impacto producido a la entidad y según la gravedad propone la activación del PCO al titular de la entidad.
- Informa a secretaría general, la situación de la entidad y las acciones de Continuidad Operativa adoptadas.

Después.

- Evaluar las condiciones para la recuperación progresiva de la entidad, a fin de volver a la normalidad.
- Desarrollar acciones de restablecimiento o rehabilitación
- Documentar las lecciones aprendidas sobre el desastre ocurrido.

Ocurrido la materialización de un peligro o cuando éste es reportado por el encargado (a) del Plan de Seguridad de la sede central del MEF, inmediatamente se desarrolla la **Gestión de Crisis**, para tal efecto, el Jefe (a) de la OGRO convoca a sesión de Grupo de Comando virtual o presencial, desarrollándose las siguientes actividades:

- La doble asignación de funciones, que se define como el compromiso y la responsabilidad del personal, de ejecutar funciones en forma temporal y diferente de las que habitualmente desempeña, debido al cambio de la condición de funcionamiento, ante un evento adverso
- Se declara en sesión permanente al Grupo de Comando para la continuidad operativa en el MEF.
- El Jefe(a) de la OGRO solicita al representante de la OSDN, en el marco de la Gestión del Riesgo de Desastres (GRD), se realice las evaluaciones y/o coordinaciones correspondientes.
- Asimismo, el Jefe(a) de la OGRO solicita al representante de la Oficina General de Administración (OGA) se evalúe los daños en la sede central así como identificar el estado de la emergencia, en coordinación con la OSDN si el caso amerita, respecto a la existencia de una amenaza o potencial amenaza que afecte a la vida humana y/o infraestructura física, y que puedan generar una interrupción prolongada de las actividades del MEF.
- El Jefe(a) de la OGRO solicita al representante de la OGTI se evalúe el nivel de afectación al Centro de Procesamiento de Datos Principal, Centro de Procesamiento de Datos de Contingencia y Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres.
- El Jefe (a) de la OGRO solicita a los miembros del Grupo Comando contactar al personal titular y alterno que desarrollan las actividades críticas en los órganos que representan, a fin de que dicho personal inicie actividades en teletrabajo o inicien su traslado a la sede alterna.

Los supuestos que activan el PCO son:

- Daño físico a las instalaciones del MEF, como consecuencia de la materialización de un peligro (sismo, incendio, inundación, debilidad estructural y/o ataque terrorista u otro), imposibilitando el acceso del personal a dicha sede.
- Daño físico al Centro de Procesamiento de Datos, como consecuencia de la materialización de un peligro (sismo, incendio, inundación, debilidad estructural y/o ataque terrorista u otro), imposibilitando el acceso a la información administrada para el MEF.

La activación del PCO es propuesta por el Grupo de Comando al Titular de la Entidad; dicha propuesta es sustentada en base a los resultados de la evaluación reportados

por los representantes de la OGA, la OSDN, la OGTI, así como de la disponibilidad del personal titular y alterno de los órganos que desarrollan las actividades críticas.

Las comunicaciones para la sesión del Grupo de Comando en la gestión de crisis y activación del PCO se desarrolla según se indica en el **anexo 2.**

5.8 Activación y desactivación de Sede Alterna

Acciones para el desarrollo de las actividades críticas en forma presencial en la Sede Alterna.

a) Activación de la Sede Alterna

Una vez activado el PCO, el Jefe(a) de la OGRO realiza las coordinaciones con el gerente de riesgos del Banco de la Nación[8] o quien haga su vez, respecto del ingreso del personal del MEF hacia la sede alterna. Asimismo, en sesión de Grupo de Comando, el Jefe(a) de la OGRO coordina con el representante de la OGTI las acciones para el traslado del personal de soporte TI hacia la Sede Alterna. En **anexo 3** se presenta el directorio del Grupo de Comando.

b) Punto de reunión del personal titular

El Jefe (a) de la OGRO, en sesión de Grupo de Comando y a través de los representantes de los órganos y unidades orgánicas bajo el alcance de la continuidad operativa, convoca al personal titular que requiere ser trasladado a la Sede Alterna. Los puntos de reunión son los siguientes:

Cuadro 21: Puntos de reunión

Supuestos para la continuidad operativa	Punto de reunión del personal titular que realiza trabajo presencial en la Sede Alterna
Durante la hora de trabajo	Plaza de Armas de Lima Esquina Jr. Junín con Jirón Carabaya – Lima
Fuera de la hora de trabajo	Local Alterno – Sede Alterna Jr. Antonio Elizalde 495 – Cercado de Lima, Piso 2 (Altura entre la cuadra 8 y 9 de la Av. Argentina, cercado de Lima)
	Av. Javier Prado Nro. 1115, San Isidro – Sede Tribunal Fiscal

Fuente: Elaboración de la OGRO

c) Traslado del personal titular

Para el traslado del personal titular a la Sede Alterna, se ha previsto dos supuestos para la continuidad operativa:

- **Durante la hora de trabajo**: La OGA traslada al personal clave desde el punto de reunión (Plaza de Armas de Lima) hasta las instalaciones de la Sede Alterna, en coordinación con el Jefe (a) de la OGRO.

- **Fuera de la hora de trabajo**: La OGA traslada al personal clave desde los puntos de reunión indicadas en el literal “b”, hasta las instalaciones de la Sede Alterna, en coordinación con el Jefe (a) de la OGRO.

[8] En concordancia con la cláusula sexta del convenio de colaboración interinstitucional entre el Ministerio de Economía y Finanzas y el Banco de la Nación. **Ver disposiciones de acceso y directorio del Banco de la Nación en Anexo 2 numeral 3.2**

d) Desactivación de la Sede Alterna

El Jefe (a) de la OGRO, en sesión de Grupo de Comando, propone a los representantes de los órganos y unidades orgánicas que están bajo el alcance de la continuidad operativa la culminación de la ejecución de las actividades críticas en la Sede Alterna y recomendará al titular de la entidad desactivación del PCO.

5.9 Desarrollo de las actividades críticas

Se ha identificado nueve (09) actividades críticas, las cuales, en caso de activarse el PCO, éstas serán desarrolladas en la modalidad de trabajo presencial y/o teletrabajo Total.

Trabajo Presencial : Personal titular ejecuta el procedimiento de la MAPRO vinculada a cada actividad crítica, con los equipos informáticos ubicados en la Sede Alterna.

Teletrabajo Total : El personal titular ejecuta el procedimiento de la MAPRO vinculada a cada actividad crítica, con el equipo informático que el personal recibe del MEF.

a) Actividad Crítica 1:

Implementar y mantener las capacidades tecnológicas que aseguren la Continuidad Operativa

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	S03.03.02Diseño, implementación y mantenimiento de la Plataforma Tecnológica	OIT- OGTI	Hardware instalado y Software implementado. Mantenimiento ejecutado
2	S03.03.03Gestión de incidencias de los servicios de Tecnologías de la Información		Incidencias registradas, atendidas y comunicadas al usuario

b) Actividad Crítica 2:

Brindar asesoría y opinión legal, así como, coordinar requerimientos de opinión a instrumentos normativos propuestos por diversos Sectores.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	S01.01.01Asesoría legal a órganos del MEF	OAJH- OGAJ	Informe que absuelve consulta legal.
2	S01.01.02Opinión legal a documentos de gestión e instrumentos normativos		Informe que contiene opinión legal/ Proyecto de Instrumento normativo.
3	S01.03.02Elaboración de Carpeta de la Comisión de Coordinación Viceministerial	OAJEA-OGAJ	Carpeta de la Comisión de Coordinación Viceministerial con opinión.

c) Actividad Crítica 3

Brindar orientación especializada, así como, de emisión, asistencia y capacitación técnica especializada a entidades públicas.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	M03.02.01Emisión de opinión técnica económica y Financiera	DGPP DGGFRH DGPIP DGPMI DGPPIP	Informes de opinión técnica especializada económica y financieramente emitida

2	M03.02.02Emisión de opinión Técnica en análisis de calidad regulatoria - ACR sectorial y multisectorial	DENPC- DGAEICP	Informes de opinión técnica en análisis de calidad regulatoria (sectorial y multisectorial)
3	M03.03.01Asistencia técnica en el marco de la administración financiera del sector Público	DGA DGPMI	Informes de asistencias técnicas ejecutadas
4	M03.03.03Asistencia técnica no vinculada a la administración financiera del sector público	DGPMDF DGPIP	Informes de asistencias técnicas ejecutadas de órganos no SAFI

d) Actividad Crítica 4

Mantener las capacidades para la Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	M01.01.01.01Elaboración de Proyecciones Macroeconómicas y Fiscal	DPM-DGPMDF	Proyecciones macroeconómicas y proyecciones fiscales
2	M01.01.01.02Elaboración del Marco Macroeconómico Multianual	DPM-DGPMDF	Informe de actualización de proyecciones macroeconómicas publicadas
3	M01.01.01.04Seguimiento de Reglas Fiscales	DPF-DGPMDF	Informe trimestral de reglas fiscales
4	M01.01.01.05Análisis del Contexto Macrofiscal	DPM-DGPMDF	Reportes mensual, semanal y diario de análisis de contexto macrofiscal
5	M01.01.02.01Evaluación del Desempeño Fiscal Subnacional	DGPDF-DGPMDF	Informe de evaluación del desempeño fiscal
6	M01.02.01.01.01Elaboración de Lineamientos de Política Tributaria	DGPIP	Informes que lineamiento de política tributaria
7	M01.02.02Gestión de Políticas Nacionales vinculadas al Sector economía y Finanzas	DMF- DGPMDF	Informes de política nacional aprobada
8	M01.03.01Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DN- DGTP DN- DGPP DN- DGCP DN- DGA DN- DGPMI	Expedientes de proyectos normativos, para sistemas administrativos, validado por la Dirección General
9	M01.03.02Elaboración de Instrumentos Normativos distinto de los Sistemas Administrativos	DGGFRH DGMFPP DGAEICP DGPPIP	Expedientes de proyectos normativos, distinto de los sistemas administrativos, validado por la Dirección General
10	M01.04.02Seguimiento y Evaluación de Planes Nacionales Vinculados al Sector Economía y Finanzas	DPIP-DGPPIP	Informe final de seguimiento o evaluación de planes nacionales

e) Actividad Crítica 5

Atender las consultas y administrar la gestión documental y archivo, brindando un servicio de calidad al ciudadano y al usuario interno.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	S04.01.01Recepción Documental.	OGDAU- OGSU	Documentos derivados a órgano respectivo.
2	S04.01.03Administración de Archivos.	OGDAU-OGSU	Transferencia de documentos al archivo central.
3	S04.02.01Atención de consultas	OGDAU-OGSU	Consultas atendidas y registradas
4	S04.02.02Atención de solicitudes de acceso a la información pública	OGDAU-OGSU	Informes de solicitudes acceso a la información pública atendidas

5	S04.02.03 Atención de quejas	OGDAU-OGSU	Notificaciones de atención de quejas
6	S04.02.04 Atención de reclamos	OGDAU-OGSU	Notificaciones de atención de consultas

f) Actividad Crítica 6

Asegurar la programación y asignación de recursos para la provisión de bienes y servicios requeridos en un escenario de continuidad operativa.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	S05.02.02Gestión Presupuestaria Institucional y Modificaciones.	OPICT-OGPP	Notas modificatorias entre UEs aprobadas y ajustes de la PCA aprobada
2	S05.04.03.02Proceso de Contratación	OAB- OGA	Consentimiento de buena pro, contrato menor y/o igual a 8 UIT, orden de compra, orden de servicio
3	S05.04.03.03Ejecución Contractual	OAB-OGA	Contrato suscrito derivado de procedimientos de selección, orden de compra para trámite de pago, orden de servicio para tramites de pago
4	S05.05.02.02Gestión de Pagos	OFI-OGA	Reporte de pago del bien o servicio, comprobantes de pagos emitidos por la unidad ejecutora
5	UTP-FAG.01.01Registros de contratos FAG y PAC	OGA	Contratos o adendas de contratos de los consultores FAG y PAC interno; y externo y sus respectivos registros
6	UTP-FAG.01.02Trámite de pago de los Consultores FAG y PAC	OGA	Reportes de pago PAC y FAG, estructuras cargadas en el PDT-PLAME

g) Actividad Crítica 7

Gestión de prensa para difusión en medios de comunicación.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	E02.01.01Difusión en medios tradicionales y plataformas de comunicación digital.	OC	Notas de prensa, comunicados piezas para redes sociales

h) Actividad Crítica 8

Gestionar derechos y obligaciones económicas financieras, mediante la programación, gestión y evaluación de los recursos públicos.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	M02.01.01Elaboración del programa Multianual de Inversiones del Estado (PMIE)	DPEIP-DGPMI	Programación multianual de inversiones aprobado, cartera de inversiones, criterios de priorización diagnóstico de brechas.
2	M02.01.05.01Estimación y aprobación de la Asignación Presupuestaria Multianual	DPSP-DGPP	APM aprobadas, Estimaciones de CANON, FONCOMUN, RENTA ADUANAS, información de costos de bienes, servicios y obras.
3	M02.01.05.02Desagregación de la APM, Formulación y Aprobación Presupuestaria	DPSP-DGPP	Informes de aprobación de PIA, desagregación de la APM y formulación presupuestaria.

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
4	M02.01.06Administración de la Tabla de Operaciones	DN-DGCP	Tabla de operaciones y plan contable gubernamental actualizado.
5	M02.02.01Gestión de la Inversión Pública	DGI-DGPMI	Reporte de seguimiento a cartera de inversiones priorizada
6	M02.02.02.02Habilitación o Modificación de registros en el AIRHSP	DTRI- DGGFRH	Habilitación o modificación de registros en el AIRHSP
7	M02.02.04.02.01Asignaciones financieras	DOT- DGTP	Nota de asignaciones financieras y notas de transferencia virtual
8	M02.02.04.03.01Pagos de planilla, proveedores y otros	DOT-DGTP	Aprobación de pagos de Planillas y Proveedores y otros, Respuesta del estado de pago de planillas, proveedores y otros. Información de pagos de planillas, proveedores y otros. Giro Aprobado en el SIAF. Registro de Giro de pago fuera del cronograma.
9	M02.02.04.03.09Apertura y cierre de cuentas bancarias	DOT-DGTP	Reporte de aperturas o cierre de cuenta bancaria
10	M02.02.05.01.02.01Concertación de operaciones de endeudamiento publico	DC-DGTP	Contratos de préstamos suscritos, informes, oficios
11	M02.02.05.01.02.05Gestión de la atención del pago de la deuda del gobierno nacional	DADCE- DGTP	Pago de préstamos, suscripciones y bonos, estadísticas de la deuda pública, aprobación de fases de ingreso y gasto
12	M02.02.05.02.02Gestión de los excedentes temporales de liquidez	DGIFMC-DGTP	Adjudicación y rentabilización de los excedentes de entidades del SPNF, rentabilización de excedentes temporales de liquidez del Tesoro Público.
13	M02.02.05.09Determinación de la disponibilidad de fondos públicos	DPE-DGTP	Informe de disponibilidad de fondos públicos
14	M02.02.07.01Programación de compromisos anual (PCA)	DPSP-DGTP	RD de aprobación de la PCA
15	M02.02.07.02Control presupuestario de gastos	DPSP-DGPP	Reporte de análisis de ejecución presupuestal
16	M02.02.07.03.01.01Modificaciones presupuestaria por ingresos de recursos ordinarios y por endeudamiento	DAPT/DPT- DGPP	Decreto Supremo que autoriza la transferencia de partidas por las fuentes de financiamiento Recursos Ordinarios y Recursos por Operaciones Oficiales de Crédito.
17	M02.02.07.03.01.02Modificaciones presupuestarias por otras fuentes de financiamiento	DAPT/DPT- DGPP	Decreto Supremo que autoriza la transferencia de partidas por otras fuentes de financiamiento distintas a RO y ROOC
18	M02.02.07.03.02.01Modificaciones presupuestarias para la continuidad de inversiones	DAPT/DPT- DGPP	Decreto Supremo que autoriza la transferencia de partida por continuidad de inversiones
19	M02.02.07.03.02.02Modificaciones presupuestarias por transferencia del programa de incentivos	DAPT/DPT- DGPP	Decreto Supremo que autoriza la transferencia de recursos del Programa de Incentivos
20	M02.02.07.03.02.03Modificaciones presupuestarias por transferencia de la reserva	DAPT/DPT- DGPP	Decreto Supremo que autoriza la transferencia de partidas de la reserva
21	M02.02.07.03.02.04Modificaciones presupuestarias por transferencia entre pliegos	DAPT/DPT- DGPP	Decreto Supremo que aprueba la Transferencia de partidas entre Pliegos

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
22	M02.02.07.03.03Modificaciones presupuestaria a nivel funcional y programático	DAPT/DPT- DGPP	Modificación Presupuestaria de Nivel Funcional y programática aprobada
23	M02.02.07.04.01Reconocimiento a la ejecución de inversiones y programa de incentivos	DGCP-DGPP	Resolución Directoral de resultados complementarios
24	M02.02.07.04.02Gestión de convenios de apoyo y presupuesto	DGCP-DGPP	Informe de verificación del cumplimiento del convenio, Asignación de monto para transferencia financiera
25	M02.03.04.01.01Creación y/o modificación de indicadores de intervenciones	DGCP-DGPP	Creación y modificación de indicadores de intervenciones
26	M02.03.04.01.02Programación de metas de indicadores	DGCP-DGPP	Programación de metas de indicadores
27	M02.03.04.01.03Elaboración de Reportes de valores reales de los indicadores de programas presupuestales	DGCP-DGPP	Informe de Evaluación de Indicadores
28	M02.03.04.02.01Evaluación de diseño y procesos de intervenciones públicas	DGCP-DGPP	Matriz de desempeño de compromisos de evaluación de diseño y procesos de intervenciones públicas
29	M02.03.04.02.02Evaluación de impacto de intervenciones públicas	DGCP-DGPP	Matriz de desempeño de compromisos de la evaluación de impacto de intervenciones
30	M02.03.04.02.03Evaluación de revisión de gastos de intervenciones públicas	DGCP-DGPP	Matriz de desempeño de compromisos de la evaluación de revisión de gasto de intervenciones públicas
31	M02.03.04.02.04Elaboración del informe global de gestión presupuestaria	DGCP-DGPP	Informe Global de Gestión Presupuestaria

i) Actividad Crítica 9

Gestionar el talento humano para asegurar la continuidad operativa del MEF

N°	Tarea/Procedimiento a ejecutar	Responsable	Información crítica
1	S02.02.02.02Gestión de procedimiento Administrativo Disciplinario	ORH- OGA	Acto administrativo que concluye el PAD notificado
2	S02.03.02Elaboración de Planilla única de Pago	ORH-OGA	Planilla Única de Pago emitida, Archivo de abono al Banco TX
3	S02.05.01Gestión de la Seguridad y Salud en el Trabajo	ORH-OGA	Resultados de la aplicación del Plan de Seguridad y Salud en el Trabajo

En **anexo 4** se detalla el servicio por cada proveedor interno y externo para la ejecución de las actividades críticas, en concordancia con cada procedimiento. Asimismo, en **anexo 5** se detalla el protocolo de comunicación interna y externa una vez activado el PCO.

VI. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

El Plan de Continuidad Operativa del MEF responde a la realidad y a las necesidades de garantizar la continuidad de sus actividades críticas, es por ello que se hace necesario programar ensayos, simulacros y simulaciones, que permitan medir la operatividad de este Plan.

El objetivo principal que se persigue al realizar los ejercicios es determinar el nivel de respuesta deseado para la continuidad operativa y la capacidad para gestionar las actividades críticas predeterminadas.

Cada ejercicio a realizar es organizado por la OGRO en coordinación con los miembros del Grupo de Comando, sin que ello interrumpa el normal funcionamiento del MEF.

El cronograma anual de ejercicios del Plan de Continuidad Operativa del MEF se detalla en el cuadro 22:

Cuadro 22: Puntos de reunión

N°	Fecha	Supuesto	Responsable
1	Última semana del mes de mayo	Incendio código 3, que afecte severamente la sede principal	Grupo de Comando
2	Segunda semana del mes de setiembre	Ataque informático, que ocasione el colapso total de los sistemas de información del MEF	
3	Primera semana del mes de noviembre	Sismo de 8.5 de magnitud momento, que afecte totalmente a la sede central	

Fuente: Elaboración de la OGRO

El Grupo de Comando es responsable de realizar la actualización del PCO. Esta acción se basa en seis criterios descritos en el cuadro 23:

Cuadro23: Puntos de reunión

Criterio	Descripción
Criterio 1	Modificación del Reglamento de Organización y Funciones de la entidad o cualquier otro documento de gestión institucional similar.
Criterio 2	Modificación parcial de la estructura, función u organigrama de la institución o de las unidades orgánicas a cargo de actividades críticas.
Criterio 3	Modificación total de la estructura, función u organigrama de la entidad o de las unidades orgánicas a cargo de actividades críticas.
Criterio 4	Ejecución de ensayos y pruebas cuyos resultados sugieren una mejora continua parcial o total del Plan
Criterio 5	Actualización por el periodo de tiempo transcurrido, después de dos (2) años de vigencia
Criterio 6	Actualización por modificación del marco normativo nacional sobre Continuidad Operativa.

Fuente: Elaboración de la OGRO

En **anexo 6** se describe el cronograma de implementación del PCO y las actividades a desarrollar.

VII. ANEXOS

Anexo 1: Plan de Recuperación de los servicios informáticos.

Anexo 2: Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades críticas

Anexo 3: Directorio del Grupo de Comando.

Anexo 4: Organización para el desarrollo de las actividades críticas

Anexo 5: Sistema de comunicaciones de emergencia.

Anexo 6: Cronograma de implementación de la Gestión de la Continuidad Operativa.

ANEXO 1: Plan de recuperación de los servicios informáticos

HISTORIAL DE REVISIONES

Versión	Fecha	Detalle de cambios realizados	Elaborado por:	Revisado por:	Aprobado por:
1.0	31.05.2016	Adaptación de entregables desarrollados por firma consultora ISEC Information Security del Perú mediante proceso de contratación AMC-072-2014-EF/43.	Delfor Chacón Cornejo José Visalot Trujillo	Jorge Ávila Elías Julio Molina Gárate	Percy Caro Céspedes
1.1	16.06.2016	Aplicación de elementos gráficos según Manual de Identidad Gráfica del MEF.	Delfor Chacón Cornejo	Julio Molina Gárate Jorge Ávila Elías	Percy Caro Céspedes
2.0	20/07/2021	Estructura de contenidos modificada. Referencias al Plan de Recuperación de Desastres – DRP y a los Centros de Procesamiento de Datos (CPD). Actualización de roles. Inclusión de subtipos de pruebas operacionales. Mejoras de redacción en general.	Delfor Chacón Cornejo José Romucho Sotelo	Raúl Tapia Diaz Julio Molina Gárate	Eduardo Ibarra Santa Cruz
3.0	22/10/2021	Consolidación de Plan de Contingencia Informático, Plan de Recuperación de Desastres – DRP y Plan de Pruebas de Contingencia Informática.	José Romucho Sotelo Rolly S. Villegas Delgado	Raúl Tapia Diaz	Eduardo Ibarra Santa Cruz
4.0	19/11/2021	Consolidación de Plan de Recuperación de Desastres – DRP	José Romucho Sotelo Rolly S. Villegas Delgado	Raúl Tapia Diaz	Eduardo Ibarra Santa Cruz
5.0	25/05/2023	Actualización de Plan de Recuperación de Desastres – DRP	José Romucho Sotelo Rolly S. Villegas Delgado	Raúl Tapia Diaz	Eduardo Ibarra Santa Cruz

ÍNDICE

1. PLAN DE RECUPERACIÓN DE DESASTRES – DRP

1.1. SECCIÓN I: OBJETIVO Y ALCANCE DEL PLAN

1.1.1. Introducción

El Plan de Recuperación de Desastres, tiene como objetivo ser una guía para la coordinación efectiva y el restablecimiento de los servicios críticos que provee el Ministerio de Economía y Finanzas, en adelante el MEF, a las diversas áreas internas, así como también los servicios que se brinda a nivel nacional, ante un evento que incapacite su infraestructura tecnológica inhabilitando el uso de sus CPD Principal y CPD de Contingencia de manera total.

El presente documento denominado “Plan de Recuperación de Desastres”, tiene como finalidad establecer los controles adecuados en los sistemas informáticos, que se requiere que sean preparados y programados con anticipación a fin de mantener la continuidad del servicio, el presente plan está compuesto conformado por “Plan de Recuperación de desastres - DRP” y “Plan de Pruebas”, dichos documentos se deben mantener y actualizar periódicamente, así como también deben ser autorizado y aprobados.

Cabe precisar que el riesgo en tecnologías de la información, se define con la posibilidad de ocurrencia de pérdida o incapacidad de cumplir correctamente con los objetivos del Ministerio de Economía y Finanzas, debido a los daños, interrupción, alteración o fallas derivadas de los sistemas físicos (hardware) o lógicos (software), sistemas y/o aplicaciones, redes y cualquier otro mecanismo de distribución de la información que resulten necesarias para la ejecución de procesos operacionales por parte del Ministerio.

La OGTI, ha elaborado el presente “Plan de Recuperación de Desastres”, que tiene como objetivo definir un conjunto de medidas para enfrentar adecuadamente a eventos de desastre o de interrupción de las operaciones de los sistemas informáticos esenciales del Ministerio, de tal forma que se restablezcan los servicios y sistemas de información afectados dentro de un periodo aceptable para el negocio.

1.1.2. Alcance

Plan de Recuperación de Desastres, contiene toda la información y pasos necesarios con la finalidad de habilitar los servicios críticos del MEF en el Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres - CPD DRS. Asimismo, se detalla las aplicaciones y servicios, configuraciones de redes, configuraciones de seguridad y publicaciones. También se detalla los diversos equipos de “Continuidad de TI” conformados por: Líder de Continuidad de TI, Especialista de TI, Administradores de base de datos, Administradores de redes y comunicaciones, Administrador de seguridad Informática, Soporte Tecnológico y Desarrollo de APP. Todo ello con la finalidad de minimizar el impacto ante posibles eventos disruptivos y asegurar la operatividad de los servicios críticos del MEF.

1.1.3. Propósito

El Plan de Recuperación de Desastres (DRP), tiene como objetivo ser una guía para la coordinación efectiva y el restablecimiento de los servicios críticos que provee el Ministerio de Economía y Finanzas, en adelante el MEF, a las diversas áreas internas, así como también los servicios que se brinda a nivel nacional, ante un evento que incapacite su infraestructura tecnológica inhabilitando el uso de sus CPD Principal y CPD de Contingencia de manera total.

1.1.4. Situación Actual

El Ministerio de Economía y Finanzas con la finalidad de garantizar la disponibilidad de los servicios cuenta con tres (3) Centros de Procesamiento de Datos:

- ✓ CPD Principal (GTD, Calle Enrique Villanueva 105 – Surco)
- ✓ CPD Contingencia (Lumen, Av. Manuel Olguin 381 Surco)
- ✓ CPD DRS – Sitio de Recuperación de Desastres (Av. Larco 857, Trujillo)

Ubicados en sitios distintos, conectados por fibra oscura, diseñado y construido con especificaciones establecidas por los estándares y recomendaciones de UPTIME INSTITUTE para un tipo TIER III, para el CPD Principal y CPD Contingencia garantizan un nivel de disponibilidad mínimo de 99.982% anual.

La infraestructura de cómputo está compuesta de:

- ✓ Servidor de Bases de Datos
- ✓ Servidor de Aplicaciones Web y C/S.
- ✓ Servidor Web.
- ✓ Servidores de correo electrónico
- ✓ Servidores de directorio activo
- ✓ Servidores File Server

1.1.5. Descripción General

El Plan de Recuperación de Desastres, en adelante DRP, constituye una herramienta que permitirá a la Oficina de Infraestructura Tecnológica – OGTI del Ministerio de Economía y Finanzas continuar con sus operaciones críticas en el menor tiempo posible a través de la recuperación de los recursos críticos de TI que soportan la operatividad de sus procesos críticos del SIAF-SP, ante un evento que incapacite su infraestructura tecnológica inhabilitando el uso de su CPD Principal y CPD de Contingencia de manera total.

El presente documento incluye el propósito, descripción general y objetivos del DRP, la organización de los equipos de continuidad de TI, los procedimientos de recuperación de TI y la metodología de Pruebas del DRP. Asimismo, presenta la relación de aplicaciones críticas de TI definidos en función de los procesos críticos del Ministerio de Economía y Finanzas.

El DRP contiene toda la información necesaria para recuperar los servicios críticos del Ministerio de Economía y Finanzas, considerando los procedimientos para la puesta en funcionamiento de equipamiento alojado en el CPD DRS (Housing Trujillo), que le permita operar en condiciones de contingencia al MEF.

Las actualizaciones, aprobaciones y distribución del presente documento son responsabilidad de la Oficina de Infraestructura Tecnológica OIT de la OGTI, y deberán efectuarse en coordinación con el responsable del mantenimiento del

Plan de Continuidad Operativa y con las áreas críticas del Ministerio de Economía y Finanzas.

Este plan está basado en la conformación de equipos y grupos, y sus responsabilidades para cada una de las fases de un evento que afecta la Continuidad de TI, las cuales se han definido a manera que permitan la ejecución de las actividades de recuperación y sostenibilidad del presente DRP en el tiempo.

El siguiente gráfico resume las fases que garantizan la vigencia de las estrategias de recuperación de un evento de continuidad TI:

Antes del Desastre
El enfoque presentado comprende actividades de prevención para reducir el impacto del desastre y preparación para contar con la información respaldada necesaria para recuperar los servicios críticos en caso de desastre.

Durante el Desastre
Las actividades de Respuesta al incidente, Activación y Operación en Contingencia, permiten habilitar los servicios de TI para que operen en modo contingencia. El cumplimiento de las actividades previas al desastre garantizará el éxito en la presente etapa, de lo contrario todo esfuerzo que se realice demandará gastos imprevistos e impactos no esperados.

Después del Desastre
Las actividades de Reparación y Retorno a la Normalidad, permiten restaurar las operaciones en el centro de cómputo principal una vez que los daños fueron reparados y la Oficina de Seguridad y Defensa Nacional acredite las condiciones adecuadas para la puesta en marcha en condiciones normales.

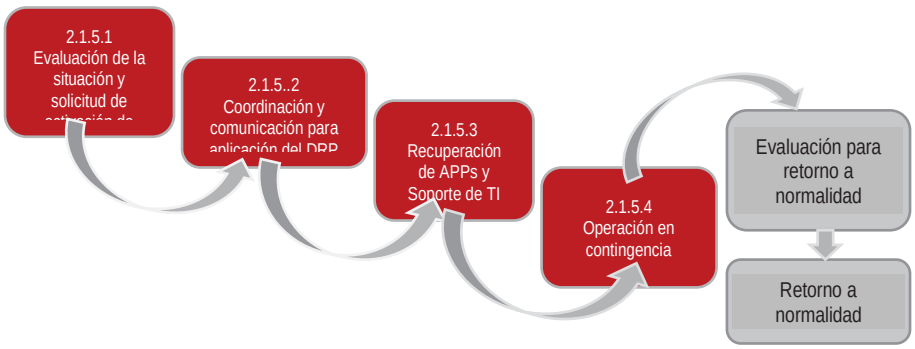
1.1.6. Objetivo general del DRP
Definir el marco necesario que permita asegurar la operatividad de los servicios y/o aplicaciones de tecnologías de la información que son considerados como servicios críticos por el Ministerio de Economía y Finanzas, ante eventos disruptivos que impacte de manera parcial o total y garantizar de esta forma que se continúe prestando los servicios de TI esenciales para la continuidad operativa.

1.1.7. Objetivos específicos del DRP
El DRP tiene como objetivos específicos los siguientes:

- ✓ Definir las actividades y pasos a realizar como parte del entrenamiento para las pruebas de contingencia que permita tener los conocimientos y habilidades necesarios, a fin operar en contingencia ante eventos disruptivos que afecten los servicios del MEF.
- ✓ Organizar los diversos equipos de trabajo que permitan realizar la habilitación de los servicios de TI en contingencia.
- ✓ Definir las actividades y estrategias que permitan que permitan cumplir los objetivos del DRP para una correcta operación antes, durante y después de un evento.
- ✓ Definir el escenario de desastre para los cuales aplican los procedimientos de recuperación y operación en contingencia descritos en el presente documento.
- ✓ Señalar los recursos de tecnología de información y aplicaciones críticas de forma que se pueda priorizar la asignación de recursos para su recuperación en caso de ocurrir una contingencia.
- ✓ Planificar las acciones a seguir para permitir la continuidad operativa, definiendo estrategias y procedimientos que aseguren la recuperación de los servicios que brinda el Ministerio de Economía y Finanzas, en caso de una seria interrupción de los servicios de cómputo en el Centro de Computo Principal.

1.1.8. Flujo Macro del DRP durante el desastre

A continuación, se describe un flujo macro de actividades que se llevarán a cabo durante el desastre:



1.1.8.1. Evaluación de la situación y solicitud de activación de contingencia

Notificación del Evento

El Líder de Continuidad de TI debe realizar lo siguiente:

- ✓ Indagar sobre el evento ocurrido, lugar del evento, componentes afectados, efecto ocasionado, etc. Si fuera un evento interno, deben contactar a la persona de soporte apropiado para obtener un primer diagnóstico.
- ✓ Notificar al Director de la Oficina de Infraestructura de la OGTI la situación que ha generado el evento de desastre o interrupción mayor con respecto a los servicios tecnológicos.
- ✓ El Director de la Oficina de Infraestructura Tecnológica de la OGTI, envía la notificación al Director General de Tecnologías de la Información con los detalles del evento, la fuente y el primer

diagnóstico, así como una estimación del tiempo de interrupción de los servicios tecnológicos afectados.

- ✓ El Director General de Tecnologías de la Información realizará las coordinaciones con el equipo de Comando del MEF, para la declaración de la contingencia Informática.

Evaluación de Daños

- ✓ Líder de Continuidad de TI coordina con los responsables de los componentes afectados y proveedores externos de TI involucrados, para verificar y evaluar los daños del equipamiento alojado en los CPD Principal y CPD Contingencia.
- ✓ En caso de contar con equipamiento operativo en alguno de los CPD Principal y Contingencia para algunos servicios y aún se cuente con comunicación a estos, evaluar su capacidad de habilitar la totalidad de los servicios críticos y poder prescindir de la contingencia en el CPD DRS.
- ✓ El reporte de evaluación de daños debe ser enviado al Director de la Oficina de Infraestructura Tecnológica de la OGTI, donde se le informará la descripción del daño, una evaluación preliminar, consecuencias y acciones prioritarias a realizar.
- ✓ El Director de la Oficina de Infraestructura Tecnológica de la OGTI, luego de revisar y analizar el reporte de evaluación de daños, solicita la autorización para activar el DRP al Director General de Tecnologías de la Información.

  El Director General de Tecnologías de la Información, mantendrá informado al Grupo de Comando del MEF sobre la ejecución del plan.

DIRECTORIO DE CONTACTOS								
N°	**Apellidos**	**Nombres**	**Cargo actual**	**Telf. MEF**	**Telf. Personal**	**Anexo**	**Telf. Misión Critica Tetra**	**Correo electrónico**
Oficina General de Tecnologías de la Información								
1	Eduardo Carlos	Ibarra Santa Cruz	Director OGTI	+51 981 680 039	*	3401		eibarra@mef.gob.pe
2	Tapia Díaz	Vicente Raúl	Director OIT	+51 993 878 816	*	3601		vtapia@mef.gob.pe
3	Molina Garate	Julio	Director GobTI		+51 5966 342 396	3602		jmolina@mef.gob.pe
4	Robles Cruz	Agustin	Director OSI		+51 5995 099 774	3408		arobles@mef.gob.pe
5	Romucho Sotelo	Jose	Coordinador del Centro de computo	+51 975 695 085		4118		jromucho@mef.gob.pe
6	Villegas Delgado	Rolly	Especialista en Administración de Sistemas	+51 965 366 887		4121		rvillegas@mef.gob.pe
Oficina General de Integridad Institucional y Riesgos Operativos								
1	Santillán Ramírez	Segundo Marcos	Director de la Oficina de Gestión de Riesgos Operativos	+51 991 349 867		2298		msantillan@mef.gob.pe

1.1.8.2. Coordinación y comunicación para aplicación del DRP

Activación del DRP

- ✓ El Director General de Tecnologías de la Información evalúa la activación del DRP, en base a la información proporcionada por el al Director de la Oficina de Infraestructura Tecnológica de la OGTI, sobre el evento desastre registrado.
- ✓ Una vez que el Director General de Tecnologías de la Información apruebe la activación del DRP, deberá notificar a todo el equipo de continuidad de TI, el inicio de la operación en contingencia.
- ✓ El Director General de Tecnologías de la Información comunica la Director de la Oficina de Infraestructura Tecnológica de la OGTI la aprobación de activación del DRP y este a su vez comunicará a todo el equipo tecnológico encargado de la recuperación.

1.1.8.3. Recuperación de APPS y soporte de TI

Actividades para restablecer los servicios del MEF en el CPD DRS.

Nro.	Componente	Descripción de la Tarea
1	Detener Replicas	El equipo de Especialistas de TI realizará las tareas para detener las réplicas.
2	Habilitar Enlaces	El equipo de Redes y Comunicaciones realizarán las configuraciones necesarias.
3	Habilitar redes y publicaciones	El equipo de Seguridad Informática realizará las configuraciones necesarias.
4	Habilitar plataforma de servidores	El equipo de Especialistas de TI realizará las tareas para habilitar la plataforma de servidores y base de datos.
5	Habilitar equipamiento de usuarios en el CAN	El equipo de Soporte Tecnológico habilitará los equipos de los usuarios en el CAN.
6	Iniciar servicios	El equipo de Especialistas de TI realizará las tareas para habilitar los servicios.
7	Validar funcionalidades de aplicaciones y base de datos.	El equipo de Desarrollo de APPS realizará la validación de los servicios de base de datos y aplicaciones en contingencia.

1.1.8.4. Operación en contingencia

Durante el periodo de operación en contingencia, los diversos equipos brindarán el soporte operativo de la plataforma en contingencia, como se realiza durante la fase de operación normal. Luego de superado el incidente que originó la activación del DRP y cuando se cuenten con las condiciones adecuadas para regresar a la operación normal se debe realizar una evaluación, la cual se detalla a continuación.

Evaluación para retorno a normalidad

Una vez operando en contingencia, se iniciará el proceso de definición de estrategias para retorno a la normalidad, que consiste en volver a operar en el CPD Principal. Este proceso define las siguientes etapas:

a) **Evaluación**: Donde se debe considerar el estado del CPD Principal y CPD Contingencia o elementos siniestrados. Si la magnitud del siniestro alcanza otros elementos o circunstancias fuera del ámbito de tecnología este proceso es liderado por el líder del Plan de Continuidad. Si el siniestro está circunscrito

exclusivamente al ámbito de tecnología este proceso será liderado por el líder de Continuidad de TI. En esta etapa se debe establecer:

a. Nivel de operatividad del CPD Principal y CPD Contingencia.
b. Elementos Faltantes para la operatividad del CPD Principal y CPD Contingencia al 100%.

b) **Definición de Restablecimiento**: Se debe definir las alternativas de restablecimiento de la operatividad de los CPD Principal y CPD Contingencia, estableciendo:
   a. Las necesidades de infraestructura y tecnología para regresar a la operatividad y ejecutar el retorno
   b. Alternativas para cubrir las necesidades identificadas
   c. Estrategia del retorno de operaciones al CPD Principal y CPD Contingencia
c) **Planificación**: Establecer un plan de actividades necesarias para la habilitación del Centro de Procesamiento Principal, incluyendo tiempos de adquisiciones e implementaciones.
d) **Reparación**: Esta etapa consiste en la ejecución del Plan de habilitación de los CPD Principal y CPD Contingencia.
e) **Pruebas**: Verificación del correcto funcionamiento de lo implementado, infraestructura, elementos tecnológicos y aplicaciones. También debe incluir pruebas de los componentes tecnológicos que intervienen en el momento del retorno.
f) **Retorno a la Normalidad**: Ejecución del Cambio.

1.1.9. Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres - CPD DRS

El CPD DRS es el lugar asignado para recuperar la funcionalidad necesaria del CPD principal del Ministerio para soportar la ejecución de los procedimientos críticos del negocio.

El CPD DRS se encuentra ubicado en las instalaciones de la empresa GTD PERU como parte del servicio de housing, ubicado en la Av. Larco N° 857 – Trujillo.

El Ministerio de Economía y Finanzas como parte del proyecto de adquisición de hardware y software para renovar la infraestructura del centro de cómputo principal y respaldo del Ministerio de Economía y Finanzas, código único de inversión N° 2455051, ha implementado el equipamiento para habilitar los servicios en CPD DRS, ante un evento que incapacite su infraestructura tecnológica inhabilitando el uso de sus CPD Principal y CPD de Contingencia de manera total.

Adicionalmente, como parte de la Contratación del servicio de Housing para la plataforma tecnológica del Ministerio de Economía y Finanzas, se cuenta con un housing en la ciudad de Trujillo que permitirá habilitar los servicios ante escenarios de desastres.

Para habilitar los servicios en el Centro de Procesamiento de Datos de Recuperación de Desastres – CPD DRS, se detallan a continuación los servicios y equipamiento implementado:

Como parte del proyecto de renovación tecnológica se ha implementado nuevo equipamiento para Base de Datos, Aplicaciones y Seguridad Perimetral en el CPD DRS, permitiendo replicar y asegurar la información de los distintos servicios y/o aplicaciones críticas del Ministerio de Economía y Finanzas como el SIAF-SP (Base de Datos y Aplicaciones).

Características principales:

- ✓ El CPD DRS tiene adoptadas medidas de seguridad en sus instalaciones para el control de acceso a las personas expresamente autorizadas.
- ✓ Espacio de alojamiento para los equipos del Centro de Cómputo (servidores y equipos de comunicación) en un Rack debidamente acondicionado.
- ✓ Están habilitados los servicios requeridos:
  - Servidor RISC para Base de Datos – IBM Power9.
  - Sistema de Almacenamiento para base de datos y aplicaciones
  - Servidores de aplicaciones, web, file server y c/s.
  - Servidor controlador de dominio.
  - Servidor de correo electrónico Exchange
  - Solución de Firewall de capa 3 y 4
  - Servicio de Internet
  - Enlace de FO (MEF – CPD DRS).
  - Enlaces de comunicaciones (BN, DRS, RENIEC, CAN).

1.1.10. Relación de Aplicaciones Críticas de TI

El nivel de criticidad de los recursos de TI ha sido establecido en función a las aplicaciones de servicios críticos según lo especificado en el Anexo 3.1 - Inventario de aplicaciones.

Las aplicaciones de servicios críticos son componentes básicos para el funcionamiento de los procesos críticos del Ministerio de Economía cuya paralización haría que el MEF no brinde los servicios a nivel nacional.

1.1.11. Escenarios de Desastre

El presente Plan de Recuperación de Desastres se ha elaborado ante un **escenario de indisponibilidad total** ante un evento que incapacite su infraestructura tecnológica inhabilitando el uso de sus dos CPD Principal y CPD de Contingencia de manera total. Este escenario se puede dar ante una catástrofe, terremoto, incendio, derrumbe, inundación, entre otros.

1.1.12. Tiempos Objetivo (RTO y RPO)

Dos de los parámetros importantes son el Objetivo del Punto de Recuperación (RPO, por sus siglas en inglés) y el Objetivo del Tiempo de Recuperación (RTO, por sus siglas en inglés).

RPO es importante porque, en la mayoría de los casos, la pérdida de datos será inevitable. Incluso la información respaldada en tiempo real corre el

riesgo de perderse para siempre, el RPO mide cuánta información se puede perder producto de un desastre.

Para el punto objetivo de recuperación RPO, el Ministerio de Economía y Finanzas cuenta con una política de backup que se realizan a los activos de la información a nivel de software:

Bakups de Software: Este se ejecuta en horas de la noche según la tarea programada, la información es almacenada en storage de la solución de backups y es llevada a las cintas de almacenamiento para ser organizada por el robot de cintas dispuesto para este fin, una vez terminada la copia en cinta son almacenada en las Cintotecas de los CPD Principal y CPD Contingencia.

La descripción de frecuencia, tipo de backup y sistema, se adjuntan en los Anexos 2 - Inventario de Backups.

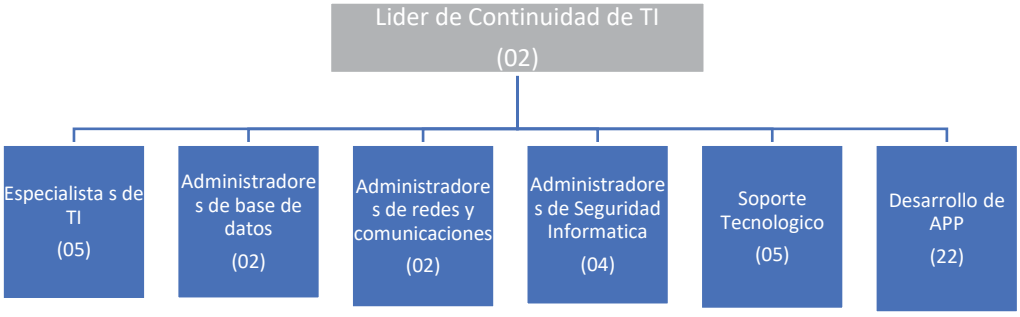
El RTO está relacionado con el tiempo de inactividad, y representa cuánto se tarda la restauración desde el incidente hasta que las operaciones normales estén disponibles para los usuarios.

El tiempo objetivo de recuperación RTO, de los servicios especificados en el Anexo 3.1 Inventario de Aplicaciones, un RTO de 3 horas permite una recuperación empezando por el bare metal y terminando con una disponibilidad completa de aplicaciones y datos en el CPD DRS, ver Anexo 3.2 - RPO y RTO de los Servicios Críticos y no críticos. Asimismo, el RPO máximo es de 15 minutos.

1.1.13. Organización de Equipos de Continuidad de TI

La función principal del Equipo de Continuidad de TI es la recuperación de los recursos y aplicaciones críticas en el CPD DRS, a fin de garantizar la operatividad de los procesos críticos descritos en el DRP y que serán ejecutados por los equipos de continuidad en el CPD DRS. Esta función a su vez tiene como punto de partida las funciones relacionadas a la prevención y preparación que permitirán mantener vigente el plan y las estrategias que asegurarán la recuperación de los recursos y aplicaciones de servicios críticos en el CPD DRS.

Se han definido siete (07) equipos de Continuidad de TI que se encuentran conformado por 42 personas, distribuido de acuerdo al siguiente organigrama:



La responsabilidad de cumplimiento recae sobre el Líder de Continuidad de TI. Las funciones y responsabilidades podrán ser asignadas a los Líderes de los Grupos de Continuidad de TI. Asimismo, los datos como nombres, teléfono, correo del personal identificado para la continuidad TI, se encuentra detallado en el documento "**Anexo 12 – Equipo de Continuidad de TI"**.

Equipo N◦ 01: Líder de Continuidad de TI

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Líder	Una vez recibida la notificación del desastre a través del Director de la Oficina de Infraestructura Tecnológica y la confirmación de la implementada la infraestructura en el CPD DRS.
2		**Activación**
2.1	Líder	Coordinar y monitorear las actividades de recuperación, en comunicación permanente con los líderes de cada grupo.
2.2	Líder	Informar al Director de la Oficina de Infraestructura Tecnológica sobre la situación de las tareas de recuperación de los servicios críticos en el CPD DRS
2.3	Líder	Revisar con los coordinadores los informes de ocurrencia y resultado de la ejecución de los procedimientos de recuperación de los recursos críticos del MEF por cada uno de los grupos de recuperación, antes de ponerlos en servicio.
2.4	Líder	Notificar el inicio de la Operación en Contingencia.
3		**Operación en Contingencia**
3.1	Líder	Gestionar los recursos necesarios para la operación en contingencia del Ministerio de Economía y Finanzas.
3.2	Líder	Coordinar con la Dirección y los líderes de cada grupo las actividades durante la operación en contingencia.
3.3	Líder	Coordinar y monitorear las actividades de operación en contingencia, en comunicación los líderes de cada grupo.

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Coordinador del Centro de Computo
2	Especialista en Administración de Sistemas

Equipo N◦ 02: Especialistas de TI

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación del desastre y la confirmación de la implementada la infraestructura en el CPD DRS a través del líder de continuidad, todos los miembros del grupo deben reunirse en el CPD DRS.
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el CPD DRS Coordinar con el grupo de redes y comunicaciones para la disponibilidad del

Nro.	Responsable	Actividades
		servicio de comunicaciones.
2.2	Grupo	Restaurar los backup, los servidores y las aplicaciones en el CPD DRS.
2.3	Grupo	Verificar la operatividad de las aplicaciones en el CPD DRS e informar su resultado al líder de continuidad.
2.4	Grupo	Una vez recuperados los recursos críticos de TI asignados, elaborar un informe de ocurrencias que incluya el resultado de los procedimientos de recuperación asignados, el cual deberá ser entregado al líder de continuidad de TI.
3		**Operación en Contingencia**
3.1	Grupo	Mantener operativos lo servicios en contingencia en el CPD DRS.
3.2	Grupo	Atender requerimientos de las áreas del MEF

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Administrador de Sistemas
2	Analista en Administración de Sistemas II
Integrantes	
3	Analista en Administración de Sistemas I
4	Asistente en Respaldos de Información
5	Operador de Centro de Cómputo

Equipo N◦ 03: Administradores de Base de Datos

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación del desastre y la confirmación de la implementada la infraestructura en el CPD DRS a través del líder de continuidad, todos los miembros del grupo deben reunirse en el CPD DRS.
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el CPD DRS. Coordinar con el grupo de redes y comunicaciones para la disponibilidad del servicio de comunicaciones.
2.2	Grupo	Restaurar los backup en los servidores de base de datos.
2.3	Grupo	Ejecutar sus tareas correspondientes en los procedimientos de recuperación de los servicios de base de datos.
2.4	Grupo	Comprobar el correcto funcionamiento de las bases de datos.
2.5	Grupo	Informar del restablecimiento de los servicios de base de datos al líder de continuidad.
2.6	Grupo	Una vez recuperados los recursos críticos de TI, elaborar un informe de ocurrencias que incluya el resultado de la ejecución de los procedimientos recuperación asignados, y entregarlo al líder de continuidad.
3		**Operación en Contingencia**
3.1	Grupo	Administrar el funcionamiento de servicios en los servidores de bases de datos.
3.2	Grupo	Brindar el soporte a los servicios de bases de datos recuperados en el CPD DRS.
3.3	Grupo	Brindar el soporte a los servicios de backup y medios de almacenamiento recuperados en CPD DRS.

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Administrador de Base de Datos
2	Operador de Centro de Cómputo

Equipo N◦ 04: Administradores de Redes y Comunicaciones

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación del desastre y la confirmación de la implementada la infraestructura en el CPD DRS a través del líder de continuidad, todos los miembros del grupo deben reunirse en el CPD DRS
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el CPD DRS. Coordinar con el grupo de redes y comunicaciones para la disponibilidad del servicio de comunicaciones.
2.2	Grupo	Restaurar los backup en los equipos de redes y comunicaciones.
2.3	Grupo	Ejecutar el procedimiento de recuperación de las comunicaciones.
2.4	Grupo	Coordinar con los proveedores locales la disponibilidad de los enlaces de comunicación.
2.5	Grupo	Una vez recuperadas las comunicaciones críticas, elaborar un informe de ocurrencias que incluya el resultado del procedimiento de recuperación asignado, y entregarlo al líder de continuidad.
3		**Operación en Contingencia**
3.1	Grupo	Brindar soporte técnico de telecomunicaciones y monitorear los equipos de comunicaciones.
3.2	Grupo	Atender los requerimientos de comunicaciones solicitados por las áreas del MEF

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Coordinador de Redes y Comunicaciones
2	Analista de Comunicaciones y Seguridad

Equipo N◦ 05: Administradores de Seguridad Informática

Nro	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación del desastre y la confirmación de la implementada la infraestructura en el CPD DRS a través del líder de continuidad, todos los miembros del grupo deben reunirse en el CPD DRS.
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el CPD DRS. Coordinar con el grupo de redes y comunicaciones para la disponibilidad del servicio de comunicaciones.
2.2	Grupo	Restaurar los backup en los equipos de seguridad.
2.3	Grupo	Validar los esquemas de seguridad de la información restablecidos en el CPD DRS e informarlo al líder de continuidad.
2.4	Grupo	Brindar soporte para los accesos de emergencia a los usuarios de las áreas del MEF
2.5	Grupo	Informar al líder de continuidad los incidentes de seguridad presentados durante la etapa de recuperación.
2.6	Grupo	Finalizadas las actividades, elaborar un informe de ocurrencias el cual deberá ser entregado al líder de continuidad.
3		**Operación en Contingencia**
3.1	Grupo	Administrar la seguridad del MEF a fin de garantizar el cumplimiento de las políticas de seguridad definidas para operar en modo de contingencia en el CPD DRS.
3.2	Grupo	Definir las políticas y los accesos a la información de acuerdo a la condición de contingencia en que opera el MEF.

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Coordinador de Seguridad Informática
2	Analista en Seguridad Informática
Integrantes	
3	Analista en Seguridad
4	Analista en Seguridad Informática

Equipo N◦ 06 : Soporte Tecnológico

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación a través del líder de continuidad, que los servicios se encuentran disponibles, todos los miembros del grupo deben reunirse en el Centro Alterno de Negocio – CAN.
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el Centro Alterno de Negocio – CAN. Coordinar con el grupo de redes y comunicaciones para la disponibilidad del servicio de comunicaciones.
2.2	Grupo	Configuras las aplicaciones en las PCs de los usuarios del MEF y validar el acceso a las mismas.
3		**Operación en Contingencia**
3.1	Grupo	Brindar servicio de soporte a usuarios y mantenerlos informados del estado del servicio en todo momento.

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Especialista en Redes y Comunicaciones
2	Colaborador de Soporte Tecnológico al MEF
Integrantes	
3	Colaborador de Soporte Tecnológico al MEF
4	Colaborador de Soporte Tecnológico al MEF
5	Colaborador de Soporte Tecnológico al MEF

Equipo N◦ 07: Desarrollo de APP

Nro.	Responsable	Actividades
1		**Respuesta al incidente**
1.1	Grupo	Recibida la notificación a través del líder de continuidad, que los servicios está habilitados en el CPD DRS, todos los miembros del grupo deben reunirse en el de.
2		**Activación**
2.1	Grupo	Comprobar el equipamiento de sus puestos de trabajo en el de. Coordinar con el grupo de redes y comunicaciones para la disponibilidad del servicio de comunicaciones.
2.2	Grupo	Validar la funcionalidad de las aplicaciones en contingencia.
2.3	Grupo	Finalizadas las actividades, elaborar un informe de ocurrencias el cual deberá ser entregado al líder de continuidad.
3		**Operación en Contingencia**
3.1	Grupo	Realizar los cambios a las aplicaciones, según los requerimientos de las áreas usuarias del MEF

CONFORMACIÓN DE GRUPO	
Ít.	**Cargo**
Líder de Continuidad de TI	
1	Director de la Oficina de Sistemas de Información
2	Coordinador de Desarrollo
Integrantes	
3	Desarrollo - Portal MEF
4	Analista de Soporte de Sistemas SIAF
5	Analista de Soporte de Sistemas Informáticos I
6	Analista de Control de Calidad - SIAF
7	Analista de Soporte de Sistemas SIAF
8	Analista de Sistemas PAD III
9	Analista de Soporte de Sistemas SIAF
10	Analista de Soporte de Sistemas SIAF
11	Analista de Soporte de Sistemas Informáticos I
12	Analista de Soporte de Sistemas I
13	Analista de Soporte de Sistemas SIAF
14	Analista de Soporte de Sistemas SIAF
15	Analista de Soporte de Sistemas SIAF
16	Analista de Soporte de Sistemas SIAF
17	Analista de Soporte de Sistemas SIAF
18	Analista de Soporte de Sistemas SIAF

19	Analista de Soporte de Sistemas SIAF
20	Consultor de apoyo al mantenimiento del SIAD
21	Analista de Soporte de Sistemas SIAF
22	Analista de Soporte de Sistemas I

Lista de Proveedores

N°	PROVEEDOR	SERVICIO PRESTADO	CONTACTO	TELEFONOS	EMAIL
1	CANVIA	Servidores RICS, Solución de Virtualización y Solución de Respaldos	Gianella Ojeda Patricia Santayana Joseph Ñique	213-6300 Anexo: 6082 – 6087 999-672-359	helpdesk@canvia.com psantayana@canvia.com jnique@canvia.com
2	SAPIA	Correo Electrónico y Controlador de Dominio	Dhamelys Arteaga Tanú Tavara Betty Grimaldo	T. (0800) 70610 opción 1 +51 916 671 459 +51 958 092 280 +51 993 526 906	cds@sapia.com.pe soporte@sapia.com.pe darteaga@sapia.com.pe ttavara@sapia.com.pe bgrimaldo@sapia.com.pe
3	B.S BUSINESS SOLUTION CONSULTORES S.A.C	Monitorio de Plataforma Tecnológica del MEF	Cristiam Jhoner Pérez Huatuco	+51 994 780 502	jperez@bsconsultores.com.pe
4	IMPERIA	Seguridad Perimetral	Luis Sairitupa	0800 74024 987 743 612	luis.sairitupa@imperia.com.pe
5	BMTECH	Protección Antivirus Certificados Digitales	Luis Bays	2461991 947662630	luis@bmtech.pe
6	ADEXUS	Protección Antispam	Jessica Vallejos	6161314 997588944	jvallejos@adexus.com.pe
7	IBM	Mesa de ayuda de IBM		0-800-50001 0-800-55622	
		Seguimiento a Casos	Andrea Molina	+51 969 336 904	anmolina@pe.ibm.com
8	TELEFÓNICA DEL PERÚ S.A.A.	Internet Principal	Carlos Daniel Solis Sanchez	951 067 482	carlos.solis@telefonica.com
9	CENTURY LINK	Internet Secundario	Guerrero Principe, Elizabeth Daysi	985 855 616	elizabeth.guerrero@lumen.com
10	AMÉRICA MÓVIL	Internet Inalámbrico	Jaaziel Jeremai Coz Nuñez	997 109 217	jaaziel.coz@claro.com.pe
11	EBD PERÚ S.A.C.	Mantenimiento de Switch	Angel Palacin Palacin	989 762 188	apalacin@nolden.pe
12	INET PERÚ SAC	Mantenimiento de Red Inalámbrica	Manuel Pomalazo Flores	987 972 616	manuel.pomalazo@i-net.pe
13	BANCO DE LA NACIÓN	Enlace	Miriam Mansilla	998 613 014	
15	RENIEC	Enlace	Carlos Meza Loyola	972 682 302	cmezal@reniec.gob.pe
16	Banco de la Nación	Redes	Jesus Ibarra		jibarra@bn.com.pe
		Producción	Carlos Barzola	+51 996417610	cbarzola@bn.com.pe
		Infraestructura	Oscar López	+51 998613362	olopez@bn.com.pe
17	BCRP	Envío archivos	Roberto Castro Galarza	613-2215	roberto.castro@bcrp.gob.pe
		Redes	Ana Brito	613-2379	ana.brito@bcrp.gob.pe
18	SBS	Envío Tipo de Cambio	Raúl Vasquez	630-9000	rvasquez@sbs.gob.pe
			Tito Flores	630-9000	gti-operaciones@sbs.gob.pe

19	SUNAT	Redes	Rodolfo Villafuerte David Salinas	+51 936 639 247	rvillafu@sunat.gob.pe dsalinas@sunat.gob.pe
20	GTD	Servicios de Housing	Diego Zavala Bravo	+51 943 245 149	Diego.zavala@grupogtd.com

1.2. SECCIÓN II: DESARROLLO DEL PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

1.2.1. FASE ANTES: Actividades de Preparación

Actividades Preventivas y de Preparación

EQUIPO DE CONTINUIDAD DE TI		
Nro.	**Responsable**	**Actividades**
1		**Prevención**
1.1	Líder de continuidad de TI	Monitorear el cumplimiento de las funciones y responsabilidades asignadas a los grupos de continuidad de TI para la prevención de desastres.
1.2	Grupos de continuidad de TI	Brindar el seguimiento al cumplimiento del Plan de Implementación de actividades preventivas a eventos de desastre que afecten la continuidad de TI.
1.3	Grupos de continuidad de TI	Realizar actualizaciones periódicas del DRP y documentar cualquier cambio que se realice a los activos de la información, teniendo en cuenta la infraestructura tecnológica
1.3	Grupos de continuidad de TI	Coordinar con los Grupos de Continuidad de TI el mantenimiento del DRP y llevar a cabo el respectivo Control de Versiones.
1.4	Grupos de continuidad de TI	Capacitar y preparar al personal responsable de la ejecución del plan.
1.5	Grupos de continuidad de TI	Realizar periódicamente los diferentes tipos de pruebas del DRP con los recursos que se tengan disponibles.
1.6	Grupos de continuidad de TI	Realizar reuniones periódicas para la revisión del Plan del DRP.
1.7	Grupos de continuidad de TI	Realizar los respaldos de la información completa e incremental periódicamente, trasladarlos a un lugar fuera de las instalaciones del Ministerio de Economía y Finanzas y con las prácticas de seguridad adecuadas en el transporte de los mismos.
2		**Preparación**
2.1	Grupos de continuidad de TI	Monitorear el cumplimiento de las funciones y responsabilidades asignadas al grupo para la preparación de desastres.
2.2	Grupos de continuidad de TI	Monitorear la Implementación y Adquisición del CDE ante la posibilidad de un eventual desastre que requiera su utilización

1.2.2. FASE DURANTE: Proceso de puesta en producción del CPD DRS

Objetivo

Asegurar la continuidad de los procedimientos críticos de negocios luego de ocurrido un desastre, mediante la apertura y puesta en producción del CPD DRS.

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.

1.- DETENER REPLICAS	
Tareas	**Responsable**
✓ Recuperación de desastres de la solución de VMWARE - SRM (ver Anexo 4.1) ✓ Detener réplicas de base de datos. • Servidor MEF001 (Base de Datos MEFSF) - (ver Anexo 4.2)	Equipos de Continuidad de TI

1.- DETENER REPLICAS	
Tareas	**Responsable**
• Servidor MEF002 (Base de Datos MEFPP) - (ver Anexo 4.3) • Servidor MEF015 (Base de Datos SIAFII) - (ver Anexo 4.4) • Servidor SERBD01 (Base de Datos MEFWEB) - (ver Anexo 4.5) • Servidor SERBD02 (Base de Datos BDSTD) - (ver Anexo 4.6) • Servidor SERBD03 (Base de Datos AIRHSP) - (ver Anexo 4.7)	

2.- HABILITAR ENLACES	
Tareas	**Responsable**
✓ Desconectar enlaces MEF – DRS y MEF – CAN. (ver Anexo 5) ✓ Habilitar enlaces (CAN – DRS), (DRS – BN) y (DRS – RENIEC). ✓ Realizar pruebas de conectividad.	El equipo de Redes y Comunicaciones

3.- HABILITAR REDES Y COMUNICACIONES	
Tareas	**Responsable**
✓ Habilitar VPN CAN – DRS. (ver Anexo 6) ✓ Cambiar Gateways en el FW DRS ✓ Actualizar reglas del FW DRS ✓ Realizar pruebas de conectividad y publicaciones de servicios	El equipo de Redes y Comunicaciones. El equipo de Seguridad Informática

4.- HABILITAR PLATAFORMA DE SERVIDORES	
Tareas	**Responsable**
✓ Conectarse por VPN a DRS. ✓ Cambiar IP de los servidores de Base de Datos (ver Anexo 7) o Cambiar IPS y DNS o Probar conectividad ✓ Iniciar Base de Datos (MEFSF). (ver Anexo 8.1) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Iniciar Base de Datos (MEFPP). (ver Anexo 8.2) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Iniciar Base de Datos (SIAFII). (ver Anexo 8.3) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Iniciar Base de Datos (MEFWEB). (ver Anexo 8.4) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Iniciar Base de Datos (STD). (ver Anexo 8.5) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Iniciar Base de Datos (AIRHSP). (ver Anexo 8.6) o Iniciar Base de Datos o Iniciar Listener o Pruebas de TSNAME ✓ Habilitar plataforma de servidores virtuales (ver Anexo 4.1) ✓ Habilitar servidores Controlador de Dominio. (ver Anexo 9.1 y 9.2) o Iniciar servicio de controlador de dominio. o Activar roles y servicios.	Equipos de Continuidad de TI

4.- HABILITAR PLATAFORMA DE SERVIDORES	
Tareas	**Responsable**
o Pruebas de autenticación y DN. Servidor de Correo Electrónico (ver Anexo 10.1) o Iniciar servicios Exchange. o Pruebas de envío y recepción de correo. Servidores de aplicaciones web. (ver Anexo 10.2) o Iniciar servidores. o Probar conectividad. o Iniciar instancias de aplicaciones web. o Validar recursos montados por NFS o CIFS. o Validar URL locales. Servidores de aplicaciones C/S (ver Anexo 10.3) o Iniciar servidores. o Probar conectividad. o Validación recursos compartidos. o Validación de permisos de red. o Validar aplicaciones C/S. Servidores de publicaciones. (ver Anexo 10.4) o Iniciar servidores. o Probar conectividad. o Iniciar servicios de IIS y Apache o Validar publicación de inventario de aplicaciones. Servidores SIAF. o Servidores COM (ver Anexo 10.5) o Servidores SERs. (ver Anexo 10.6) Servidores del Portal Web. (ver Anexo 10.7) o Iniciar servidores de BD MySQL. o Iniciar servicio de Apache. o Validar Portal Web ✓ Iniciar aplicaciones en Contingencia (ver Anexo 11) o Realizar pruebas de cargas de URL de las aplicaciones Web o Realizar de pruebas de conectividad de las aplicaciones C/S o Realizar pruebas de los accesos a recursos compartidos.	

5.- HABILITAR EQUIPAMIENTO DE USUARIOS EN EL CAN	
Tareas	**Responsable**
✓ Habilitar los equipos de usuarios ✓ Pruebas de red e Internet ✓ Revisión de aplicaciones web y C/S ✓ Reinstalaciones de aplicaciones.	El equipo de Soporte Tecnológico

6.- INICIAR SERVICIOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
1	Servicio de directorio Activo	✓ Levantar servidor AD. ✓ Revisar los servicios de Active Directory, DNS, NPS, WINS y GPOs ✓ Pruebas de autenticación de dominio.	Equipos de Continuidad de TI

6.- INICIAR SERVICIOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
2	Servicio de correo electrónico institucional	✓ Levantar servidor de Directorio Activo AD. ✓ Levantar nodo 1 de Exchange. ✓ Levantar nodo 2 de Exchange. ✓ Revisar todas las Base de Datos ✓ Revisar el DAG	Equipos de Continuidad de TI
3	Sistema Integrado de Administración Financiera (SIAF) y Servicios de transmisión de datos	✓ Levantar servidor de base de datos MEFSF. ✓ Levantar servidores de componentes: COM1, COM2, COM3, COM4, COM5, COM6. ✓ Levantar los servidores SERS (Sistemas de envío y recepción de SIAF) SERS01, SER02 y SERS03. ✓ Validar el servicio de Internet para las transmisiones de las Unidades Ejecutoras. ✓ Levantar servidor de aplicaciones Cliente Servidor WSAPP-2012. ✓ Validar conexiones con el BN, RENIEC y DRS.	Equipos de Continuidad de TI
4	Módulo de Formulación Presupuestal (SIAF II)	✓ Levantar el servidor de base de datos MEF015 ✓ Levantar los servidores publicadores APPS6 y APPS7 ✓ Levantar los servidores de aplicaciones JBOSS (SIAFII-MFP-AS02-PROD, SIAFII-MFP-AS03-PROD y SIAFII-MFP-AS04-PROD) ✓ Revisar la publicación de la Formulación Presupuestal SIAFII.	Equipos de Continuidad de TI
5	Web Services	✓ Levantar el servidor de base de datos ✓ Levantar los servidores publicadores WS.MINECO.GOB.PE ✓ Levantar los servidores de aplicaciones JBOSS (JBOSS-wsjavap, WS-s3.mef.gob.pe, WildFly10-HCsrv01 y JBOSS-wsjavap) ✓ Revisar la publicación de Web Services.	
6	Sistema de Personal (SISPER)	✓ Levantar servidor de base de datos MEFSF. ✓ Levantar servidor de aplicaciones Cliente Servidor WSAPP-2012.	Equipos de Continuidad de TI
7	Sistema de Gestión Presupuestal (SGP)	✓ Levantar servidores de base de datos, MEFPP ✓ Levantar servidor de aplicaciones Cliente Servidor WSAPP-2012.	Equipos de Continuidad de TI

6.- INICIAR SERVICIOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
8	Sistema de Administración de la Deuda (SIAD)	✓ Levantar servidores de base de datos MEFPP ✓ Levantar servidor de aplicaciones Cliente Servidor WSAPP-2012 ✓ Levantar servidor de aplicaciones Cliente Servidor OFIMEF01.	Equipos de Continuidad de TI
9	Sistema Integrado de Gestión Administrativa (SIGA)	✓ Levantar servidor de base de datos MEFSF. ✓ Levantar servidor de aplicaciones Cliente Servidor WSAPP-2012 ✓ Levantar el servidor de publicaciones APPS3 y APPS4 ✓ Revisar la publicación del servicio SIGAWEB y Gestión Productos.	Equipos de Continuidad de TI
10	Subastas de Fondos Públicos	✓ Levantar servidor de base de datos MEFWEB ✓ Levantar el servidor de publicaciones APPS10 ✓ Revisar la publicación del servicio COLOCACIONESEF	Equipos de Continuidad de TI
11	Seguimiento de la Ejecución Presupuestal (Consulta amigable)	✓ Levantar el servidor de base de datos MEFWEB ✓ Levantar el servidor de aplicaciones APPS5 ✓ Validar el servicio de IIS ✓ Revisar y/o actualizar la fecha de la Consulta Amigable ✓ Revisar la publicación de la Consulta Amigable	Equipos de Continuidad de TI
12	Portal de MEF	✓ Levantar servidor de base de datos MySQL ✓ Levantar el servidor del Portal Web ✓ Validar los servicios de Apache y MySQL ✓ Revisar la publicación del Portal Web ✓ Revisar el módulo de administración del Portal Web.	Equipos de Continuidad de TI
13	STD	✓ Levantar el servidor de base de datos BDSTD ✓ Levantar servidor de aplicaciones WildFly del STD. ✓ Mapear los recursos compartidos del FileServer en el servidor de aplicaciones WildFly del STD ✓ Revisar la publicación del STD.	Equipos de Continuidad de TI
14	Aplicativo Informático para el Registro Centralizado de Planillas y de Datos de los Recursos Humanos del Sector Público – AIRHSP	✓ Levantar servidores de base de datos BDAIRHSP. ✓ Levantar el servidor de aplicaciones Tomcat ✓ Levantar el servidor de publicaciones APPS2 ✓ Revisar la publicación del servicio AIRHSP	Equipos de Continuidad de TI
15	Sistema Nacional de Programación Multianual y	1. Levantar servidor de base de datos MEFSF.	Equipos de Continuidad de TI

6.- INICIAR SERVICIOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
	Gestión de Inversiones INVIERTE.PE	2. Levantar servidor de aplicaciones OFI5C y OFI6C 3. Iniciar el servicio IIS ✓ Revisar la publicación de las APPS INVIERTE.PE	

7.- VALIDAR FUNCIONALIDADES DE APLICACIONES Y BASE DE DATOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
1	Servicio de directorio Activo	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio	Equipos de Continuidad de TI
2	Servicio de correo electrónico institucional	✓ Realizar pruebas envío y recepción de correos interno y externo ✓ Validación del servicio	Equipos de Continuidad de TI
3	Sistema Integrado de Administración Financiera (SIAF) y Servicios de transmisión de datos	✓ Realizar pruebas funcionales del SIAF ✓ Validación del servicio	Equipos de Continuidad de TI
4	Módulo de Formulación Presupuestal (SIAF II)	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio	Equipo de Desarrollo de APP
5	Web Services	✓ Realizar pruebas funcionales del servicio ✓ Validación de conexiones con Entidades.	Equipo de Desarrollo de APP
6	Sistema de Personal (SISPER)	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio.	Equipo de Desarrollo de APP
7	Sistema de Gestión Presupuestal (SGP)	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio.	Equipo de Desarrollo de APP
8	Sistema de Administración de la Deuda (SIAD)	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio.	Equipo de Desarrollo de APP
9	Sistema Integrado de Gestión Administrativa (SIGA)	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio.	Equipo de Desarrollo de APP

7.- VALIDAR FUNCIONALIDADES DE APLICACIONES Y BASE DE DATOS			
Ít.	**Sistema informático**	**Descripción de la tarea**	**Responsable**
10	Subastas de Fondos Públicos	✓ Realizar pruebas funcionales del servicio ✓ Validación del servicio.	Equipo de Desarrollo de APP

1.2.3. FASE DESPUÉS: Procedimiento de Recuperación de Servidores del Centro de Procesamiento de Datos Principal

Objetivo

Asegurar la restauración del CPD principal una vez superado el desastre y dadas las condiciones necesarias para la vuelta a la operatividad en las instalaciones.

Procedimiento de Restauración y Retorno a la Normalidad.

Una vez que se haya restablecido la infraestructura en el CPD Principal y/o CPD Contingencia, el equipo de continuidad realizará la evaluación para el retorno a la normalidad y desarrollará el Plan de Acción de Retorno a la Normalidad, el cual debe ser aprobado por la Dirección de OGTI, debe contemplar lo siguiente:

- ✓ Cronograma de Actividades.
- ✓ Hitos de Control.
- ✓ Recursos tiempo, humanos, financieros y materiales.
- ✓ Riesgos asociados al Plan de Restauración y sus respectivas medidas de mitigación.

Nro.	Componente	Descripción de la Tarea
1	Adquirir equipamiento e implementación del CPD Principal del MEF	Implementación del CPD Principal o Servicio de Housing o Servicio de Hosting. Adquisición de Equipamiento de Seguridad Adquisición de Equipamiento de Redes Adquisición de Equipamiento de Internet y Enlaces de Comunicaciones Adquisición de Equipamiento de Servidores Arquitectura RISC y Almacenamiento Adquisición de Equipamiento de Servidores Arquitectura Virtual y Almacenamiento Adquisición de Equipamiento de Backup, Librería y Cintas
2	Implementación de Enlaces de Red e Internet	La oficina de Redes y Comunicaciones de la OIT definirá las consideraciones a tomar en cuenta para la implementación de los enlaces.
3	Implementación de Servicios de Seguridad	La oficina de Ciberseguridad de la OIT definirá las consideraciones a tomar en cuenta para la implementación de los equipos de seguridad.
4	Adquisición equipamiento de computo	La oficina de Cómputo de la OIT definirá las consideraciones a tomar en cuenta para la implementación de los servidores.
5	Activación de los servidores	El equipo de Especialistas de TI realizará las tareas para implementar las configuraciones iniciales de los sistemas operativos.
6	Recuperar las cintas de respaldo	El Líder de continuidad de TI realizará las coordinaciones para recuperar las cintas de respaldo.
7	Implementación de la herramienta de Backups	El equipo de Especialistas de TI realizará las tareas de configuración de los equipos de Backup para la lectura de las cintas de respaldo.
8	Restauración de Backups de Base de Datos, Servidores e Información.	El equipo de Especialistas de TI realizará la descarga de los archivos de respaldo de las cintas a disco.
9	Activación de los Servidores de Base de Datos	El equipo de Administradores de Base de Datos realizará la restauración de las bases de datos

10	Activación del Servidor Controlador de Dominio	El equipo de Especialistas de TI realizará la habilitación del AD.
11	Activación del Servidor de Correo Electrónico	El equipo de Especialistas de TI realizará la habilitación y restauración del servicio de correo electrónico.
12	Activación de los servidores de publicaciones	El equipo de Especialistas de TI realizará la restauración de los servidores de publicación.
13	Activación de los servidores de Aplicaciones	El equipo de Especialistas de TI realizará la restauración de los servidores de aplicación.
14	Activación y Validación de enlaces externos con otras entidades	El equipo de Desarrollo de APPS realizará la validación de los enlaces externos con otras entidades.
15	Validar los servicios de base de datos y aplicaciones en contingencia	El equipo de Desarrollo de APPS realizará la validación de los servicios de base de datos y aplicaciones en contingencia.

Una vez realizado el Retorno a la Normalidad, elaborar un informe de ocurrencias que incluya el resultado del proceso de retorno.

2. ANALISIS DE RIESGOS Y CONTROLES

La Oficina de Infraestructura Tecnológica (OIT), contando con la asistencia técnica de la Oficina de Gestión de Riesgos Operativos (OGRO), ha identificado los peligros que pueden interrumpir el desarrollo de las actividades críticas de los servicios informáticos del MEF. Asimismo, ha evaluado los niveles de riesgo como resultado de la valoración efectuada a los recursos y servicios informáticos en función de peligros o amenazas, la probabilidad de afectación y el impacto en dichas actividades.

Las actividades críticas de los servicios informáticos se detallan en el cuadro, las cuales están alineadas al Macroproceso **S03 Gestión de Tecnologías de la Información del MEF**, según se presenta a continuación:

Proceso nivel 0	Proceso nivel 1	Proceso nivel 2	Actividad crítica
S03 Gestión de Tecnologías de la información	S03.03 Gestión de la Plataforma Tecnológica	S03.03.02 Diseño, implementación y mantenimiento de la Plataforma Tecnológica	Realizar mantenimiento
		S03.03.03Gestión de incidencias de los servicios de tecnologías de la información	Atender requerimiento o incidencia por especialistas competentes. Los equipos son: Equipamiento central (servidores, BD), conectividad, redes, seguridad digital.

Asimismo, se ha determinado los recursos críticos que dan soporte a las actividades críticas identificadas, los cuales se muestran a continuación:

Actividad crítica	Recurso crítico	Tipo de recurso
Realizar mantenimiento	**Servidores:** - Servidores para plataforma de base de datos - Servidores para plataforma de virtualización - Servidores rackeables **Sistemas de almacenamiento** **Librerías de Respaldos** **Equipos de comunicación - Fibra** **Equipos de comunicación - Ethernet.** **Equipos Firewall**	Infraestructura

	Enlaces de redes y comunicaciones: - MEF - Internet - MEF- DRS - MEF- CAN - MEF - CPD Principal (GTD) - MEF - CPD Contingencia (Lumem) - CPD Principal - CPD Contingencia - CAN-DRS - DRS- Banco de la Nación - DRS - RENIEC	Infraestructura
	Servicios informáticos: - SIAF y Servicio de transmisión de datos - Módulo de Formulación Presupuestal (SIAF II) - Consulta amigable - SISPER - SGP - SIAD - SIGA - Subastas de Fondos Públicos - Portal MEF - STD - AIRHSP - INVIERPE.PE - Correo Electrónico - Controlador de dominio	Sistemas
Atender requerimiento o incidencia por especialistas competentes. Los equipos son: Equipamiento central (servidores, BD), conectividad, redes, seguridad digital.	**Servidores:** - Servidores para plataforma de base de datos - Servidores para plataforma de virtualización - Servidores rackeables **Sistemas de almacenamiento** **Librerías de Respaldos** **Equipos de comunicación - Fibra** **Equipos de comunicación - Ethernet.** **Equipos Firewall**	Infraestructura
	Enlaces de redes y comunicaciones: - MEF - Internet - MEF- DRS - MEF- CAN - MEF - CPD Principal (GTD) - MEF - CPD Contingencia (Lumem) - CPD Principal - CPD Contingencia - CAN-DRS - DRS- Banco de la Nación - DRS - RENIEC	Infraestructura
	Servicios informáticos: - SIAF y Servicio de transmisión de datos - Módulo de Formulación Presupuestal (SIAF II) - Consulta amigable - SISPER - SGP - SIAD - SIGA - Subastas de Fondos Públicos - Portal MEF - STD - AIRHSP - INVIERPE.PE - Correo Electrónico - Controlador de dominio	Sistemas
	Equipo de continuidad de TI (OGTI) - Líder de continuidad - Especialistas de TI - Administradores de base de datos - Administradores de redes y comunicaciones - Administradores de seguridad informática - Soporte tecnológico - Desarrollo de APP	Personas

Dichas actividades y recursos están expuestos a peligros. Los peligros identificadas son: terremoto, inundación y aniego, incendio, delitos informáticos, debilidad estructural, falla en la energía eléctrica, pandemia, ataque terrorista, disturbios sociales, actividad criminal, falla en las telecomunicaciones, caída de internet y lluvias.

Los controles permiten determinar qué tan protegidos se encuentran los recursos críticos frente a la ocurrencia de un peligro. Los controles con los que actualmente cuenta la OIT son los siguientes:

Recurso crítico	Control existente
Servidores: - Servidores para plataforma de base de datos - Servidores para plataforma de virtualización - Servidores rackeables **Sistemas de almacenamiento** **Librerías de Respaldos** **Equipos de comunicación - Fibra** **Equipos de comunicación - Ethernet.** **Equipos Firewall**	• **CPD Contingencia** ✓ Cámaras de vigilancia en el interior del Centro de Datos. ✓ Grupo electrógeno para el centro de datos. ✓ Mantenimiento para equipos de aire acondicionado del Centro de Datos. ✓ Sistema contra incendios en el Centro de Datos • **CPD DRS** ✓ Cámaras de vigilancia en el interior del Centro de Datos. ✓ Grupo electrógeno para el centro de datos. ✓ Mantenimiento para equipos de aire acondicionado del Centro de Datos. ✓ Sistema contra incendios en el Centro de Datos • **Política de Backup v3.0**
Enlaces de redes y comunicaciones: - MEF - Internet - MEF- DRS - MEF- CAN - MEF - CPD Principal (GTD) - MEF - CPD Contingencia (Lumem) - CPD Principal - CPD Contingencia - CAN-DRS - DRS- Banco de la Nación - DRS - RENIEC	• Contrato de niveles de servicio con proveedor de enlace de comunicación entre la sede central y la sede donde se encuentra ubicado el Centro de Datos.
Servicios informáticos: - SIAF y Servicio de transmisión de datos - Módulo de Formulación Presupuestal (SIAF II) - Consulta amigable - SISPER - SGP - SIAD - SIGA - Subastas de Fondos Públicos - Portal MEF - STD - AIRHSP - INVIERPE.PE - Correo Electrónico - Controlador de dominio	• **CPD Contingencia** ✓ Servicio de replicación de base de datos ✓ Servicio de replicación de servidores virtuales ✓ Servicio de replicación de correo electrónico y AD ✓ Servicio de replicación del sistema de respaldo • **CPD DRS** ✓ Servicio de replicación de base de datos ✓ Servicio de replicación de servidores virtuales ✓ Servicio de replicación de correo electrónico y AD • **Política de Backup v3.0**
Equipo de continuidad de TI (OGTI) - Líder de continuidad - Especialistas de TI - Administradores de base de datos - Administradores de redes y comunicaciones - Administradores de seguridad informática - Soporte tecnológico - Desarrollo de APP	• **Personal suplente del equipo de continuidad de TI** • **Manuales de procedimientos de recuperación (anexos del DRP)**

Para determinar el nivel de riesgo, la OGRO en coordinación con la OIT-OGTI utilizó la metodología de evaluación de riesgos descrita en anexo 2 de los “Lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno” aprobado con RM N° 320-2021-PCM del**,** obteniéndose el siguiente resultado:

RECURSO CRÍTICO	Sismo de gran magnitud	Inundación y Aniego	Incendio	Delitos Informáticos	Debilidad Estructural	Falla de Energía Eléctrica	Pandemia o Epidemia	Ataque Terrorista	Disturbios Sociales	Actividad Criminal	Falla en las Teleco.	Caída de Internet/Sistemas	Prensa Amarilla	Lluvias
Servidores: - Servidores para plataforma de base de datos - Servidores para plataforma de virtualización - Servidores rackeables **Sistemas de almacenamiento** **Librerías de Respaldos** **Equipos de comunicación - Fibra** **Equipos de comunicación - Ethernet.** **Equipos Firewall**														
Enlaces de redes y comunicaciones: - MEF - Internet - MEF- DRS - MEF- CAN - MEF - CPD Principal (GTD) - MEF - CPD Contingencia (Lumem) - CPD Principal - CPD Contingencia - CAN-DRS - DRS- Banco de la Nación - DRS - RENIEC														
Servicios informáticos: - SIAF y Servicio de transmisión de datos - Módulo de Formulación Presupuestal (SIAF II) - Consulta amigable - SISPER - SGP - SIAD - SIGA - Subastas de Fondos Públicos - Portal MEF - STD - AIRHSP - INVIERPE.PE - Correo Electrónico - Controlador de dominio														
Equipo de continuidad de TI (OGTI) - Líder de continuidad - Especialistas de TI - Administradores de base de datos - Administradores de redes y comunicaciones - Administradores de seguridad informática - Soporte tecnológico - Desarrollo de APP														

Leyenda: **Color Rojo: Muy Alto** ; **Color Naranja: Alto** ; **Color Amarillo: Medio** ; **Color Verde: Bajo**

La OIT ha establecido nuevos controles para mitigar los niveles de riesgo “Muy Alto” y “Alto”, los cuales se vienen desarrollando y se señalan a continuación:

Recurso crítico	Nuevos controles
Servidores: - Servidores para plataforma de base de datos - Servidores para plataforma de virtualización - Servidores rackeables **Sistemas de almacenamiento** **Librerías de Respaldos** **Equipos de comunicación - Fibra** **Equipos de comunicación - Ethernet.** **Equipos Firewall**	• **Proyectos de seguridad informática** • **Migración del DRS a provincia**

Enlaces de redes y comunicaciones: - MEF - Internet - MEF- DRS - MEF- CAN - MEF - CPD Principal (GTD) - MEF - CPD Contingencia (Lumem) - CPD Principal - CPD Contingencia - CAN-DRS - DRS- Banco de la Nación - DRS - RENIEC	• **Proyectos de seguridad informática** • **Migración del DRS a provincia**
Servicios informáticos: - SIAF y Servicio de transmisión de datos - Módulo de Formulación Presupuestal (SIAF II) - Consulta amigable - SISPER - SGP - SIAD - SIGA - Subastas de Fondos Públicos - Portal MEF - STD - AIRHSP - INVIERPE.PE - Correo Electrónico - Controlador de dominio	• **Proyectos de seguridad informática** • **Migración del DRS a provincia**
Equipo de continuidad de TI (OGTI) - Líder de continuidad - Especialistas de TI - Administradores de base de datos - Administradores de redes y comunicaciones - Administradores de seguridad informática - Soporte tecnológico - Desarrollo de APP	• **Virtualización de escritorio.**

3. PLAN DE PRUEBAS – DRP

3.1. Objetivo

Este documento tiene como objetivo establecer lineamientos, métodos y criterios para llevar a cabo pruebas en forma regular del "Plan de Recuperación de Desastres (DRP) del Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres - CPD DRS", en adelante Plan de Recuperación de Desastres o simplemente DRP, siendo esta la manera más eficaz de asegurar que dicho plan cumple su propósito.

3.2. Lineamientos Generales

3.2.1. Consideraciones básicas

La realización de pruebas de contingencia constituye un método para asegurar que el Plan de Recuperación de Desastres servirá en el escenario real de un evento adverso disruptivo, por lo que es imprescindible que estas pruebas confirmen la capacidad de recuperación de las tecnologías de la información del Ministerio, debiendo desarrollarse de manera periódica, con alcances definidos y recursos destinados para la ejecución de las mismas.

El programa de pruebas de contingencia que se implemente deberá demostrar la habilidad del MEF para recuperar la operatividad de los sistemas, aplicaciones, datos y redes de comunicaciones, a través de ensayos o simulacros basados en planes de pruebas.

Al respecto, se establecen las siguientes consideraciones o políticas generales con relación a las pruebas de contingencia:

a) Las pruebas serán realizadas de manera controlada sin afectar el servicio a los usuarios finales.
b) Todas las pruebas deberán calificarse en función de los resultados obtenidos y del cumplimiento de los objetivos planteados para cada prueba.

c) Los resultados de las pruebas realizadas deberán ser analizados con el fin de implementar correcciones e identificar oportunidades de mejora y, por consiguiente, perfeccionar y actualizar el Plan de Recuperación de Desastres.
d) Los informes de los resultados de las pruebas realizadas deberán ser proporcionados al Director General de la OGTI.
e) Los procedimientos de administración de cambios de la OGTI deben tener implementados los controles necesarios para asegurar y mantener la integridad del entorno de producción del Centro de Procesamiento de Datos (CPD) principal del MEF cuando se lleven a cabo las pruebas de contingencia.
f) Las pruebas se realizarán con una periodicidad anual como mínimo.

3.2.2. Objetivos de las pruebas

Para cada prueba particular que se defina en el programa deberá especificarse el objetivo o conjunto de objetivos que se desea lograr con el ejercicio. La siguiente es una lista no exhaustiva de posibles objetivos:

- ✓ Evaluar la efectividad de los procedimientos de recuperación de los sistemas informáticos en el Centro de Procesamiento de Datos del Sitio de Recuperación de Desastres (CPD DRS).
- ✓ Comprobar el funcionamiento y el rendimiento de los sistemas informáticos utilizando equipamiento alterno de contingencia.
- ✓ Validar los tiempos de recuperación establecidos.
- ✓ Detectar posibles desviaciones o modificaciones en el hardware, software, redes de comunicaciones y otros elementos que afecten la ejecución de los procedimientos del Plan de Recuperación de Desastres.
- ✓ Analizar la efectividad de los procedimientos de notificación y los de coordinación entre los equipos de recuperación.
- ✓ Constatar la disponibilidad de la información y las plataformas tecnológicas en el CPD principal del MEF.
- ✓ Identificar las revisiones y actualizaciones que requiera el Plan de Recuperación de Desastres.
- ✓ Llevar a cabo un entrenamiento periódico de los integrantes de los equipos responsables de las actividades de recuperación.

3.2.3. Alcance de las pruebas

Las pruebas de contingencia informática abarcan la realización de labores mediante las cuales se validan la estrategia y los procedimientos de recuperación definidos y se adiestra de manera sistemática al personal responsable de dichos procedimientos, de acuerdo a un programa de pruebas previamente establecido.

Para el efecto, las pruebas deben planificarse considerando las actividades documentadas en el Plan de Recuperación de Desastres, limitándose a aquellas que permitan lograr propósitos específicos como:

- ✓ Probar y validar las técnicas y procedimientos diseñados en el DRP.
- ✓ Validar los tiempos de recuperación de la tecnología que han sido previstos en el DRP.
- ✓ Probar la infraestructura de contingencia local y de los proveedores de servicios externos relacionados con la operación en contingencia del MEF.
- ✓ Evaluar las responsabilidades, competencias y desempeño del personal responsable de la ejecución de los procedimientos dispuestos en el DRP.

3.2.4. Oportunidad de las pruebas

La realización de las pruebas obedece a varios factores entre los cuales se pueden mencionar:

- ✓ Por la necesidad de ensayos periódicos que el personal responsable de TI haya establecido como mecanismo de aseguramiento de calidad de la función de recuperación.
- ✓ Cuando haya modificaciones de hardware, software de base, aplicativos o de infraestructura de soporte; o cuando existan cambios significativos en el entorno operativo cubierto por el Plan de Recuperación de Desastres.
- ✓ Cuando se prevea el riesgo de inminente ocurrencia de un evento que afecte las operaciones de TI.
- ✓ Por requerimientos de cumplimiento legal y normativo.

3.2.5. Diseño y documentación de las pruebas

Las pruebas deberán diseñarse con una complejidad y alcance progresivos de modo que eventualmente sean probados todos los aspectos del DRP, al igual que sus interacciones y dependencias con otros planes.

La complejidad y alcances progresivos se dan en la medida en que se sumen nuevos componentes a la prueba inmediatamente anterior, siempre y cuando las debilidades previamente detectadas hayan sido subsanadas antes de dar inicio a la nueva prueba.

Los siguientes aspectos deben tomarse en cuenta para la planificación de las pruebas, pues contribuirán a clarificar y organizar adecuadamente la ejecución de las mismas:

a. Alcance de la prueba

- ✓ Infraestructura
- ✓ Aplicaciones
- ✓ Participantes

b. Definición de objetivos de la prueba

- ✓ Objetivos y resultados esperados
- ✓ Límites de tiempo

c. Medición de la prueba

- ✓ Registro de tiempo durante la prueba
- ✓ Documentación de problemas/desviaciones de la prueba

d. Evaluación de la prueba

- ✓ Cumplimiento de objetivos
- ✓ Problemas/Fortalezas/Desviaciones.

La documentación de la prueba debe estar enfocada a registrar los problemas y desviaciones presentadas en su ejecución, entendiendo los problemas como los imprevistos presentados durante el desarrollo de la prueba que afectan el cumplimiento de los objetivos de la misma, y las desviaciones como las actividades no planificadas que tuvieron que ejecutarse para asegurar la culminación de la prueba prevista. En el presente plan se describen cuatro tipos de documentos que ayudan a estos fines: Programa Anual de Pruebas que contiene la relación de pruebas de

un periodo dado, Plan de Trabajo con la planificación de cada prueba programada, Informe de Resultados de cada prueba ejecutada, y Plan de Acción para resolver los riesgos o incidencias que se hayan encontrado durante la prueba.

Luego de realizada la prueba, es necesario revisar y evaluar su desempeño general analizando los resultados obtenidos, el cumplimiento de objetivos, las fallas y las fortalezas encontradas, y proponiendo posibles mejoras en el diseño de la prueba.

3.3. Roles y responsabilidades

3.3.1. Líder de continuidad de TI

El Líder de Continuidad de TI controla y supervisa que los Equipos de Continuidad de TI[9] mantengan actualizado el presente Plan de Pruebas de Contingencia Informática y vigila que se cumplan los lineamientos básicos establecidos sobre las pruebas de contingencia. Es responsable de la creación del programa de pruebas anualizado y de la coordinación de su ejecución con los Líderes de los Equipos de Continuidad de TI.

Sus principales actividades referidas a las pruebas son:

- ✓ Formular el objetivo, alcance y resultados esperados de las pruebas.
- ✓ Elaborar el Programa Anual de Pruebas (ver numeral 3.7) en coordinación con los Líderes de los Equipos de Continuidad de TI.
- ✓ Aprobar los planes de trabajo elaborados por los Líderes de los Equipos de Continuidad de TI.
- ✓ Supervisar y controlar el desarrollo de las pruebas.
- ✓ Analizar los resultados de las pruebas realizadas y coordinar con los Líderes de Equipos de Continuidad de TI las posibles modificaciones al presente Plan.
- ✓ Elaborar los Informes de Resultados (ver numeral 3.5.3) de las pruebas de contingencia realizadas, indicando las observaciones y oportunidades de mejora.
- ✓ Hacer seguimiento a la implementación de mejoras y al levantamiento de observaciones encontradas como resultado de las pruebas, en coordinación con los Líderes de Equipos de Continuidad de TI.
- ✓ Presentar a la Dirección de la OGTI los resultados de las pruebas.

3.3.2. Líder de equipo de continuidad de TI

El Líder de cada Equipo de Continuidad de TI es el responsable de dirigir las actividades de prueba de contingencia informática y la planificación técnica con los integrantes de su correspondiente equipo responsable de la recuperación, vigilando que éstos lleven a cabo las acciones requeridas antes, durante y después de cada prueba de contingencia.

Sus principales actividades referidas a las pruebas son:

- ✓ Formular el cronograma de pruebas a incluirse en el Programa Anual de Pruebas, en coordinación con el Líder de Continuidad de TI.
- ✓ Elaborar con anticipación el Plan de Trabajo (ver numeral 3.5.1) de cada prueba a efectuar, en coordinación con los integrantes del Equipo de Continuidad de TI.

[9] La organización de los Equipos de Continuidad de TI se describe en el Plan de Recuperación de Desastres.

- ✓ Organizar, con los integrantes de su Equipo de Continuidad de TI, la revisión previa de los planes de trabajo y procedimientos de contingencia antes de las pruebas.
- ✓ Concertar con los proveedores de servicios externos relevantes la planificación de la prueba de contingencia en la que intervendrán dichos proveedores.
- ✓ Dirigir la prueba de acuerdo a lo planificado, con el objetivo de cumplir los objetivos trazados de la prueba.
- ✓ Coordinar activamente con el Líder de Continuidad de TI durante la ejecución de la prueba, informando el estado de la misma y los incidentes encontrados y solucionados.
- ✓ Cumplir con los tiempos de recuperación acordados como objetivo de la prueba.
- ✓ Detener la prueba de contingencia ante un incidente que afecte los objetivos establecidos y/o imposibilite la continuación de la misma.
- ✓ Participar activamente y tomar decisiones en las pruebas que involucren la intervención de proveedores de servicios externos relevantes.
- ✓ Brindar toda la información necesaria al Líder de Continuidad de TI para la elaboración del informe de resultados de la prueba de contingencia.
- ✓ Disponer la implementación de las oportunidades de mejora encontradas y las acciones correctivas necesarias para subsanar las incidencias ocurridas durante la ejecución de las pruebas.

3.4. Tipos de prueba

Para lograr el propósito de mejorar la capacidad institucional de preparación, respuesta y recuperación ante eventos disruptivos que afecten a las tecnologías de información, las pruebas de contingencia pueden diseñarse, en general, bien sea como métodos de ensayo para validar el funcionamiento de los sistemas informáticos o de sus componentes en el entorno operativo especificado en el DRP, o como ejercicios que permitan validar los contenidos del DRP o la capacidad de respuesta de los Equipos de Continuidad de TI en situaciones de emergencia simulada.

De este modo, en el presente plan se consideran tres (3) tipos de pruebas:

a) Pruebas de Comunicación-Notificación.
b) Pruebas de Escritorio.
c) Pruebas Operacionales.

Los dos primeros tipos de prueba mencionados se diseñan como ejercicios y se emplean habitualmente para efectos de entrenamiento de los integrantes de los Equipos de Continuidad de TI. Las pruebas operacionales se diseñan como ensayos de las operaciones de recuperación, por lo que involucran el empleo de equipamiento y recursos necesarios de acuerdo al alcance particular con el que se diseñe cada prueba de este tipo.

A continuación, se describen las principales características de cada tipo de prueba considerado en el presente plan.

3.4.1. Pruebas de comunicación – notificación

Este tipo de prueba consiste básicamente en la realización de ejercicios que permitan a los Equipos de Continuidad de TI adiestrarse en las tareas de coordinación establecidas en las primeras etapas del Plan de

Recuperación de Desastres. De este modo, el personal puede conocer y poner en práctica las partes de dicho plan asociadas a las actividades de gestión de la emergencia previstas en las fases iniciales de la respuesta al evento de contingencia (identificación y notificación del evento, evaluación de daños, activación del DRP), excluyendo las tareas de la propia recuperación y operación en contingencia.

La prueba de comunicación - notificación brinda un método seguro y de bajo costo para verificar que la información necesaria para las coordinaciones se encuentre actualizada, detectando potenciales problemas causados por omisiones o cambios en los datos de los diversos puntos de contacto, rotación del personal participante, modificación de roles o variaciones en la estructura jerárquica de reporte, que afectarían a la apropiada ejecución de las acciones relacionadas con la respuesta inmediata a las emergencias.

Las pautas para desarrollar los procedimientos generales de este tipo de ejercicios se describen en el numeral 3.8.1 del presente documento.

3.4.2. Pruebas de escritorio

Esta modalidad de prueba se focaliza en revisar a detalle el Plan de Recuperación de Desastres y toda documentación asociada, evaluando la integridad y efectividad de las actividades y tareas asignadas a los Equipos de Continuidad de TI sin involucrar el uso del actual entorno operativo del CPD. Se brinda así una oportunidad para entrenar a los integrantes de dichos equipos evitando interrumpir las operaciones normales de producción, debido a que el ejercicio se llevará a cabo en las oficinas de la institución en lugar de las instalaciones donde esté alojado el equipamiento central de TI.

El objetivo principal de este tipo de prueba es asegurar, mediante un ejercicio de reflexión y análisis crítico, que en el Plan de Recuperación de Desastres se encuentren definidas todas las funciones, tareas y responsabilidades necesarias para una recuperación exitosa y que esté incluida toda la información de soporte. También puede utilizarse para identificar el hardware, el software de base o las aplicaciones que pudieran haber sufrido cambios recientemente.

La prueba de escritorio, también denominada “prueba en papel”, idealmente debería ejecutarse en corto tiempo –usualmente entre 2 y 4 horas– pues solamente se requiere elegir una situación de posible interrupción de las operaciones (escenario de prueba) a partir de la cual se revisan y analizan los procedimientos de recuperación pertinentes. Esta modalidad de prueba asumirá que el control de daños ya ha sido efectuado y que el desastre ha sido declarado.

Durante la ejecución de una prueba de escritorio, las tareas que los Equipos de Continuidad de TI deben examinar son aquellas que se describen en el Plan de Recuperación de Desastres como secuencias de actividades correspondientes al escenario de prueba que se haya seleccionado.

Las pautas para desarrollar los procedimientos generales de este tipo de ejercicios se describen en el numeral 3.8.2 del presente documento.

3.4.3. Pruebas operacionales

Las pruebas operacionales son ensayos planificados en los que aquellos sistemas y aplicaciones críticas residentes en el CPD principal se habilitan en el CPD DRS, mediante el traslado de los recursos humanos y tecnológicos de contingencia necesarios y ejecutando las estrategias y actividades de recuperación contenidas en el Plan de Recuperación de Desastres.

Esta modalidad de pruebas podrá tener un alcance parcial –por ejemplo, validación de los procedimientos de recuperación de TI, o solo probar la infraestructura de contingencia de servidores, bases de datos o de comunicaciones– o total (al incluir a la totalidad de los componentes del Plan de Recuperación de Desastres). También pueden participar en estas pruebas usuarios representantes de los distintos órganos del MEF que sean relevantes para las pruebas particulares, así como los proveedores de servicios externos relacionados con la operación en contingencia.

Se identifican los siguientes beneficios de este tipo de prueba:

a) Corroborar, con frecuencia predeterminada, que el Plan de Recuperación de Desastres ha sido debidamente documentado y que permitirá una adecuada recuperación de las plataformas tecnológicas críticas.
b) Mejorar las habilidades de los Equipos de Continuidad de TI responsables del restablecimiento de las operaciones de TI.
c) Apoyar al mantenimiento de procedimientos documentados para recuperar la operación de los sistemas informáticos considerados en la contingencia.
d) Brindar mayor confianza a los usuarios finales.

En el presente plan se han previsto dos subtipos de prueba operacional:

1. Prueba interna de sistemas

   Se realiza cuando se considera oportuno verificar individualmente la funcionalidad de alguno de los servicios instalados en el CPD DRS, pudiendo presentarse los siguientes casos:

   - ✓ Promoción de algún nuevo servicio y/o aplicativo.
   - ✓ Promoción de una nueva versión o liberación (release) de un aplicativo.
   - ✓ Cambio o reparación de algún dispositivo de hardware o software base.

2. Prueba integral del DRP

   Se realiza con las siguientes finalidades:

   - ✓ Revisar los procedimientos definidos en el Plan de Recuperación de Desastres, simulando una situación de desastre.
   - ✓ Verificar y validar los servicios del CPS DRS contando con la participación de las áreas usuarias.

   Este tipo de prueba se distingue por las siguientes características:

   - ✓ Frecuencia de realización: se deberá efectuar por lo menos una prueba del DRP dos veces al año.
   - ✓ Responsable de su ejecución: este tipo de prueba es planificada por la Oficina General de Integridad Institucional y Riesgos Operativos y coordinada con todos los órganos del MEF.

3.5. Fases de las pruebas

En la realización de las pruebas del Plan de Recuperación de Desastres se distinguen las siguientes fases:

- ✓ Preparación (Pre-Prueba)
- ✓ Ejecución (Prueba)
- ✓ Revisión (Post-Prueba)

Cada una de estas fases constituyentes de las pruebas de contingencia se desarrollará seguidamente.

3.5.1. Preparación de la prueba

Con anticipación a cada prueba programada, el Líder de Continuidad de TI mantendrá reuniones de planificación con los Líderes de Equipos de Continuidad de TI donde se deliberarán y acordarán los siguientes aspectos que se consideren relevantes sobre la configuración de las pruebas:

a) Tipología de la prueba de contingencia a ejecutar.
b) Objetivos de la prueba y sus respectivos resultados esperados.
c) Escenario de prueba:
   - ✓ Descripción del evento a simular.
   - ✓ Supuestos y condiciones previas.
   - ✓ Situación final esperada.
d) Recursos necesarios:
   - ✓ Sistemas / datos / aplicaciones a recuperarse.
   - ✓ Equipamiento de TI e instalaciones físicas.
   - ✓ Servicios externos.
   - ✓ Procedimientos de contingencia a ensayar o evaluar.
e) Desarrollo de la prueba:
   - ✓ Fechas estimadas para la preparación de los recursos.
   - ✓ Fechas estimadas de inicio y finalización de la prueba.
   - ✓ Secuencia de actividades a realizar durante la prueba.
   - ✓ Tiempos estimados de inicio, fin y duración de cada actividad.
f) Identificación de participantes y datos de contacto
   - ✓ Equipos de Continuidad de TI.
   - ✓ Usuarios finales participantes.
   - ✓ Proveedores de servicios externos.

Esta información puede utilizarse para elaborar el Plan de Trabajo de cada prueba de contingencia informática que se haya programado, sugiriéndose la siguiente estructura de documento cuyos contenidos pueden desarrollarse a partir de los aspectos enunciados en los párrafos precedentes, según se indica a continuación:

Contenido del Plan de Trabajo	Aspectos a incluir
Objetivo(s) de la prueba de contingencia	a, b
Alcance de la prueba	c, d
Descripción de la prueba	e
Participantes de la prueba	f

3.5.2. Ejecución de la prueba

La ejecución se realizará en la fecha y hora programada a cargo de los equipos de recuperación previamente coordinados y con los recursos necesarios para llevar a cabo la prueba.
Estos recursos indispensables son: el Plan de Recuperación de Desastres, recursos informáticos (servidores, equipos de comunicaciones, software, base de datos, etc.), las copias de seguridad necesarias, la coordinación con los proveedores críticos de TI, los ambientes de recuperación desde donde los especialistas ejecutarán las pruebas, y los procedimientos técnicos de recuperación que constituyen la principal herramienta para la recuperación de los servicios de TI.

El Líder de Continuidad de TI se encargará de supervisar y controlar la prueba, coordinando en todo momento las actividades de recuperación según lo planificado con los Líderes de los Equipos de Continuidad de TI. También se encargará de medir el tiempo de ejecución con la finalidad de cumplir con los tiempos de recuperación establecidos para restablecer las operaciones.

3.5.3. Revisión de resultados

La revisión de la prueba se realizará luego de la ejecución de la misma y, para el efecto, el Líder de Continuidad de TI se encargará de elaborar y emitir un Informe de Resultados de la prueba realizada, reporte que debe contener el siguiente contenido mínimo:

a) Descripción de la prueba:
   Se describe el escenario de prueba desarrollado, indicando en resumen las actividades y objetivos de la prueba.
b) Alcance de la prueba:
   Se indica el ámbito de la prueba efectuada, indicando premisas, excepciones y límites de la misma.
c) Equipos de ejecución:
   Se incluye una relación de los equipos organizados que participaron en el desarrollo de la prueba.
d) Resultados de la prueba:
   Se detallan los resultados obtenidos luego de la ejecución de la prueba.
e) Comparación del resultado obtenido versus el planificado:
   Considerando los resultados de la prueba, se comparan los objetivos propuestos antes de la prueba y lo obtenido luego de su ejecución.
f) Incidentes de las pruebas:
   Se indican y detallan todos los eventos o inconvenientes que surgieron durante la ejecución de la prueba, y la manera en que esto afectó al resultado esperado.
g) Observaciones de la prueba:
   Incluye los comentarios u observaciones emitidos por observadores o auditores presentes en la prueba, y que contribuyen a la mejora de los resultados de la prueba.
h) Evaluación de resultados:
   Se efectúa un análisis y evaluación del cumplimiento de los objetivos de la prueba.

i) Anexos y evidencias.
Corresponde a todas las acciones registradas con el fin de documentar el resultado y que servirá para las mejoras o correcciones posteriores.

j) Oportunidades y acciones de mejora:
Se describen situaciones detectadas que van a permitir mejorar el Plan de Recuperación de Desastres.

3.6. Incidencias y acciones correctivas

Durante la ejecución de las pruebas de contingencia podrían presentarse incidencias de cuya revisión y análisis posteriores se estime recomendar y aplicar acciones correctivas, con el objetivo de solucionar los inconvenientes identificados y mejorar el Plan de Recuperación de Desastres, el Plan de Pruebas de Contingencia, o los procedimientos técnicos operativos que sean relevantes.

La siguiente es una lista de posibles incidencias que requerirán acciones correctivas en la infraestructura, aplicaciones y procedimientos de recuperación del Plan de Recuperación de Desastres:

- ✓ Las operaciones y sistemas informáticos no pueden restaurase adecuadamente por insuficiente detalle en los procedimientos técnicos de recuperación.
- ✓ Ocurren errores en la recuperación de las operaciones en el CPD DRS u otras dependencias de la institución por configuraciones deficientes o insuficiente capacidad de los recursos en el CPD DRS o en los servicios externos proporcionados por proveedores.
- ✓ Los datos de respaldo presentan deficiencias en su integridad que no permiten recuperar las operaciones.
- ✓ Proveedores de TI que no tienen conocimiento de las actividades a ejecutar, por lo que su participación no brinda beneficios en el desarrollo de la prueba.
- ✓ Personal responsable de la prueba sin conocimiento adecuado o con capacidades limitadas para ejecutar las actividades de la prueba.
- ✓ Incumplimiento de los objetivos y los parámetros de tiempo de recuperación a causa de retrasos en el inicio, ejecución o término de la prueba.

Para cada incidencia que se haya reportado en el Informe de Resultados se debe formular un Plan de acción para implementar las acciones correctivas recomendadas. En dicho documento se especificarán las tareas a realizar, los responsables de su ejecución, las fechas estimadas de inicio y fin, los resultados esperados, fecha de revisión y el estado de situación de avance.

Los planes de acción elaborados deben ser revisados periódicamente por los Líderes de Equipo de Continuidad de TI para asegurar su cumplimiento, corregir las posibles desviaciones y evaluar su eficacia.

3.7. Programa anual de pruebas

Las pruebas deben realizarse en forma periódica a fin de difundir y conocer las actividades a realizar en el Plan de Recuperación de Desastres, así como para mantener y perfeccionar los procedimientos que la constituyen. Se debe realizar como mínimo una (01) prueba semestral.

Las pruebas a llevarse a cabo se establecerán en un programa de pruebas de periodicidad Anual, el que se registrará con la información similar a la mostrada en el siguiente formato:

Programa Anual de Pruebas de Contingencia					
Año:			Aprobado por:		
Ítem	Alcance (1)	Tipo de Prueba (2)	Objetivo(s) (3)	Responsable(s) (4)	Fecha de Prueba

1. Indicar el sistema, servicio o plataforma a probar, de acuerdo a los inventarios del PRD y a las consideraciones dadas.
2. Indicar el tipo de prueba a emplear.
3. De acuerdo a las consideraciones dadas.
4. Indicar el nombre del Líder de Equipo de Continuidad de TI designado.

Las características de las pruebas propuestas (alcance, tipo de prueba, objetivos de cada prueba, fecha de realización) serán formuladas en forma coordinada por los Líderes de los Equipos de Continuidad de TI y el personal integrante de dichos equipos, a fin de garantizar la factibilidad técnica del programa de pruebas.

Para la determinación del calendario de pruebas se deben tomar en cuenta los factores que pueden condicionar la necesidad y oportunidad de llevarlas a cabo, de acuerdo a lo señalado en el numeral 3.2.4 del presente documento.

3.8. Pautas de entrenamiento para las pruebas

Para asegurar el logro de los objetivos de las pruebas de contingencia que se programen, los participantes deben conocer la mecánica de actuación propia de cada tipo de prueba, según se han definido en la descripción de los tipos de prueba.

Puesto que las acciones a efectuar en las pruebas operacionales dependen de las plataformas de soporte de los sistemas informáticos considerados para fines de contingencia, el entrenamiento en este tipo de pruebas se da lugar cuando se ejercitan, de forma controlada, las estrategias y tareas de recuperación descritas en el Plan de Recuperación de Desastres.

Para los casos de pruebas de comunicación / notificación y pruebas de escritorio, a continuación, se describen los procedimientos generales de ejecución que deberán llevarse a cabo con participación del Líder de Continuidad de TI y los diferentes Equipos de Continuidad de TI.

3.8.1. Entrenamiento de prueba de comunicación-notificación

a) El Líder de Continuidad de TI convocará a los Líderes de los Equipos de Continuidad de TI para coordinar la prueba de comunicación-notificación. El Líder de Continuidad de TI brindará los detalles de las pruebas explicando el objetivo de la prueba, la fecha de ejecución, la duración de la prueba, la lista de las personas que serán notificadas, el mensaje de la comunicación y los resultados esperados. Estas pruebas se ejecutarán, de preferencia, en días de semana fuera del horario de oficina.

b) El día de la ejecución el Líder de Continuidad de TI se encargará de iniciar las comunicaciones telefónicas –o por otros medios previstos– según las actividades de “Respuesta al incidente” y “Activación” definidas en el Plan de Recuperación de Desastres para cada Equipo de Continuidad de TI. Luego, realizará un seguimiento de la prueba y registrará el tiempo de ejecución de la misma.
c) Al culminar la prueba, el Líder de Continuidad de TI se encargará de elaborar el informe de resultados de la prueba de comunicación-notificación, en el cual se deberán mostrar tiempos de ejecución registrados y la relación de notificaciones realizadas con su estado (confirmada / no confirmada).
d) El Líder de Continuidad de TI presentará los resultados de la prueba realizada los Líderes de los Equipos de Continuidad de TI, con quienes efectuará un análisis y evaluación del desempeño encontrado, formulando las acciones correctivas o de mejora que se estimen necesarias.
e) Los Líderes de los Equipos de Continuidad de TI se encargarán de actualizar los datos relacionados a los integrantes de sus respectivos Equipos de Continuidad de TI. De ser necesario, se actualizará la información relevante consignada en el Plan de Recuperación de Desastres.

3.8.2. Entrenamiento de prueba de escritorio

a) El Líder de Continuidad de TI convocará a los Equipos de Continuidad de TI para ejecutar la prueba de escritorio, la que se dará lugar en ambientes que puedan albergar a todos los participantes. Estos equipos deberán disponer de sus respectivos procedimientos de recuperación para la prueba, así como cualquier otra documentación de apoyo al Plan de Recuperación de Desastres.
b) Primera Revisión: Agrupados en mesas de trabajo, revisarán el detalle de los procedimientos de recuperación con el objetivo de verificar el contenido y las actividades que estas contengan. Asimismo, identificarán los riesgos que podrían impactar en el resultado de la prueba como producto de la ejecución de alguna actividad. Los riesgos identificados se evaluarán y se propondrán las respectivas medidas mitigantes.
c) Segunda Revisión: Luego de la revisión de los procedimientos de recuperación en detalle, se procederá a la revisión de la estrategia de recuperación con todas las personas que asistieron a esta prueba. Los participantes verificarán las actividades predecesoras e identificarán si se pueden realizar algunas modificaciones en las secuencias de actividades, a fin de obtener mejores resultados en cumplimiento de los objetivos de la prueba y en reducción de tiempo.
d) Culminada la reunión, se procederá a documentar en el informe de resultados de la prueba todas las observaciones encontradas en el Plan de Recuperación de Desastres, así como las modificaciones propuestas, los riesgos identificados y las medidas de mitigación. Luego se encargará al Líder de cada Equipo de Continuidad de TI la actualización que se estime necesaria en sus procedimientos de recuperación.

4. ANEXOS

Se precisa que los anexos de esta sección del documento, serán administrado en un repositorio de datos compartidos de actualización constante administrado por la OGTI cuya ruta es: \\ws2012-fs.mef.gob.pe\PCO\DRP\ANEXOS

- ✓ Anexo 1 - Control de Cambios DRP
- ✓ Anexo 2 - Política de Backups
- ✓ Anexo 3.1 - Inventario de Aplicaciones
- ✓ Anexo 3.2 - RTO Y RPO de los servicios críticos y no críticos.
- ✓ Anexo 3.3 – Inventario de servidores.
- ✓ Anexo 4.1 - Recuperación de desastres de la solución VMWARE SRM
- ✓ Anexo 4.2 - Detener Réplicas de BD - MEF001
- ✓ Anexo 4.3 - Detener Réplicas de BD - MEF002
- ✓ Anexo 4.4 - Detener Réplicas de BD - MEF015
- ✓ Anexo 4.5 - Detener Réplicas de BD - MEFWEB
- ✓ Anexo 4.6 - Detener Réplicas de BD - BDSTD
- ✓ Anexo 4.7 - Detener Réplicas de BD - AIRHSP
- ✓ Anexo 5 - Habilitar Enlaces CAN – CPD DRS
- ✓ Anexo 6 - Habilitar Firewall y red VPN
- ✓ Anexo 7 - Cambiar IP en Servidores de Base de Datos
- ✓ Anexo 8.1 - Iniciar Base de Datos MEFSF
- ✓ Anexo 8.2 - Iniciar Base de Datos MEFPP
- ✓ Anexo 8.3 - Iniciar Base de Datos SIAFII
- ✓ Anexo 8.4 - Iniciar Base de Datos MEFWEB
- ✓ Anexo 8.5 - Iniciar Base de Datos BDSTD
- ✓ Anexo 8.6 - Iniciar Base de Datos BDAIRHSP
- ✓ Anexo 9.1 - Controlador de Dominio
- ✓ Anexo 9.2 – NPS DHCP
- ✓ Anexo 10.1 - Correo Electrónico Exchange
- ✓ Anexo 10.2 - Iniciar Servicios en los Servidores de Aplicaciones WEB
- ✓ Anexo 10.3 - Iniciar Servidores de Aplicaciones C.S.
- ✓ Anexo 10.4 - Iniciar Servidores de Publicaciones
- ✓ Anexo 10.5 - Iniciar Servidores del Sistema Componente COM
- ✓ Anexo 10.6 - Iniciar Servidores del sistema SERS.
- ✓ Anexo 10.7 - Iniciar Servidores del Portal MEF
- ✓ Anexo 11 - Iniciar Aplicaciones en Contingencia.
- ✓ Anexo 12 - Equipo de Continuidad de TI
- ✓ Anexo 13 - Ficha de Análisis de Riesgos y Controles en PCO- OGTI

1.1 Plan de acción para el cierre de brechas de TI[10]

[10] Informe de Análisis de Brechas OIT-OGTI; mayo 2023

Las actividades que permitirán cerrar las brechas identificadas son:

Nro.	Actividades para el cierre de brechas	Importancia	Responsable
1	Identificar las brechas	Alta	OGIIRO y OGTI
2	Identificar los recursos de Hardware y Software requeridos.	Alta	OGTI
3	Instalar almacenamiento adquirido con Orden de Compra N° 005-2022-BID 5301	Alta	OGTI
4	Realizar los TDR para adquirir los recursos de Hardware y Software y equipamiento informático.	Alta	OGTI
5	Realizar los procesos de selección	Alta	OGA-OGTI
6	Implementar y configurar los recursos de Hardware y Software.	Alta	OGTI
7	Asignar equipos informáticos al personal crítico	Media	OGA- OGTI
8	Replicar la información de los nuevos aplicativos y recursos compartidos al CPD DRS.	Alta	OGTI
9	Realizar pruebas operativas de los servicios replicados.	Media	OGTI
10	Actualizar la documentación correspondiente al Plan de Recuperación de Desastres (DRP)	Media	OGTI

Todas las actividades requieren ser ejecutadas, pues contribuyen, en mayor o menor escala, en poder cerrar las brechas identificadas. A continuación, se muestra los costos proyectados que involucra la implementación del cierre de brechas tecnológicas de nuevas aplicaciones y recursos compartidos identificados:

Nro.	Hardware y Software	Costo total (S/.)
1	Adquirir e instalar 03 servidores físicos	S/ 370,000.00
2	Licencias para replicación.	S/ 130,000.00
3	Licencia de sistema operativo	S/ 150,000.00
4	Adquirir equipos informáticos (laptops)	S/ 594,000.00
	Total	**S/ 1,244,000.00**

La adquisición de los 03 servidores físicos y licencia de sistema operativo permitirá incrementar los recursos de procesamiento (CPU) y memoria (RAM) para soportar la ejecución de los servidores virtuales en un escenario de Desastres. Asimismo, la adquisición de licenciamiento de replicación da derecho a replicar los 26 servidores virtuales.

Por otro lado, la adquisición de equipos informáticos (laptops) permitirá que todo el personal crítico cuente con equipamiento informático que les permita poder operar ante un escenario de desastres.
Por último, mediante Orden de Compra N° 005-2022-BID 5301, la Unidad Coordinación de Proyecto SIAF adquirió 06 discos de almacenamiento para el Sistema de almacenamiento del CPD-DRS, lo que permitirá incrementar el recurso de almacenamiento y soportar el almacenamiento de los 26 servidores virtuales a replicar.

A continuación, se presenta el cronograma de cierre de brechas:

Nro	Actividades para el cierre de brechas	2023						
		may	jun	ago	set	oct	nov	dic
1	Identificar las brechas							
2	Identificar los recursos de Hardware y Software y equipos informáticos requeridos							
3	Instalar almacenamiento y replicar servidores							
4	Realizar los TDR para adquirir los recursos de Hardware y Software y equipos informáticos							
5	Realizar los procesos de selección							
6	Implementar y configurar los recursos de Hardware y Software							
7	Asignar equipos informáticos al personal crítico							
8	Replicar la información de los nuevos aplicativos y recursos compartidos al CPD DRS							
9	Realizar pruebas							
10	Actualizar la documentación DRP							

ANEXO 2: Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades críticas.

1. Los medios de comunicación a emplear, según orden de prioridad, son:

    a. Mensaje al Chat de WhatsApp o Telegram del Grupo de Comando
    b. Mensaje de texto por celular
    c. Redes sociales y correos
    d. Llamada al teléfono fijo y celular
    e. Cualquier otro medio que permita la comunicación

2. Ejecución de la convocatoria y actividades a desarrollar

    a. El Jefe(a) de la OGRO toma la decisión de convocar a los miembros del Grupo de Comando e informa a la Secretaría General la situación de la condición de funcionamiento del MEF, recomendando la necesidad de activar el PCO.

    b. En caso de activar el PCO, el jefe (a) de la OGRO coordina, en sesión de Grupo de Comando, con el representante de la OGA la movilización del personal titular que realizará trabajo presencial en la Sede Alterna.

    c. Los representantes de cada órgano o unidad orgánica, que forman parte del Grupo de Comando, solicitarán al personal Titular que realiza Teletrabajo total informar sobre la disponibilidad de su equipo informático y de los aplicativos, a fin de dicho representante informe en la sesión de Grupo de Comando.

    d. En el caso en que el personal titular que realiza teletrabajo total no tenga la disponibilidad de su equipo o de un aplicativo informático, inmediatamente comunica al representante de su órgano o unidad orgánica para que este informe en sesión de Grupo de Comando.

e. El personal titular que realiza teletrabajo total informará al representante de su órgano o unidad orgánica toda situación respecto al desarrollo de las actividades críticas, fotografiando evidencias y que estas serán comunicadas en la sesión de Grupo de Comando

f. La comunicación se confirma retornando la llamada o mensaje a quien lo hizo, hasta llegar nuevamente al primer emisor o quien inició la llamada.

3. Directorio de teléfonos y correos de instancias responsable de atender como **primera respuesta** ante algún evento disruptivo.

3.1 Respuesta inicial ante eventos disruptivos en el MEF:

- **Para eventos relacionados a servicios de TI**
  - ✓ Teléfono: 311-5930 anexo 67777
  - ✓ Correo: soporte@mef.gob.pe
  - ✓ Responsable Principal: Napoleón Alva
    Teléfono : 311-5930 anexo 3622
    Celular : 958 789 132
    Correo : nalva@mef.gob.pe
  - ✓ Responsable Alterno 1: Cesar muñoz
    Teléfono : 311-5930 anexo 67777
    Celular : 975 696 197
    Correo : jromucho@mef.gob.pe
  - ✓ Responsable Alterno 2 : José Romucho
    Teléfono : 311-5930 anexo 4118
    Celular : 975 695 085
    Correo : jromucho@mef.gob.pe
  - ✓ Responsable Alterno 3: Vicente Tapia
    Teléfono : 311-5930 anexo 3601
    Celular : 993 878 816
    Correo : vtapia@mef.gob.pe

- **Para eventos relacionados a los servicios básicos**
  - ✓ Teléfono: 311-5930 anexo 2979 ó 428-2065
  - ✓ Correo: serviciosauxiliares@mef.gob.pe
  - ✓ Responsable Principal: Mario Jiménez
    Teléfono : 311-5930 anexo 2640
    Celular : 988 070 141
    Correo : mjimenez@mef.gob.pe
  - ✓ Responsable Alterno: David Huachaca
    Teléfono : 311-5930 anexo 2604
    Celular : 991 597 183
    Correo : dhuachaca@mef.gob.pe

- **Seguridad y Salud de los Trabajadores**
  - ✓ Responsable Principal: James Francisco Hiroyasu Tanaka Yzena
    Celular : 940 381 640
    Correo : jtanaka@mef.gob.pe
  - ✓ Responsable Alterno: Rosa Augusta Tenorio Ortiz
    Celular : 958 796 970

Correo : rtenorio@mef.gob.pe

- **Para eventos relacionados a Seguridad en la Sede Central**
  - ✓ Teléfono: 311-5930 anexo 2051
  - ✓ Correo: seguridad@mef.gob.pe
  - ✓ Responsable Principal: Tomás Rentera
    Teléfono : 311-5930 anexo 2052
    Celular : 976 361 264
    Correo : trentera@mef.gob.pe
  - ✓ Responsable Alterno: Alexander Fanola
    Teléfono : 311-5930 anexo 2051
    Celular : 947 422 070
    Correo : seguridad@mef.gob.pe

- **Grupo de Comando para la Continuidad Operativa**
  - ✓ Responsable Principal: Marcos Santillán Ramírez
    Celular : 991349867
    Correo : msantillan@mef.gob.pe
  - ✓ Responsable Alterno: Miguel Ruiz Gutarra
    Celular : 997373845
    Correo : mruizg@mef.gob.pe

3.2 ~~Para~~ coordinaciones con el Banco de la Nación (Acceso a la Sede Alterna):

Control de Acceso

- El personal del MEF autorizado para solicitar el acceso al Centro de Operaciones Alterno (COA) del BN es:

  - ➢ *Jefe (a) de la Oficina de Gestión de Riesgos Operativos del MEF*
  - ➢ *Director (a) de la Oficina General de Integridad Institucional y Riesgos Operativos*

- Para un adecuado control de acceso al COA del BN, en el marco del desarrollo de los ejercicios y pruebas del PCO del MEF, el MEF remitirá, con una ***antelación de 72 horas***, la relación de personal (nombre, DNI) y otros datos a solicitud del BN

Actividades de riesgos

- En el caso de las actividades de riesgos que sean realizados por el personal del MEF o terceros a nombre del MEF, dicho personal debe contar con su respectiva póliza de seguros contra riesgos laborales.
- Para dichas actividades se debe contar siempre con un supervisor del MEF.
- Toda actividad que realice el MEF en las instalaciones del COA BN es de entera responsabilidad del MEF.

Aspectos técnicos BN-MEF

- Si producto de las actividades del MEF, se requiera contar con la participación de personal especializado del BN (telecomunicaciones, instalaciones eléctricas, cableado UTP, etc.) en el COA, estos ***deberán ser solicitados con un plazo de 5 días útiles al BN***, a fin de coordinar con la

Gerencia responsable del BN para su acompañamiento (sea para instalación como desinstalación).

- No está permitido que ningún equipo servidor u otro se mantenga prendido fuera de las actividades de mantenimiento u prueba, debido que las instalaciones no están construidas para albergar este tipo de equipos.

Actividades de Mantenimiento

- Para actividades de mantenimiento de PC, actualizaciones de software, etc. ***deben ser comunicadas con 48 horas de anticipación y su visita será de lunes a viernes. en el horario de 8:30 am a 5:30 pm.***

Respecto a los activos del MEF:

- Se debe contar con la relación de bienes de activo fijo ingresado a las instalaciones del COA.
- Todo ingreso de activos será mediante el Formulario "Registro de Ingreso de Equipos o Materiales en el cual se consigne el nombre del propietario, detalle de los equipos y/o materiales ingresados.
- ***Todo retiro e ingreso de activo fijo debe ser comunicado el BN de forma previa y el MEF debe indicar la única área/persona que podrá solicitar dicha acción al BN, esta acción debe ser comunicada con 48 horas de anticipación***.
- Remitir anualmente los activos que se encuentran en el COA (de ser el caso indicar por piso).
- La verificación de los mismos se realizará entre el personal del MEF y BN (Riesgos-Seguridad).

Registro de equipos o materiales:

- Para cualquier otro aspecto no detallado, se definirá entre el BN y el MEF.

REGISTRO DEINGRESO DE EQUIPO O MATERIALES

Propietario:		ingreso verificador por			firma
Motivo de ingreso:		fecha:	hora:		puerta
ITEM	CANTIDAD	DESCRIPCIÓN	SALIDA		
			fecha	cantidad	supervisor que autoriza

Observaciones:

Salida parcialverificada por				Salida total verificada por			
Nombre:		Fecha:		Nombre:		Fecha:	
Firma:		Hora:		Firma:		Hora:	

Contacto para coordinación:

- ✓ Responsable Principal: Gerencia de Riesgos
  Teléfono : 01- 519 2000
  Anexo : 94500
- ✓ Responsables: Eduardo Diaz

Teléfono : 01- 519 2000
Anexo : 94541
Celular : 981 923 272
Correo : ediaz@bn.gob.pe

- ✓ Responsables: Rodolfo Silva
  Teléfono : 01- 519 2000
  Anexo : 95397
  Celular : 977 280 721
  Correo : rsilva@bn.gob.pe
- ✓ Responsables: Raul Llanos
  Celular : 997 905 043
  Correo : rllanos@bn.gob.pe
- ✓ Responsables: Julio Revolledo
  Correo : jrevolledo@bn.edu.pe
- ✓ Responsables: Julio Lazo
  Correo : jlazo@bn.com.pe

Otros aspectos:

- Para cualquier otro aspecto no detallado se definirá entre el BN y MEF

ANEXO 3: Directorio del Grupo de Comando

N°	Órgano o unidad orgánica	Representantes	Teléfono	Correo electrónico
1	Oficina de Gestión de Riesgos Operativos	Marcos Santillán Ramírez	991 349 867	msantillan@mef.gob.pe
2	Dirección General del Tesoro Público	Alberto Hinostroza Panca	976 061 747	ahinostroza@mef.gob.pe
3	Dirección General de Presupuesto Público	Edinson David Vega Zavala	993 040 194	evegaz@mef.gob.pe
4	Dirección General de Contabilidad Pública	Cecilia Herrera Tejada	995 929 725	herrerac@mef.gob.pe
		Juan Pablo Diaz Soria	972 732 584	jdiazs@mef.gob.pe
5	Dirección General de Abastecimiento	Lourdes Marcelina Jiménez Morales	975 695 143	ljimenez@mef.gob.pe
6	Dirección General de Gestión Fiscal de los Recursos Humanos	Wilson Ávila Romero	940 169 547	wavila@mef.gob.pe
7	Dirección General de Política Macroeconómica y Descentralización Fiscal	Rosa Edelmira Torres Huayané	998 927 573	rtorres@mef.gob.pe
8	Dirección General de Política de Ingresos Públicos	Eliana Zavala Urbiola	980 484 319	ezavala@mef.gob.pe
9	Dirección General de Programación Multianual de Inversiones	Samuel Ruidias Romero	998 190 782	sruidias@mef.gob.pe
10	Dirección General de Mercados Financiero y Previsional Privado	Omar Coronado	987 006 803	ocoronado@mef.gob.pe
		Pablo Oviedo Velásquez	998 278 313	poviedo@mef.gob.pe
11	Dirección General de Asuntos de Economía Internacional, Competencia y Productividad.	Franklin Thompson Loyola Rafael vera Tudela (Titular DAEI)	989 834 990	fthompson@mef.gob.pe
		Israel Infantas Barbachan (Alterno DAEI)		iinfantas@mef.gob.pe
		Rafael Vera Tudela (Titular DENPC)	997 922 430	rveratudela@mef.gob.pe
		Armando Pijo Perez (Alterno DENPC)	953 999 762	apijo@mef.gob.pe
12	Dirección General de Política de Promoción de la Inversión Privada	Karla Cuadros Ygar	946 345 377	kcuadros@mef.gob.pe

13	Oficina General de Asesoría Jurídica	Gladys Bonilla Sonco	995 657 151	gbonilla@mef.gob.pe
14	Oficina General de Planeamiento y Presupuesto	Oscar Vega Farias	991 365 486	ovegaa@mef.gob.pe
15	Oficina General de Servicios al Usuario	German Álvarez Arbulú	997 356 441	galvarez@mef.gob.pe
		Danilo cochachin Torres	948 924 350	dcochachin@mef.gob.pe
16	Oficina de Seguridad y Defensa Nacional	Carlos Echevarría Munarriz	948 868 029	cechevarria@mef.gob.pe
17	Oficina General de Administración	Laura Montes de Oca	993 49 1078	lmontesdeoca@mef.gob.pe
18	Oficina de Recursos Humanos	Catalina Magaly Acasiete Romaní	942 177 527	cacasiete@mef.gob.pe
		Diana Judith Gómez Martínez	987 791 858	dgomez@mef.gob.pe
19	Oficina General de Tecnologías de la Información	José Romucho Sotelo	975 695 085	jromucho@mef.gob.pe
		Rolly Villegas Delgado	965 366 887	rvillegas@mef.gob.pe
20	Oficina de Comunicaciones	Sonia Gilvonio Malaca	987 537 330	sgilvonio@mef.gob.pe
		Ricardo Serra Fuertes	990 059 304	rserra@mef.gob.pe

ANEXO 4: Organización para el desarrollo de las actividades críticas

En el escenario de impacto ante un evento adverso, el desarrollo de las actividades críticas estará a cargo de los órganos y unidades orgánicas responsables, según su competencia en cada una de las nueve (09) actividades identificadas como criticas (numeral 5.9 del presente). El detalle de nombres, correos y teléfonos de contacto se ubica en el siguiente link: \\ws2012-fs.mef.gob.pe\pco

1. Relación de actividades críticas y proveedores

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
E02	Gestión de la Comunicación e Imagen Institucional	E02.01.01	Difusión en medios tradicionales y plataformas de comunicación digital	OC	OC	Grupo de Comando	Interno	Requerimiento de sacar un comunicado relacionado al PCO
E04	Gestión de la Prevención e Integridad Institucional	E04.03.02	Formulación, Actualización y Ejecución del Plan de Continuidad Operativa	OGIIRO	OGRO	OSDN	Interno	Informe de evaluación de daños
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGTP	DN	MINJUS	Externo	SPIJ
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGPP	DN	MINJUS	Externo	SPIJ
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGCP	DN	DGPP	Interno	Clasificador presupuestario de ingreso y gasto
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGCP	DN	OGTI	Interno	Publicación de normativa de ampliación
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGA	DN	DGTP	Interno	Apertura de cuenta y transferencia de recursos a los pliegos

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.02	Elaboración de Instrumentos Normativos distinto de los Sistemas Administrativos	DGGFRH	DGPA	VMH	Interno	Informe de requerimiento de opinión técnica
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.01	Elaboración de Proyecciones Macroeconómicas y Fiscal	DGPMDF	DPM	Ministerio de Energía y Minas	Externo	Información de programación de inversiones y producción
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.01	Elaboración de Proyecciones Macroeconómicas y Fiscal	DGPMDF	DPM	EESI	Interno	Información de programación de inversiones
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.02	Elaboración del Marco Macroeconómico Multianual	DGPMDF	DPM	Bloomberg	Externo	Información en tiempo real de variables macroeconómicas/financieras
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.02	Elaboración del Marco Macroeconómico Multianual	DGPMDF	DPM	Dirección de Política Fiscal	Interno	Proyección del gasto público
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.05	Análisis del Contexto Macrofiscal	DGPMDF	DPM	Ositran	Externo	Información de programación de inversiones
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.05	Análisis del Contexto Macrofiscal	DGPMDF	DPM	Sunat	Externo	Información de exportaciones e importaciones
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.01.04	Seguimiento de Reglas Fiscales	DGPMDF	DPF	Sunat	Externo	Información de exportaciones e importaciones
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.01.02.01	Evaluación del Desempeño Fiscal Subnacional	DGPMDF	DPDF	DPDF	Interno	Información de finanzas subnacionales

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.02.01.01.01	Elaboración de Lineamientos de Política Tributaria	DGPIP	DIEOT, DRP, DCTCE, DATI, DTS	DGPMDF	Interno	Supuestos macroeconómicos, reglas fiscales
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.02.01.01.01	Elaboración de Lineamientos de Política Tributaria	DGPIP	DIEOT, DRP, DCTCE, DATI, DTS	DGPP	Interno	Data de recaudación y de programas de incentivos
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.02.01.01.01	Elaboración de Lineamientos de Política Tributaria	DGPIP	DIEOT, DRP, DCTCE, DATI, DTS	SUNAT	Externo	Propuestas normativas e información sobre recaudación tributaria
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.01	Elaboración de Instrumentos Normativos para los Sistemas Administrativos	DGPMI	DN	Editora Perú	Externo	Servicio de Publicación de normas
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.02.02	Gestión de Políticas Nacionales vinculadas al Sector economía y Finanzas	DGMFPP	DMF	DGTP	Interno	Evaluación de garantías nacionales
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.02	Elaboración de Instrumentos Normativos distinto de los Sistemas Administrativos	DGMFPP	DMF	OGAJ	Interno	Revisión de anteproyecto en la parte normativa
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.02	Elaboración de Instrumentos Normativos distinto de los Sistemas Administrativos	DGAEICP	DAEI	DGPIP	Interno	Validación de disposiciones normativas que involucren tributos internos
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.03.02	Elaboración de Instrumentos Normativos distinto de los Sistemas Administrativos	DGPPIP	DPIP (Políticas)	OGAJ	Interno	Revisión de anteproyecto en la parte normativa
M01	Gestión de Políticas, Planes y Normas Económicas y Financieras del Sector Público	M01.04.02	Seguimiento y Evaluación de Planes Nacionales Vinculados al Sector Economía y Finanzas	DGPPIP	DPIP (Promoción)	VME	Interno	Informe relacionado a planes nacionales vinculados al sector economía
M02	Administración Financiera del Sector Público	M02.02.04.02.01	Asignaciones financieras	DGTP	DOT	BCRP	Externo	Sistema LBTR

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M02	Administración Financiera del Sector Público	M02.02.04.02.01	Asignaciones financieras	DGTP	DOT	Banco de la nación	Externo	Aplicativo Extra
M02	Administración Financiera del Sector Público	M02.02.04.03.01	Pagos de planilla, proveedores y otros	DGTP	DOT	Banco de la nación	Externo	Aplicativo Extra
M02	Administración Financiera del Sector Público	M02.02.04.03.09	Apertura y cierre de cuentas bancarias	DGTP	DOT	RENIEC	Externo	Identificación de autoridades
M02	Administración Financiera del Sector Público	M02.02.04.03.09	Apertura y cierre de cuentas bancarias	DGTP	DOT	Banco de la nación	Externo	Aplicativo Extra
M02	Administración Financiera del Sector Público	M02.02.05.01.02.01	Concertación de operaciones de endeudamiento publico	DGTP	DC	DGTP	Interno	Programación de concertación de préstamos y bonos
M02	Administración Financiera del Sector Público	M02.02.05.01.02.05	Gestión de la atención del pago de la deuda del gobierno nacional	DGTP	DADCE	DGTP	Interno	Contratos, suscripciones y compromisos firmados
M02	Administración Financiera del Sector Público	M02.02.05.02.02	Gestión de los excedentes temporales de liquidez	DGTP	DGIFMC	BCRP	Externo	Cancelación anticipada de Depósitos a plazo
M02	Administración Financiera del Sector Público	M02.02.05.02.02	Gestión de los excedentes temporales de liquidez	DGTP	DGIFMC	Datatec	Externo	Información financiera
M02	Administración Financiera del Sector Público	M02.02.05.02.02	Gestión de los excedentes temporales de liquidez	DGTP	DGIFMC	Bloomberg	Externo	Información financiera
M02	Administración Financiera del Sector Público	M02.02.05.02.02	Gestión de los excedentes temporales de liquidez	DGTP	DGIFMC	DPFE	Interno	Plan de inversión de excedentes
M02	Administración Financiera del Sector Público	M02.02.05.09	Determinación de la disponibilidad de fondos públicos	DGTP	DPFE	SUNAT	Externo	Información de recaudación
M02	Administración Financiera del Sector Público	M02.02.05.09	Determinación de la disponibilidad de fondos públicos	DGTP	DPFE	DOT	Interno	Información de otros ingresos
M02	Administración Financiera del Sector Público	M02.02.05.09	Determinación de la disponibilidad de fondos públicos	DGTP	DPFE	DC	Interno	Programa anual de desembolsos
M02	Administración Financiera del Sector Público	M02.01.05.01	Estimación y aprobación de la Asignación Presupuestaria Multianual	DGPP	DPSP	DGPMDF	Interno	Información de Estimación de Recursos Públicos de RO y límite de gasto corriente y no financiero
M02	Administración Financiera del Sector Público	M02.01.05.01	Estimación y aprobación de la Asignación Presupuestaria Multianual	DGPP	DPSP	DGGFRH	Interno	Información del AIRSHP y conceptos remunerativos que no se registran en el

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
								AIRSHP, personal pensionista
M02	Administración Financiera del Sector Público	M02.01.05.01	Estimación y aprobación de la Asignación Presupuestaria Multianual	DGPP	DPSP	DGTP	Interno	Estimación de ingresos por Recursos Directamente Recaudados, Programación del servicio de deuda y el Programa de desembolsos de las operaciones de endeudamiento externo e interno.
M02	Administración Financiera del Sector Público	M02.01.05.02	Desagregación de la APM, Formulación y Aprobación Presupuestaria	DGPP	DPSP	DGPMDF	Interno	Actualización de Información de Estimación de Recursos Públicos de RO y límite de gasto corriente y no financiero
M02	Administración Financiera del Sector Público	M02.01.05.02	Desagregación de la APM, Formulación y Aprobación Presupuestaria	DGPP	DPSP	DGTP	Interno	Actualización de estimación de ingresos por Recursos Directamente Recaudados, Programación del servicio de deuda y el Programa de desembolsos de las operaciones de endeudamiento externo e interno.
M02	Administración Financiera del Sector Público	M02.01.05.02	Desagregación de la APM, Formulación y Aprobación Presupuestaria	DGPP	DPSP	OGTI	Interno	Servicios de soporte y mantenimiento de sistemas de información
M02	Administración Financiera del Sector Público	M02.02.07.01	Programación de compromisos anual (PCA)	DGPP	DPSP	DGTP	Interno	Información de Proyección de Ingresos
M02	Administración Financiera del Sector Público	M02.02.07.01	Programación de compromisos anual (PCA)	DGPP	DPSP	DGPP	Interno	Validación de Montos de PCA por la DPT y DAPT
M02	Administración Financiera del Sector Público	M02.02.07.01	Programación de compromisos anual (PCA)	DGPP	DPSP	DGPMDF	Interno	Información de Reglas Fiscales, Techos de Gastos y Programación RO
M02	Administración Financiera del Sector Público	M02.02.07.02	Control presupuestario de gastos	DGPP	DPSP	OGTI	Interno	Entrega de Información de Ejecución Presupuestaria del SIAF y publicación de Informe

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M02	Administración Financiera del Sector Público	M02.02.07.03.03	Modificaciones presupuestarias a nivel funcional y programático	DGPP	DAPT/DPT	DGGFRH	Interno	Información de Costos y Validación de la legalidad de los conceptos a pagar
M02	Administración Financiera del Sector Público	M02.02.07.03.03	Modificaciones presupuestarias a nivel funcional y programático	DGPP	DAPT/DPT	DGA	Interno	Información de contratos de bienes y servicios y obras
M02	Administración Financiera del Sector Público	M02.02.07.03.03	Modificaciones presupuestarias a nivel funcional y programático	DGPP	DAPT/DPT	DGTP	Interno	Opinión técnica en el marco sus funciones
M02	Administración Financiera del Sector Público	M02.02.07.03.03	Modificaciones presupuestarias a nivel funcional y programático	DGPP	DAPT/DPT	DGPMI	Interno	Información sobre Proyectos
M02	Administración Financiera del Sector Público	M02.02.07.03.01.01	Modificaciones presupuestarias por ingresos de recursos ordinarios y por endeudamiento	DGPP	DAPT/DPT	DGPMDF	Interno	Información de proyecciones por fuentes de financiamiento
M02	Administración Financiera del Sector Público	M02.02.07.03.01.01	Modificaciones presupuestarias por ingresos de recursos ordinarios y por endeudamiento	DGPP	DAPT/DPT	DGTP	Interno	Información de situación de préstamos
M02	Administración Financiera del Sector Público	M02.02.07.03.01.02	Modificaciones presupuestarias por otras fuentes de financiamiento	DGPP	DAPT/DPT /DPSP	DGPMDF	Interno	Información de proyecciones de mayor espacio para incluir más recursos al gasto
M02	Administración Financiera del Sector Público	M02.02.07.03.02.01	Modificaciones presupuestarias para la continuidad de inversiones	DGPP	DAPT/DPT /DPSP	DGPMI	Interno	Información registrada en el banco de inversiones sobre los proyectos
M02	Administración Financiera del Sector Público	M02.02.07.03.02.01	Modificaciones presupuestarias para la continuidad de inversiones	DGPP	DAPT/DPT /DPSP	OSCE	Externo	Información vinculada a los compromisos y contratos
M02	Administración Financiera del Sector Público	M02.02.07.03.02.02	Modificaciones presupuestarias por transferencia del programa de incentivos	DGPP	DCGP	Pliego Responsables de la Evaluación de las Metas de PI	Externo	Información de Evaluación de cumplimiento de Metas de PI

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M02	Administración Financiera del Sector Público	M02.02.07.03.02.03	Modificaciones presupuestarias por transferencia de la reserva	DGPP	DAPT/DPT /DPSP	Pliego Presupuestario	Externo	Sustento de Solicitud de acuerdo a los lineamientos y directiva vigentes
M02	Administración Financiera del Sector Público	M02.02.07.03.02.04	Modificaciones presupuestarias por transferencia entre pliegos	DGPP	DAPT/DPT	Pliego Presupuestario	Externo	Sustento de Solicitud de acuerdo a los lineamientos y directiva vigentes
M02	Administración Financiera del Sector Público	M02.02.07.03.02.05	Modificaciones presupuestarias por transferencias a la reserva	DGPP	DAPT/DPT	Pliego Presupuestario	Externo	Sustento de la no ejecución
M02	Administración Financiera del Sector Público	M02.02.07.04.01	Reconocimiento a la ejecución de inversiones y programa de incentivos	DGPP	DCGP	Pliego Presupuestario	Externo	Información concerniente a la medición y evaluación de las Metas
M02	Administración Financiera del Sector Público	M02.02.07.04.01	Reconocimiento a la ejecución de inversiones y programa de incentivos	DGPP	DCGP	DGPMI	Interno	Información de las inversiones provenientes del BI
M02	Administración Financiera del Sector Público	M02.02.07.04.02	Gestión de convenios de apoyo y presupuesto	DGPP	DCGP	Pliego Presupuestario	Externo	Remite al MEF información sobre indicadores, metas y ámbitos priorizados a ser medidos en el marco de los convenios
M02	Administración Financiera del Sector Público	M02.02.07.04.02	Gestión de convenios de apoyo y presupuesto	DGPP	DCGP	Entidad Cooperante	Externo	Establece los lineamientos, estrategia y la entidad a priorizar con la donación
M02	Administración Financiera del Sector Público	M02.02.07.04.02	Gestión de convenios de apoyo y presupuesto	DGPP	DCGP	DGTP	Interno	Apertura de cuenta y transferencia de recursos a los pliegos
M02	Administración Financiera del Sector Público	M02.02.07.04.02	Gestión de convenios de apoyo y presupuesto	DGPP	DCGP	Despacho Ministerial	Interno	Suscripción del aporte financiero y aceptación de la donación
M02	Administración Financiera del Sector Público	M02.03.04.01.01	Creación y/o modificación de indicadores de intervenciones	DGPP	DCGP	Pliego responsable del Programa Presupuestal	Externo	Información de las Fichas técnicas de los indicadores
M02	Administración Financiera del Sector Público	M02.03.04.01.01	Creación y/o modificación de indicadores de intervenciones	DGPP	DCGP	DPSP	Interno	Provee del Aplicativo Informático que soporta la actividad crítica
M02	Administración Financiera del Sector Público	M02.03.04.01.02	Programación de metas de indicadores	DGPP	DCGP	Pliego responsable	Externo	Información de las Fichas técnicas de los indicadores

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
						del Programa Presupuestal		
M02	Administración Financiera del Sector Público	M02.03.04.01.02	Programación de metas de indicadores	DGPP	DCGP	DPSP	Interno	Provee del Aplicativo Informático que soporta la actividad crítica
M02	Administración Financiera del Sector Público	M02.03.04.01.03	Elaboración de Reportes de valores reales de los indicadores de programas presupuestales	DGPP	DCGP	Pliego responsable del Programa Presupuestal	Externo	Información de las Fichas técnicas de los indicadores
M02	Administración Financiera del Sector Público	M02.03.04.01.03	Elaboración de Reportes de valores reales de los indicadores de programas presupuestales	DGPP	DCGP	DPSP	Interno	Provee del Aplicativo Informático que soporta la actividad crítica
M02	Administración Financiera del Sector Público	M02.03.04.02.01	Evaluación de diseño y procesos de intervenciones públicas	DGPP	DCGP	Proveedor de Evaluaciones	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.01	Evaluación de diseño y procesos de intervenciones públicas	DGPP	DCGP	Organización Especializada (BIF, FIDA, FAO, IPA, ETC)	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.01	Evaluación de diseño y procesos de intervenciones públicas	DGPP	DCGP	Pliego Presupuestario	Externo	Información de las Intervenciones Públicas o Programas Presupuestales
M02	Administración Financiera del Sector Público	M02.03.04.02.02	Evaluación de impacto de intervenciones públicas	DGPP	DCGP	Proveedor de Evaluaciones	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.02	Evaluación de impacto de intervenciones públicas	DGPP	DCGP	Organización Especializada (BIF, FIDA, FAO, IPA, ETC)	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.02	Evaluación de impacto de intervenciones públicas	DGPP	DCGP	Pliego Presupuestario	Externo	Información de las Intervenciones Públicas o Programas Presupuestales

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M02	Administración Financiera del Sector Público	M02.03.04.02.03	Evaluación de revisión de gastos de intervenciones públicas	DGPP	DCGP	Proveedor de Evaluaciones	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.03	Evaluación de revisión de gastos de intervenciones públicas	DGPP	DCGP	Organización Especializada (BIF, FIDA, FAO, IPA, ETC)	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M02	Administración Financiera del Sector Público	M02.03.04.02.03	Evaluación de revisión de gastos de intervenciones públicas	DGPP	DCGP	Pliego Presupuestario	Externo	Información de las Intervenciones Públicas o Programas Presupuestales
M02	Administración Financiera del Sector Público	M02.03.04.02.04	Elaboración del informe global de gestión presupuestaria	DGPP	DGCP	OGIP	Interno	Información de los Proyectos mayores a S/ 800,000
M02	Administración Financiera del Sector Público	M02.03.04.02.04	Elaboración del informe global de gestión presupuestaria	DGPP	DGCP	DGPMDF	Interno	Información del Entorno Macro
M02	Administración Financiera del Sector Público	M02.01.06	Administración de la Tabla de Operaciones	DGCP	DN	DOT-DGTP	Interno	Tipo de operación para Registro en tabla de operaciones
M02	Administración Financiera del Sector Público	M02.01.06	Administración de la Tabla de Operaciones	DGCP	DN	DGA	Interno	Vinculación de Item del catálogo MEF
M02	Administración Financiera del Sector Público	M02.02.02.02	Habilitación o Modificación de registros en el AIRHSP	DGGFRH	DTRI	ORH	Interno	Informe de Requerimiento de habilitación
M02	Administración Financiera del Sector Público	M02.01.01	Elaboración del programa Multianual de Inversiones del Estado (PMIE)	DGPMI	DPEIP	Infoobras	Externo	Información de obras
M02	Administración Financiera del Sector Público	M02.02.01	Gestión de la Inversión Pública	DGPMI	DGI	SEACE	Externo	Información de contrataciones
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.01	Emisión de opinión técnica económica y Financiera	DGPP	DGPP	Todos UO	Externo	Servicio especializado de evaluaciones de impacto, diseño, procesos y revisiones de gasto
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada	M03.03.01	Asistencia técnica en el marco de la administración	DGA	DN	DGPMI	Interno	Información de las inversiones provenientes del BI

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
	Económica y Financiera del Sector Público		financiera del sector Público					
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.01	Emisión de opinión técnica económica y Financiera	DGGFRH	DGPA	VMH	Interno	Informe de requerimiento de opinión técnica y financiera
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.03.03	Asistencia técnica no vinculada a la administración financiera del sector público	DGPMDF	DPDF	OGSU	Interno	Contactos de funcionarios municipales
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.01	Emisión de opinión técnica económica y Financiera	DGPIP	DIEOT, DRP, DCTCE, DATI, DTS	VME	Interno	Directrices sobre políticas de gobierno en situación de emergencia
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.03.03	Asistencia técnica no vinculada a la administración financiera del sector público	DGPIP	DTS	VME	Interno	Directrices sobre políticas de gobierno en situación de emergencia
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.01	Emisión de opinión técnica económica y Financiera	DGPMI	DSEIP	Infoobras	Externo	Información de obras
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.03.01	Asistencia ténica en el marco de la administración financiera del sector Público	DGPMI	DPEIP/DGI/ DSEIP	OGTI	Interno	Soporte técnico a los aplicativos de la DGPMI
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.02	Emisión de opinión Técnica en análisis de calidad regulatoria - ACR sectorial y multisectorial	DGAEICP	DAEI	SUNAT	Externo	Propuesta de proyectos normativos y remisión de información operativa

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
M03	Gestión de la Asistencia, Opinión y Capacitación Técnica Especializada Económica y Financiera del Sector Público	M03.02.01	Emisión de opinión técnica económica y Financiera	DGPPIP	DPIP (Promoción)	VME	Interno	Informe relacionado a opinión vinculados al sector economía
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.01	Asesoría legal a órganos del MEF	OGAJ	OAJEA	VMH	Interno	Antecedentes e informes Técnicos del VMH relacionado con Asesoría
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.01	Asesoría legal a órganos del MEF	OGAJ	OAJEA	VME	Interno	Antecedentes e informes Técnicos del VME Relacionado con Asesoría
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.01	Asesoría legal a órganos del MEF	OGAJ	OAJEA	SG- OGPP	Interno	Antecedentes e informes técnicos para aprobación de normas de la SG
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.02	Opinión legal a documentos de gestión e instrumentos normativos	OGAJ	OAJH	VMH	Interno	Antecedentes e informes Técnicos del VMH relacionado opinión legal
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.02	Opinión legal a documentos de gestión e instrumentos normativos	OGAJ	OAJH	VME	Interno	Antecedentes e informes Técnicos del VME relacionado opinión legal
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.01.02	Opinión legal a documentos de gestión e instrumentos normativos	OGAJ	OAJEA	SG- OGPP	Interno	Antecedentes e informes técnicos para aprobación de normas de la SG
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.03.02	Elaboración de Carpeta de la Comisión de Coordinación Viceministerial	OGAJ	OAJH	VMH	Interno	Antecedentes e informes Técnicos del VMH de coordinación Viceministerial
S01	Asesoramiento Jurídico y Defensa Jurídica	S01.03.02	Elaboración de Carpeta de la Comisión de Coordinación Viceministerial	OGAJ	OAJH	VME	Interno	Antecedentes e informes Técnicos del VME de coordinación Viceministerial
S02	Gestión del Talento Humano	S02.02.02.02	Gestión de procedimiento Administrativo Disciplinario	OGA	ORH	OGSU	Interno	SGDD
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	DGGFRH	Interno	Habilitación de registros en el AIRHSP
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	SUNAT	Externo	T-registro -PLAME

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Cooperativa de servicios Múltiples MEFC	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Cooperativa de Ahorro y Crédito San Isidro	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Cooperativa El Tumi	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Banco de Comercio	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Cooperativa de Ahorro y Crédito Finantel	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Rimac Seguros y Reaseguros o Rimac S.A	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Cooperativa de Ahorro y Crédito de Trabajadores del Sector Salud – TSS	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Coop. de Ahorro y Crédito Servicio Aduanero del Perú	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Coop. de Ahorro y Crédito SERFINCO	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Coop. de Ahorro y	Externo	Reporte de descuentos

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
						Crédito El Dorado		
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Coop. de Crédito y Asistencia - COOPCREAS	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.03.02	Elaboración de Planilla única de Pago	OGA	ORH	Coop. de Ahorro y Crédito San Miguel Ltda.	Externo	Reporte de descuentos
S02	Gestión del Talento Humano	S02.05.01	Gestión de la Seguridad y Salud en el Trabajo	OGA	ORH	EPS de salud	Externo	Coordinación de seguro del personal
S03	Gestión de Tecnología de la Información	S03.03.02	Diseño, implementación y mantenimiento de la Plataforma Tecnológica	OGTI	OIT	Órganos MEF	Interno	Mantenimiento relacionado a TI
S03	Gestión de Tecnología de la Información	S03.03.03	Gestión de incidencias de los servicios de Tecnologías de la Información	OGTI	OIT	Órganos MEF	Interno	Requerimiento de solución de incidencias
S04	Gestión Documental y de Atención al Usuario	S04.01.01	Recepción Documental	OGSU	OGDAU	OGTI	Interno	Almacenamiento y conservación de microformas
S04	Gestión Documental y de Atención al Usuario	S04.02.01	Atención de consultas	OGSU	OGDAU	DGPP	Interno	Lineamientos técnicos y normativos relacionados a presupuesto
S04	Gestión Documental y de Atención al Usuario	S04.02.01	Atención de consultas	OGSU	OGDAU	DGTP	Interno	Lineamientos técnicos y normativos relacionados a tesorería
S05	Gestión de Recursos Institucionales	S05.02.02	Gestión Presupuestaria Institucional y Modificaciones	OGPP	OPICT	DGPP	Interno	Aprobación de la PCA vía SIAF (web operaciones en línea)
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	Órganos MEF	Interno	Requerimiento de contratación
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	SEDAPAL	Externo	Abastecimiento de agua
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	ENEL	Externo	Energía eléctrica
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	Luz de Sur	Externo	Energía eléctrica

COD	Actividades críticas	COD	Tarea / Procedimiento	Órgano	Unidad orgánica	Proveedor	Tipo	Servicio
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	La Protectora	Externo	Brocker de Seguros
S05	Gestión de Recursos Institucionales	S05.04.03.02	Proceso de Contratación	OGA	OAB	La Positiva Seguros	Externo	Brocker de Seguros
S05	Gestión de Recursos Institucionales	S05.04.03.03	Ejecución Contractual	OGA	OAB	Órganos MEF	Interno	Consentimiento de buena pro
S05	Gestión de Recursos Institucionales	S05.05.02.02	Gestión de Pagos	OGA	OFI	Órganos MEF	Interno	Expediente Administrativo de pagos
S05	Gestión de Recursos Institucionales	S05.05.02.02	Gestión de Pagos	OGA	OFI	Banco de la Nación	Externo	Pagos de transferencias interbancarias
S05	Gestión de Recursos Institucionales	UTP-FAG.01.01	Registros de contratos FAG y PAC	OGA	UTP FAG	Órganos MEF	Interno	Expediente Administrativo de pagos
S05	Gestión de Recursos Institucionales	UTP-FAG.01.02	Trámite de pago de los Consultores FAG y PAC	OGA	UTP FAG	Órganos MEF	Interno	Expediente Administrativo de pagos

ANEXO 5: Sistema de comunicaciones de emergencia

1. Recursos de comunicaciones

Los recursos que se emplean como Sistemas de Comunicaciones Convencionales (Canales Primarios) que brindan las empresas proveedoras de servicio de telecomunicaciones en el país y funcionan permanentemente; sin embargo, se estima que serán los primeros en bloquearse, saturarse o dejar de funcionar ante la afectación por diferentes motivos.

Los canales de comunicación empleados por el MEF son:

a. Chat WhatsApp y Telegram
b. Mensaje de texto
c. Redes sociales
d. Llamadas a celular y teléfono fijo

Para garantizar la Continuidad Operativa se realizará una mayor explotación de los sistemas de comunicaciones existentes empleando los equipos disponibles y se deberá considerar la posibilidad de adquirir equipos de radio o solicitar el apoyo de la OSDN para la comunicación RECSE[11]

2. Protocolo de comunicación externa

2.1. Objeto

Garantizar la transmisión de información a la ciudadanía en general sobre la situación, acciones y medidas tomadas por el Ministerio de Economía y Finanzas (MEF) frente a la ocurrencia de escenarios de crisis y/o emergencia.

2.2. Escenario de activación

Evento disruptivo

2.3. Participantes

- Ministro(a)
- Viceministros(as)
- Secretario(a) General
- Directores(as) de los órganos
- Coordinador del COES-EF (Oficina de Seguridad y Defensa Nacional - OSDN)
- Coordinador del COEN (Presidencia del Consejo de Ministros - PCM)

2.4. Vocero Oficial

Es el/la funcionario(a) del MEF, designado(a) como tal por la alta dirección, tendrá las funciones de portavoz en situaciones de crisis y/o emergencia. El director(a) a cargo de la Oficina de Comunicaciones comunicará al Vocero(a) Oficial el momento o la oportunidad de la comunicación, previa coordinación de la información o temas a difundir, según sea el caso.

[11] Actualmente cuenta con esta red de comunicación: Despacho Ministerial; viceministro de Hacienda; viceministro de Economía y el Coordinador COES-MEF (director de la OSDN)

Toda comunicación o información oficial se deberá coordinar con la Oficina de Comunicaciones, siendo la única autorizada para su difusión. Ningún funcionario(a), no autorizado(a) o designado vocero(a), podrá brindar información que no esté autorizado(a) a emitir.

2.5. Herramientas para la Comunicación

Los documentos que son parte de las herramientas de comunicación serán elaborados por la Oficina de Comunicaciones, con información proporcionada por los órganos de línea. La Oficina de Comunicaciones estará a cargo de la coordinación y relacionamiento con los medios de comunicación.

Toda información antes de ser difundida a través de los canales oficiales deberá ser aprobada por la Alta Dirección.

Entre las herramientas de comunicación se encuentran:

- Comunicado
  Documento informativo breve, con información concisa y específica sobre un tema que se considere de especial interés. Se difundirá a través de los canales oficiales del MEF y se enviará a los medios de comunicación.

- Nota de Prensa
  Documento con información de interés que se desarrolla, de manera preferente, como máximo en dos páginas. Este documento contiene mensajes e información clave que se explica de manera detallada, la cual se requiere comunicar de manera oficial a través de los medios de prensa.

- Entrevistas
  Es el encuentro concertado del Vocero Oficial con un periodista de un medio de prensa, en la cual se desarrollan los temas de coyuntura e interés para el conocimiento público.

- Conferencia de prensa
  Reunión con los medios de prensa a fin de comunicar información de relevancia que se requiere difundir de manera directa.

- Redes Sociales
  Las cuentas institucionales del MEF en redes sociales tienen por finalidad la difusión de la información oficial de la institución.

2.6. Periodicidad con la que se comunica información

Se realizará en coordinación con la Oficina de comunicaciones, cada vez que la Alta Dirección o el Grupo Comando vea por conveniente brindar información acerca de la situación o actividades de la institución en el marco de la ocurrencia de escenarios de crisis y/o emergencia, mientras se recuperan los servicios esenciales (o priorizados) que brinda el MEF en su totalidad.

2.7. Procedimiento de comunicación externa

Declarada la crisis y/o emergencia, y definida la información que se difundirá a los medios de comunicación por parte de la Alta Dirección o el Grupo Comando, el Director(a) de la Oficina de Comunicaciones coordinará las acciones de comunicación externa que se requieran.

Fase Inicial

a. Evaluar la situación (escenarios, riesgos) de la crisis/emergencia y su visualización en los medios de prensa.
b. Recopilar la información disponible y necesaria con los órganos de línea.
c. Alertar a la Alta Dirección y los jefes o directores de las áreas involucradas acerca de las principales informaciones difundidas en los medios de prensa.
d. Identificar las necesidades de información.

Fase de estrategia

a. Determinar los posibles escenarios de requerimiento de información generados por la crisis/emergencia, de ser necesario.
b. Identificar las herramientas de comunicación a utilizar, según sea el caso.
c. Identificar los medios de prensa que ayudarán a una comunicación más eficientes, teniendo en cuenta la crisis/emergencia, de la información y mensajes de la institución.
d. Los materiales de comunicación desarrollados deben contener mensajes claros, breves y directos.

Fase de ejecución

a. Comunicación externa a través del uso de las herramientas de comunicación.
b. Evaluar el progreso o desarrollo de la comunicación: monitoreo de las publicaciones o difusiones de los medios de prensa.

La Oficina de Comunicaciones continuará con el monitoreo de los medios de comunicación para reportar cualquier problema o incidente sobre los servicios esenciales (o priorizados) que brinda el MEF.

3. Protocolo de comunicación interna

Comprende las comunicaciones al interior del MEF, entre la Alta Dirección por los medios convencionales y la RECE[12], mientras que el resto de personal involucrado en la continuidad operativa la comunicación se desarrolla a través de los medios convencionales[13].

[12] Despacho Ministerial; Viceministro de Hacienda; Viceministro de Economía y el Coordinador COES-MEF (Director de la OSDN)
[13] Chat Grupo de Comando para la continuidad operativa del MEF

ANEXO 6: Cronograma de implementación de la Gestión de la Continuidad Operativa

En el cronograma de implementación, se considera las actividades a ejecutar, detallando la modalidad de la ejecución, los órganos responsables con la coordinación del Grupo de Comando y se indican también las fechas probables.

Nº	Actividad	Medio/Modalidad	Responsable	Fecha estimada
Actividades para la integración de la Continuidad Operativa a la Cultura Organizacional				
1	Evaluación del grado de conocimiento sobre la gestión de Continuidad Operativa	Encuestas	Quien preside el Grupo de Comando	**Semestral:** Febrero y agosto
2	Desarrollo y mejora de la cultura de continuidad Operativa.	Charlas	Quien preside el Grupo de Comando	**Semestral:** Marzo y Setiembre
3	Acciones de sensibilización a fin de internalizar la Continuidad Operativa.	Campaña de sensibilización	Oficina de Comunicaciones / Grupo de Comando	**Trimestral:** Marzo Junio Setiembre Diciembre
4	Reporte de seguimiento para alta dirección (según formato Anexo 4 de lineamiento para la Gestión de la Continuidad Operativa y la Formulación del Plan de Continuidad de las Entidades Públicas en los tres niveles de gobierno)	Documento que contiene la confirmación o posibles variaciones de actividades (MAPROS), personal asignado, materiales, entre otros, necesarios para la ejecución de cada actividad crítica	Quien preside el Grupo de Comando	**Semestral:** Mayo y Noviembre
Actividades de monitoreo y evaluación de los recursos para la Continuidad Operativa				
1	Evaluación del funcionamiento de los recursos informáticos en la Sede Alterna.	Informe	Representante de la OGTI/Grupo de Comando	**Semestral:** Abril y Octubre
2	Monitoreo y actualización del personal titular y alterno que desarrolla las actividades críticas	Correo de confirmación	Quien preside el Grupo de Comando	**Mensual:** Actualización mensual plazo máx. hasta 1era quincena de cada mes
3	Actualización de los integrantes del Grupo de Comando.	Correo de confirmación	Quien preside el Grupo de Comando	**Semestral:** Enero y Julio
4	Actualización de los BIAs	Archivo Excel	Quien preside el Grupo de Comando	**Anual** (de enero a marzo)
5	Evaluación del PCO en ejercicios programados	Informe	Quien preside el Grupo de Comando	Según cronograma establecido de ejercicios