Resolución de Secretaría General

Nº 012-2016-MIDIS/SG

Lima, 31 MAYO 2016

VISTOS:

El Memorando N° 224-2016-MIDIS/SG/OGTI, emitido por la Oficina General de Tecnologías de la Información; y el Informe N° 244-2016-MIDIS/SG/OGPP, emitido por la Oficina General de Planeamiento y Presupuesto;

CONSIDERANDO:

Que, mediante Ley N° 29792, se creó el Ministerio de Desarrollo e Inclusión Social, determinándose su ámbito, competencias, funciones y estructura orgánica básica;

Que, de conformidad con lo establecido en el artículo 33 del Reglamento de Organización y Funciones del Ministerio de Desarrollo e Inclusión Social, aprobado por Decreto Supremo N° 011-2012-MIDIS, la Oficina General de Tecnologías de la Información es el órgano de apoyo encargado de brindar soluciones en materia de comunicaciones e informática a los órganos del Ministerio para la mejor ejecución de sus políticas y funciones, y tiene entre sus funciones, diseñar, gestionar y proponer las normas sobre la seguridad de los sistemas de información, red informática y de comunicaciones del Ministerio;

Que, en el marco de dichas competencias, mediante el Memorando N° 224-2016-MIDIS/SG/OGTI, la Oficina General de Tecnologías de la Información propone la aprobación del "Plan de Continuidad del Centro de Datos del Ministerio de Desarrollo e Inclusión Social – 2016", el cual tiene por objetivo definir acciones y procedimientos necesarios para garantizar la rápida y oportuna recuperación y puesta en marcha de los sistemas que soportan las operaciones del centro de datos del Ministerio;

Que, mediante Informe N° 244-2016-MIDIS/SG/OGPP, la Oficina General de Planeamiento y Presupuesto emite opinión técnica favorable y considera procedente la aprobación del proyecto de plan propuesto;

Que, en consecuencia, en el marco de las competencias asignadas a la Oficina General de Tecnologías de la Información, y considerando lo informado por la Oficina General de Planeamiento y Presupuesto, resulta procedente aprobar el proyecto de "Plan de Continuidad del Centro de Datos del Ministerio de Desarrollo e Inclusión Social – 2016", a fin de coadyuvar al mejor cumplimiento de los fines institucionales; y,

Con el visado de la Oficina General de Tecnologías de la Información, de la Oficina General de Planeamiento y Presupuesto, y de la Oficina General de Asesoría Jurídica; y,

De conformidad con lo dispuesto por la Ley Nº 29792, Ley de Creación, Organización y Funciones del Ministerio de Desarrollo e Inclusión Social; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo Nº 011-2012-MIDIS;

SE RESUELVE:

Artículo 1.- Aprobación del Plan de Continuidad del Centro de Datos del Ministerio de Desarrollo e Inclusión Social – 2016

Aprobar el "Plan de Continuidad del Centro de Datos del Ministerio de Desarrollo e Inclusión Social – 2016", conforme al anexo que forma parte integrante de la presente resolución.

Artículo 2.- Difusión

Disponer la publicación de la presente resolución y del plan que se aprueba en el Portal Institucional del Ministerio de Desarrollo e Inclusión Social (www.midis.gob.pe).

Artículo 3.- Notificación

Notificar la presente resolución y su anexo a la Oficina General de Tecnologías de la Información, para su cumplimiento y fines pertinentes.

Regístrese y comuníquese.

MIDIS V°B° Oficina General de Asesoría Jurídica

Oficina General de Tecnologías de la Información V°B° W. Carcheri G. Jefe MIDIS

MIDIS Oficina General de Planeamiento y Presupuesto

IVÁN SÁNCHEZ GONZÁLES
Secretario General
MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL

PERÚ | Ministerio de Desarrollo e Inclusión Social

PLAN DE CONTINUIDAD DEL CENTRO DE DATOS DEL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL 2016

Oficina General de Tecnologías de la Información

INDICE

Oficina General de Tecnologías de la Información
V°B°
W. Cardheri G.
Jefe
MIDIS

1. OBJETIVO

Definir las acciones y procedimientos necesarios para garantizar la rápida y oportuna recuperación y puesta en marcha de los sistemas que soportan las operaciones del centro de datos.

2. ALCANCE

El presente Plan aplica a la continuidad operativa de los servicios críticos del Centro de Datos del Ministerio de Desarrollo e Inclusión Social basado en los escenarios identificados durante el análisis de riesgos.

3. DOCUMENTOS DE REFERENCIA

- NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

4. DEFINICIONES Y ABREVIATURAS

- **Activo de Información:** Comprende a cada elemento que soporta la información, es decir que la contiene, la procesa o la transporta.
- **CID:** Confidencialidad, Integridad y Disponibilidad de la Información.
- **Confidencialidad:** Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la exactitud y completitud de la información.
- **Disponibilidad:** Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.
- **Riesgo:** Incertidumbre que podría causar una desviación de los objetivos.
- **Amenazas:** Causa potencial de un incidente no deseado que podría resultar en la puesta en peligro de un sistema o una organización
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Probabilidad:** Posibilidad de que algún hecho se produzca.
- **Impacto:** Resultado de un suceso que afecta a los objetivos.
- **Plan de Continuidad:** Conjunto de acciones específicas que conducen a responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción.
- **Continuidad Operativa:** Capacidad de la institución para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.
- **Activación:** Acto de declarar que las disposiciones sobre continuidad del negocio de la institución se deben poner en marcha con objeto de continuar suministrando los productos y servicios principales.
- **Prueba:** Proceso para adiestrar, evaluar, practicar y mejorar el rendimiento de una institución.
- **Incidente Disruptivo:** Situación que podría provocar o conducir a una interrupción, una pérdida, una emergencia o una crisis.
- **Parte Interesada:** Persona u organización que puede afectar, ser afectada por, o percibir que ella misma puede verse afectada por una decisión o actividad.

Oficina General de Tecnologías de la Información V°B° W. Carcheri G. Jefe

- **SISFOH:** Sistema de Focalización de Hogares
- **SIAF:** Sistema Integrado de Administración Financiera
- **SIGA:** Sistema Integrado de Gestión Administrativa
- **CAS:** Contratos Administrativos de Servicios

5. DESARROLLO

5.1. SERVICIOS CRÍTICOS

- Sistema de Focalización de Hogares - SISFOH
- Orienta MIDIS
- Convocatorias CAS
- Info MIDIS
- SIAF (Sistema Integrado de Administración Financiera)
- SIGA (Sistema Integrado de Gestión Administrativa)
- Sistema Nacional de Alertas Cuna Mas
- Sistema de Administración de Usuarios MIDIS
- Correo Electrónico
- Página Web

5.2. ACTIVOS DE INFORMACIÓN CRÍTICOS

Nº	ACTIVO ASOCIADO	PROPIETARIO
	Sistema de Focalización de Hogares - SISFOH	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
7.	Servidores Web en Máquina Virtuales	OGTI
8.	Servidores de base de datos	OGTI
9.	Sistemas Operativos	OGTI
	Orienta MIDIS	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidor de aplicaciones web orientaDMZ.midis.gob.pe	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	Convocatorias CAS	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI

Oficina General de Tecnologías de la Información V°B° W. Carcheri G. Jefe MIDIS

Nº	ACTIVO ASOCIADO	PROPIETARIO
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidor de aplicaciones web	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	Info MIDIS	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidores Web en Máquina Virtuales	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	SIAF (Sistema Integrado de Administración Financiera)	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidor SIAF (Hera)	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	SIGA (Sistema Integrado de Gestión Administrativa)	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI

Oficina General de Tecnologías de la Información
VºBº
W. Cancheri G.
Jefe
MIDIS

Nº	ACTIVO ASOCIADO	PROPIETARIO
8.	Servidores Web en Máquina Virtual Pegasus.midis.gob.pe	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	Correo Electrónico	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidores de Correo Zimbra	OGTI
9.	Servidor de Contingencia	OGTI
10.	Sistemas Operativos	OGTI
	Página Web – Portal MIDIS	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidores Web en Máquina Virtuales	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	Sistema Nacional de Alertas Cuna Mas	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidores Web en Máquina Virtuales	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI
	Sistema de Administración de Usuarios MIDIS	
1.	BATERIA UPS GENERAL DATA CENTER - Fuente de Poder	OGTI

Oficina General de Tecnologías de la Información
V°B°
W. Carcheri G.
Jefe
MIDIS

Nº	ACTIVO ASOCIADO	PROPIETARIO
2.	Grupo electrógeno de todo el Centro de Datos - Fuente de Poder	OGTI
3.	Switch Core Principal	OGTI
4.	Switch Core de Contingencia	OGTI
5.	TRANSFORMADOR DE AISLAMIENTO DATA CENTER - Fuente de Poder	OGTI
6.	UPS GABINETE DATA CENTER - Fuente de Poder	OGTI
7.	UPS GENERAL DATA CENTER - Fuente de Poder	OGTI
8.	Servidores Web en Máquina Virtuales	OGTI
9.	Servidores de base de datos	OGTI
10.	Sistemas Operativos	OGTI

Oficina General de Tecnologías de la Información
V°B°
W. Cardenas G.
Jefe
MIDIS

5.3. IDENTIFICACIÓN DE ESCENARIOS

Nº	ESCENARIO	SERVICIOS AFECTADOS	PROBABILIDAD	IMPACTO
1.	Pérdida del suministro eléctrico	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Correo Electrónico • Página Web	Baja	Alto
2.	Pérdida de disponibilidad de servidor físico	• SIAF	Baja	Alto
3.	Pérdida de disponibilidad de las máquinas virtuales	• Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Página Web	Baja	Alto
4.	Indisponibilidad del personal encargado del centro de datos	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA	Media	

Oficina General de Tecnologías de la Información
V°B°
W. Carchen G.
Jefe
MIDIS

Nº	ESCENARIO	SERVICIOS AFECTADOS	PROBABILIDAD	IMPACTO
		• Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Correo Electrónico • Página Web		
5.	Pérdida de disponibilidad del servicio de internet	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Correo Electrónico • Página Web	Baja	Alto
6.	Pérdida del servicio de correo electrónico	• Correo Electrónico	Media	Alto
7.	Caída del servidor de base de datos	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS	Baja	Alto
8.	Corrupción de información critica	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS	Baja	Alto

Oficina General de Tecnologías de la Información
V°B°
W. Catcheri G.
Jefe
MIDIS

Nº	ESCENARIO	SERVICIOS AFECTADOS	PROBABILIDAD	IMPACTO
		• Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Correo Electrónico • Página Web		
9.	Caída en el servicio de red	• Sistema de Focalización de Hogares - SISFOH • Orienta MIDIS • Convocatorias CAS • Info MIDIS • SIAF (Sistema Integrado de Administración Financiera) • SIGA • Sistema Nacional de Alertas Cuna Mas • Administrador de Usuarios MIDIS • Correo Electrónico • Página Web	Baja	Alto

Oficina General de Tecnologías de la Información
V°B°
W. Cacchiarí G.
Jefe
MIDIS

6. DESARROLLO DE LOS ESCENARIOS

6.1. PÉRDIDA DEL SUMINISTRO ELÉCTRICO

Acciones:

En caso ocurra algún incidente o suceso que interrumpa el suministro de energía eléctrica, el Oficial de Seguridad de la Información se asegurará que se ejecuten las acciones descritas en este apartado.

- Se activa el grupo electrógeno automáticamente, tomando en consideración que se tienen UPS presentes en el centro de datos como contingencia al grupo electrógeno.
- Verificar que se cuente con la cantidad de combustible suficiente para el correcto encendido y funcionamiento del grupo electrógeno.
- Comunicarse con la empresa proveedora de energía eléctrica para obtener información sobre el corte de energía eléctrica que ha ocurrido.
- Comunicar a las partes interesadas que está ocurriendo un incidente relacionado al suministro eléctrico, indicando las implicaciones sobre la disponibilidad de los sistemas involucrados.
- Monitorear continuamente el nivel del combustible para proceder con la recarga del tanque de combustible del grupo mientras dure el corte de energía.
- Comunicarse continuamente con la empresa proveedora de energía eléctrica para asegurar el restablecimiento del suministro eléctrico.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad una vez que el corte de energía eléctrica se haya restablecido y continuar con el normal funcionamiento de sus operaciones.

6.2. PÉRDIDA DE DISPONIBILIDAD DE SERVIDOR FÍSICO

Acciones:

En el caso de que ocurra algún incidente que imposibilite el uso de uno o más servidores físicos gestionados en el centro de datos, se requerirá realizar las siguientes acciones para reestablecer los servicios que pudieran haber sido afectados. Las siguientes acciones serán ejecutadas por el Analista y Programador de Infraestructura Electrónica supervisado por el Oficial de Seguridad de la Información.

- Contactar al proveedor de custodia de las cintas de respaldo para su transporte al centro de datos.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de las aplicaciones asociadas a los servidores no disponibles.
- Crear máquina virtual y restaurar el back up desde la cinta.
- Restaurar en la máquina virtual los datos del servidor físico que no está disponible.
- Realizar la investigación de las causas de la indisponibilidad y restaurar el servicio en el servidor físico original de ser posible.
- En caso no sea posible restaurar el servicio original, evaluar la posibilidad de acondicionar una máquina física para restaurar el servicio o acondicionar la máquina virtual para convertirse en el servidor definitivo.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones.

6.3. PÉRDIDA DE DISPONIBILIDAD DE LAS MÁQUINAS VIRTUALES

Acciones:

En el caso de que ocurra algún incidente que imposibilite el uso de una o más máquinas virtuales gestionadas en el centro de datos, se requerirá realizar las siguientes acciones para reestablecer los servicios que pudieran haber sido afectados. Las siguientes acciones serán ejecutadas por el Analista y Programador de Infraestructura Electrónica supervisado por el Oficial de Seguridad de la Información.

- Contactar al proveedor de custodia de las cintas de respaldo para su transporte al centro de datos.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de las aplicaciones asociadas a las máquinas virtuales no disponibles.
- Restaurar las imágenes de las máquinas virtuales para restaurar las que no están disponibles.
- Realizar la investigación de las causas de la indisponibilidad y restaurar el servicio en la máquina virtual original de ser posible.
- En caso no sea posible restaurar el servicio original, acondicionar la máquina virtual de contingencia.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones.

6.4. INDISPONIBILIDAD DEL PERSONAL ENCARGADO DEL CENTRO DE DATOS

Acciones:

En el caso que el personal del Data Center no se encuentre disponible, se asignará a un personal de soporte con las capacidades técnicas suficientes para suplir temporalmente al personal del Data Center.

El personal de soporte utilizará los instructivos de operación provistos para continuar con la labor diaria y atender las diferentes solicitudes o inconvenientes que se puedan presentar.

La asignación de responsables de contingencia para las operaciones del centro de datos, designados debido a sus habilidades técnicas, será la siguiente:

Actividad	Responsable Alternativo
Administración de los servidores de bases de datos Oracle, MySQL y MSSQL	Julio Cerna / José Cárdenas
Administración del servidor de correo Zimbra	Julio Cerna / Maurice Frayssinet
Administración del Hypervisor y las máquinas virtuales	Julio Cerna / Maurice Frayssinet
Administración de los servidores de aplicaciones y página web	Julio Cerna / Fredy Papa

Vuelta a la normalidad

Una vez vuelva a sus labores el personal del Centro de Datos, el personal de contingencia le informará sobre lo realizado durante su ausencia, los requerimientos, incidentes y cambios que pudieran haber ocurrido en su ausencia.

6.5. PÉRDIDA DE DISPONIBILIDAD DEL SERVICIO DE INTERNET

Acciones:

Considerando el caso en que se pierda el servicio de internet por falla en el proveedor se tendrán que realizar las siguientes acciones con el fin de recuperar el servicio.

- Comunicar con el proveedor para identificar el punto de fallo.
- Comunicar a los usuarios la pérdida del servicio de internet.
- Habilitar el enlace de contingencia con la configuración del enlace primario.
- Asegurar que las aplicaciones funcionen adecuadamente externamente.
- Validar que los usuarios tengan salida a internet.
- Coordinar con el proveedor la vuelta a la normalidad del servicio de internet.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones.

6.6. PÉRDIDA DEL SERVICIO DE CORREO ELECTRÓNICO

Acciones:

En el caso que se produzca una indisponibilidad en el servicio de correo electrónico debido a problemas en el servidor de correo, se cuenta con un equipo de contingencia en réplica con el servidor principal, la cual se realiza a diario. Para la continuidad del servicio de correo el Analista y Programador de Infraestructura Electrónica requiere realizar las siguientes actividades:

- Comunicar a los usuarios la indisponibilidad del servicio de correo.
- Cambiar la dirección IP del servicio de correo.
- Levantar el servicio de correo del servidor de contingencia.

Oficina General de Tecnologías de la Información VoBº W. Carcheri G. Jefe MIDIS

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones. Además de notificar a las partes interesadas sobre la posible pérdida que se haya podido ocasionar si no se recuperó la información en su completitud.

6.7. CAÍDA DEL SERVIDOR DE BASE DE DATOS

Acciones:

En el caso que se pierda disponibilidad del servidor de base de datos, se requiere realizar las siguientes acciones para asegurar la continuidad operativa de los servicios relacionados a estas bases de datos.

- Contactar al proveedor de custodia de las cintas de respaldo para su transporte al centro de datos.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de las aplicaciones asociadas a las máquinas virtuales no disponibles.
- Reinstalar el servidor de base de datos en la cuchilla de contingencia.
- Restaurar los backups de las bases de datos en la cuchilla de contingencia disponible.
- Restaurar el servicio de base de datos en la cuchilla de contingencia.
- Realizar la investigación de las causas de la indisponibilidad.
- En caso no sea posible restaurar el servicio de producción original, se utilizará el servidor de contingencia como producción y la cuchilla de producción será la nueva contingencia de ser posible.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones. Además de notificar a las partes interesadas sobre la posible pérdida que se haya podido ocasionar si no se recuperó la información en su completitud.

6.8. CORRUPCIÓN DE INFORMACIÓN CRÍTICA

Acciones:

En el caso que ocurra una corrupción o pérdida de información crítica de la institución, se realizarán las siguientes actividades para asegurar que se restaure el servicio asociado a la información que se quiere recuperar.

- Contactar con el responsable de la información para saber cuál es la información faltante.
- Contactar al proveedor de custodia para hacer efecto el traslado de emergencia de las cintas de respaldo para su transporte al centro de datos.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de la información crítica inaccesible.
- Restaurar la información requerida de las copias de respaldo correspondientes.
- Validar con el responsable de la información la integridad de los datos.

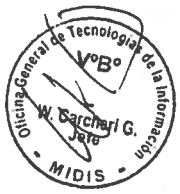
Vuelta a la normalidad:

Notificar a las partes interesadas sobre la recuperación exitosa de la información o de la pérdida que se haya podido ocasionar si no se recuperó la información en su completitud

6.9. CAÍDA EN EL SERVICIO DE RED

Acciones:

En el caso de que ocurra algún incidente que imposibilite el uso de uno o más dispositivos de red gestionados en el centro de datos, se requerirá realizar las siguientes acciones para reestablecer los servicios que pudieran haber sido afectados. Las siguientes acciones serán ejecutadas por el Analista y Programador de Infraestructura Electrónica supervisado por el Oficial de Seguridad de la Información.



- Identificar el punto de fallo en la infraestructura de red.
- Reestablecer los parámetros de operación normal y realizar un reinicio del dispositivo afectado.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de las aplicaciones asociadas a las máquinas virtuales no disponibles.
- Instalar y configurar equipo de contingencia para reestablecer el servicio en las áreas afectadas hasta que ocurra una acción del proveedor.
- Contactar con el proveedor para hacer efecto de la garantía del dispositivo.
- Coordinar constantemente con el proveedor para asegurarse de la correcta ejecución de la garantía del equipo afectado.

Vuelta a la normalidad:

Se comunicará por los medios establecidos a todos las partes interesadas la vuelta a la normalidad de los servicios que hayan sido afectados por el incidente disruptivo y continuará con el normal funcionamiento de sus operaciones.

Para la ejecución de las acciones detalladas, la Oficina General de Tecnología de la Información – OGTI, será la encargada de incluir en el Plan Operativo Institucional Anual de cada año los recursos que requiera para su implementación en el contexto del Plan Operativo Informativo Anual.

7. PLAN DE PRUEBAS

El Plan de Continuidad comprende, finalmente, el desarrollo de un plan de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.

Los siguientes son los objetivos de control de las pruebas del plan:

- Validar la habilidad de los encargados y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.
- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación
- Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias.
- Motivar a los encargados involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos inherentes.

La ejecución del cronograma de pruebas se realizará en una solución de virtualización y/o servidores físicos dependiendo sea el caso, donde se montarán los servidores acordes a los aplicativos y se restauraran los servicios, bajo los procedimientos indicados por el Jefe de la OGTI y especialistas que estén apoyando.

7.1. CRONOGRAMA DE PRUEBAS

Actividad	Junio	Julio – Septiembre	Octubre -Diciembre
Pérdida del suministro eléctrico	X		
Pérdida de disponibilidad de servidor físico	X		
Pérdida de disponibilidad de las máquinas virtuales	X		
Indisponibilidad del personal encargado del centro de datos		X	
Pérdida de disponibilidad del servicio de internet		X	
Pérdida del servicio de correo electrónico		X	
Caída del servidor de base de datos			X
Corrupción de información critica			X
Caída en el servicio de red			X

Oficina General de Tecnologías de la Información V°B° W. Carcheri G. Jefe

8. MANTENIMIENTO DEL PLAN

El responsable del mantenimiento del plan es el Oficial de Seguridad de la Información. El plan debe ser revisado, probado y actualizado en su documentación y su alcance, esto quiere decir que el plan debe tener revisiones de acuerdo a los siguientes parámetros:

- Implementación de nuevos activos críticos de TI.
- Resultados de una nueva evaluación de riesgos.
- Requisitos legales o contractuales.

Revisión como parte del sistema de gestión por lo menos 1 vez al año.

9. CONTACTOS

9.1. INTEGRANTES DE MIDIS EN CASO DE CONTINGENCIAS O DESASTRES

N°	NOMBRE APELLIDOS	TELÉFONOS		
		OFICINA	CELULAR	DOMICILIO
1.	William Carcheri Girón	OGTI	966991537	-
2.	Maurice Frayssinet Delgado	OGTI	980997203	-
3.	William García Jacobo	OGTI	952285817	-
4.	Julio Cerna Arbayza	OGTI	972032593	-
5.	Carlos Farro Vallejo	OGTI	977271029	-

9.2. PROVEEDORES DE TECNOLOGÍA DE LA INFORMACIÓN (Servicios Críticos)

RECURSO	PROVEEDOR	PERSONA DE CONTACTO	MEDIO DE COMUNICACIÓN
PROVEEDOR DE RECURSOS			
ENLACE DE DATOS	Claro Empresa	Mesa de ayuda Claro	0800 00 800
ENLACE RENIEC	Optical Networks	Soporte Optical	5003400 / 7554
SERVICIO DE CUSTODIA DE CINTA	RANSA	Servicio al Cliente	201-8200
-SOPORTE A10 -SOPORTE ANTIMALWARE -SOPORTE DDOS -SOPORTE EQUIPO VULNERABILIDAD	Desysweb	Soporte Desysweb	630 8080
-SOPORTE ANTISPAM -SOPORTE FIREWALL CHECKPOINT -SOPORTE PROXY	Electrodata	Soporte Electrodata	4760808 / 4760401
SOPORTE CENTRO DE DATOS Y SWITCH	EBDPERU	Soporte EBD	soporte@ebdperu.com
SOPORTE DELL	DELL	Soporte DELL	0800 50 869
SOPORTE WAF	SISCOTEC	Soporte Técnico	226-5883
INTERNET	Telefónica del Perú	Mesa de ayuda Movistar	595 0104
SUMINISTRO DE ENERGÍA ELECTRICA	LUZ DEL SUR	FONOLUZ	617-5000

Oficina General de Tecnologías de la Información
V°B°
W. Carcheri G.
Jefe