Resolución Directoral

N° 03-2024-VIVIENDA/OGEI

Lima, 14 de febrero del 2024

VISTO:

El informe N.º 16-2024/OGEI-GFERNANDEZ del Oficial de Seguridad de la Información;

CONSIDERANDO:

Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

Que, el artículo 55 del Reglamento de Organización y Funciones - ROF del Ministerio de Vivienda, Construcción y Saneamiento MVCS, establece que la Oficina General de Estadística e Informática - OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como planificar, desarrollar, implementar y gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, con Resolución Directoral N° 022-2022-INACAL/DN, se aprueba la NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición, el cual reemplaza a la NTP-ISO/IEC 27001:2014;

Que, la referida Norma Técnica Peruana NTP-ISO/IEC 27001 señala en el Anexo A.5.30 Preparación de las TIC para la continuidad del negocio. Control. La preparación de las TIC debe planificarse, implementarse, mantenerse y aprobarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC;

Que, en este marco normativo la Oficina de Tecnologías de la Información propone la aprobación del Plan de Contingencia de la Oficina General de Estadística e Informática;

Que, con Resolución Ministerial Nº 356-2018-VIVIENDA, del 23 de octubre de 2018 se constituyó el Comité de Gobierno Digital en el marco de la Resolución Ministerial N° 119-2018-PCM, entre cuyas funciones destaca la de liderar y dirigir el proceso de transformación digital en la entidad;

Que, mediante el informe N° 16-2024/OGEI-GFERNANDEZ el Oficial de Seguridad de la Información comunica que respecto a las materias de su competencia se ha emitido opinión favorable respecto a la aprobación del citado Plan;

Resolución Directoral

Que, estando a lo expuesto y conforme a la propuesta remitida por el Oficial de Seguridad de la Información, contando con la opinión favorable de la Oficina de Tecnologías de la Información, corresponde expedir la presente Resolución aprobando el Plan de Contingencia de la Oficina General de Estadística e Informática, según lo expresado en los documentos de visto;

SE RESUELVE:

Artículo 1.- Aprobar el Plan de Contingencia de la Oficina General de Estadística e Informática para el 2024, el mismo que forma parte integrante de la presente Resolución.

Artículo 2- - Dejar sin efecto la Resolución Directoral N° 004-2023-VIVIENDA/OGEI, que aprueba el Plan de Contingencia de la Oficina General de Estadística e Informática 2023.

Artículo 3.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento.

Regístrese y comuníquese

FIRMA DIGITAL
Firmado digitalmente por: SUCA ANCACHI Helmer Efrain FAU 20504743307 hard
Motivo: Soy el autor del documento
Fecha: 2024/02/14 11:57:00-0500

Ing. HELMER EFRAIN SUCA ANCACHI
Director General
Oficina General de Estadística e Informática

PERÚ | Ministerio de Vivienda, Construcción y Saneamiento | Secretaría General | Oficina General de Estadística e Informática

PLAN DE CONTINGENCIA

OFICINA GENERAL DE ESTADÍSTICA E INFORMÁTICA

Año 2024

HOJA DE CONTROL DE DOCUMENTO

DOCUMENTO / ARCHIVO

Título	Plan de Contingencia de OGEI
Fecha	07.02.2024
Versión	2024
Localización	Ministerio de Vivienda, Construcción y Saneamiento (MVCS)

REGISTRO DE CAMBIOS

Versión	Páginas	Fecha Modificación	Motivo del cambio
2018	77	08.03.2018	Actualización del documento
2019	47	30.04.2021	Actualización del documento
2022	56	23.09.2022	Actualización del documento
2023	56	17.01.2023	Actualización del documento

CONTROL DEL DOCUMENTO

ROL	NOMBRE	CARGO	VISTO
Elaborado por:	Guillermo Fernández Namuche	Especialista en Seguridad de la Información	FIRMA DIGITAL Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2024/02/07 13:10:04-0500
Revisado por:	Kenny Rodríguez Cáceres	Coordinador de Infraestructura Tecnológico	FIRMA DIGITAL Firmado digitalmente por:RODRIGUEZ CACERES Kenny Mirko FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2024/02/07 14:02:51-0500
	Maria Isabel Vasquez Aldame	Directora de la Oficina de Tecnologías de la Información	FIRMA DIGITAL Firmado digitalmente por:VASQUEZ ALDAVE Maria Isabel FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2024/02/13 14:31:52-0500
Aprobado por:	Helmer Suca Ancachi	Director General de la Oficina General de Estadística e Informática	FIRMA DIGITAL Firmado digitalmente por:SUCA ANCACHI Helmer Efrain FAU 20504743307 hard Motivo: En señal de conformidad Fecha: 2024/02/13 14:54:19-0500

ÍNDICE DE CONTENIDO

RESUMEN EJECUTIVO

El presente documento denominado Plan de Contingencia de la Oficina General de Estadística e Informática (OGEI), tiene como objetivo recuperar y restablecer los procesos críticos de los sistemas informáticos de OGEI dentro de un tiempo predeterminado luego de ocurrida alguna emergencia o interrupción excepcional de dichos sistemas.

Los objetivos y el alcance de este plan guardan relación con la infraestructura informática, así como los procedimientos relevantes asociados con la plataforma tecnológica implementada.

La infraestructura informática está conformada por hardware, software y elementos complementarios que soportan la información o datos críticos para la continuidad del servicio del Ministerio.

INTRODUCCIÓN

El Plan de Contingencia de OGEI, es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las Comunicaciones que tiene como fin, garantizar la continuidad de los servicios de TI.

El Ministerio de Vivienda, Construcción y Saneamiento (MVCS), para asegurar el cumplimiento de su misión, se apoya en los procesos de tecnología con el fin de asegurar que los servicios brindados tanto a sus colaboradores como ciudadanos y demás partes interesadas, se den con la eficiencia que se requiere; así mismo, para que los productos que generan, con la oportunidad y calidad planificadas.

El presente documento, establece roles y responsabilidades para la operación del Plan de Contingencias de OGEI, presenta la identificación de los riesgos y los responsables de su administración, contiene el inventario de activos de Tecnología de la Información (TI), sobre los cuales se deben realizar las actividades prioritarias en caso de presentarse un evento que pongan en riesgo la continuidad de la operación y la prestación de los servicios de TI.

El plan aplica las actividades necesarias para mantener en operatividad los sistemas de información del MVCS, para lo cual, establece los aspectos técnicos, humanos y de logística, que permitan afrontar cualquier contingencia.

De igual forma, el Plan de Contingencias de OGEI define las pruebas a realizar con el objetivo de reducir la probabilidad de riesgos a un nivel aceptable, tanto para el hardware como del software y la adecuada recuperación de la información.

El Plan de Contingencia de OGEI, se encuentra diseñado en el marco de la Norma Técnica Peruana ISO 27001 y Norma Técnica Peruana ISO 31000, además de la Política de Seguridad de la Información del MVCS; en consecuencia, se toman las provisiones necesarias para modificar los procedimientos establecidos en el presente plan.

1. OBJETIVOS

1.1. Objetivos Generales

Definir el conjunto de actividades, roles y responsabilidades que permitan el restablecimiento de la operación normal de la plataforma tecnológica de la entidad, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI, que pueda alterar el normal funcionamiento de los sistemas de información críticos de la entidad, buscando la mejor calidad en los servicios que brinda la Oficina General de Estadística e Informática del MVCS, a los colaboradores como a los ciudadanos.

Recuperar y restaurar los procesos críticos de la OGEI parcial o totalmente interrumpidos dentro de un tiempo predeterminado después de una interrupción no deseada o desastre, mediante mecanismos apropiados que deben validarse mediante un cronograma de pruebas luego de su implementación.

1.2. Objetivos Específicos

1.2.1 Restablecer con la mayor brevedad posible el funcionamiento de la infraestructura tecnológica cuando ocurra un evento, en aras de minimizar el impacto y garantizar la correcta recuperación de los sistemas y procesos del Ministerio que involucren la Infraestructura de TI.

1.2.2 Continuar brindando los servicios informáticos en las diferentes Oficinas del MVCS que se hayan visto afectadas por una situación adversa.

1.2.3 Optimizar los recursos necesarios para atender cualquier contingencia de TI, de manera oportuna y eficiente, definiendo a las personas responsables de las actividades a desarrollar antes, durante y después de la emergencia.

1.2.4 Definir actividades y procedimientos a ejecutar en caso de una interrupción de las operaciones de los sistemas y/o procesos que involucren la infraestructura de TI del MVCS, a fin de garantizar la continuidad en la ejecución de los objetivos estratégicos de la entidad en el menor tiempo posible.

1.2.5 El presente Plan de Contingencia de OGEI para el año 2023, tendrá vigencia hasta la generación del plan de contingencia del año siguiente, salvo disposición de la autoridad superior.

2. BASE LEGAL

2.1.1 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.

2.1.2 Ley Nº 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.

2.1.3 Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastre (SINAGERD).

2.1.4 Decreto Supremo N° 038-2021-PCM que aprueba la Política Nacional de Gestión del Riesgo de Desastre al 2050.

2.1.5 Resolución Ministerial N° 248-2022, que aprueba la actualización del Plan de Continuidad Operativa del Ministerio de Vivienda, Construcción y Saneamiento.

2.1.6 Norma Técnica Peruana “NTP-ISO/IEC 27001:2022 EDI. señala en el Anexo A. 5.30 Preparación de las TIC para la continuidad del negocio. “Control”: La preparación de las TIC debe planificarse, implementarse, mantenerse y

probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

2.1.7 Norma Técnica Peruana "NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición.

2.1.8 Norma Técnica Peruana "NTP-ISO/IEC 31000:2018. proporciona los principios y las directrices genéricas sobre la Gestión de Riesgo.

2.1.9 Norma Técnica Peruana "NTP-ISO/IEC 22301:2020, seguridad y resiliencia. Sistemas de gestión de Continuidad del Negocio".

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

3. ALCANCE

El Plan de Contingencia de OGEI, descrito en este documento define los roles y responsabilidades, así como, las actividades para tomar control frente a situaciones que puedan afectar la continuidad de las operaciones, delimitado en la protección y funcionalidad de los sistemas considerados como críticos y plataformas tecnológicas que soportan los procesos misionales del Ministerio.

El Plan de Contingencia de OGEI, aplica y da cubrimiento al Centro de Datos de la sede principal ubicada en la Av. República de Panamá Nº 3650 - San Isidro, cuarto piso, a sus equipos informáticos y de comunicaciones instalados que se encuentran bajo la responsabilidad de la OGEI.

4. METODOLOGÍA

Si bien los planes de contingencia de tecnologías de la información se realizan a fin de prevenir fallas o accidentes en las operaciones de una entidad, para la elaboración de los mismos es importante tener en cuenta el estado de la infraestructura informática y de los servicios informáticos de la Institución, por lo que los planes de cada Institución son muy propios.

En ese sentido, el desarrollo del Plan se basa en las siguientes seis (6) fases:

Fase 1: Planificación
Fase 2: Determinación de Vulnerabilidades
Fase 3: Estrategias del Plan de Contingencia
Fase 4: Elaboración del Plan de Contingencia
Fase 5: Implementación del Plan de Contingencia
Fase 6: Monitoreo

A continuación, se detalla cada fase:

4.1 FASE 1: PLANIFICACIÓN

4.1.1 Organización

El compromiso de la Oficina General de Estadística e Informática, de la Oficina de Tecnología de la Información y los integrantes del área de Tecnología, es fundamental debido a que son ellos quienes tienen la responsabilidad de responder de forma adecuada ante un incidente inesperado en la operación de la entidad y el desarrollo del trabajo, desde el momento que se declare la interrupción hasta la vuelta a la normalidad, (prevención, mitigación, preparación, alertas, respuestas, rehabilitación y reconstrucción) de forma que se reduzca al mínimo el impacto sobre la prestación del servicio.

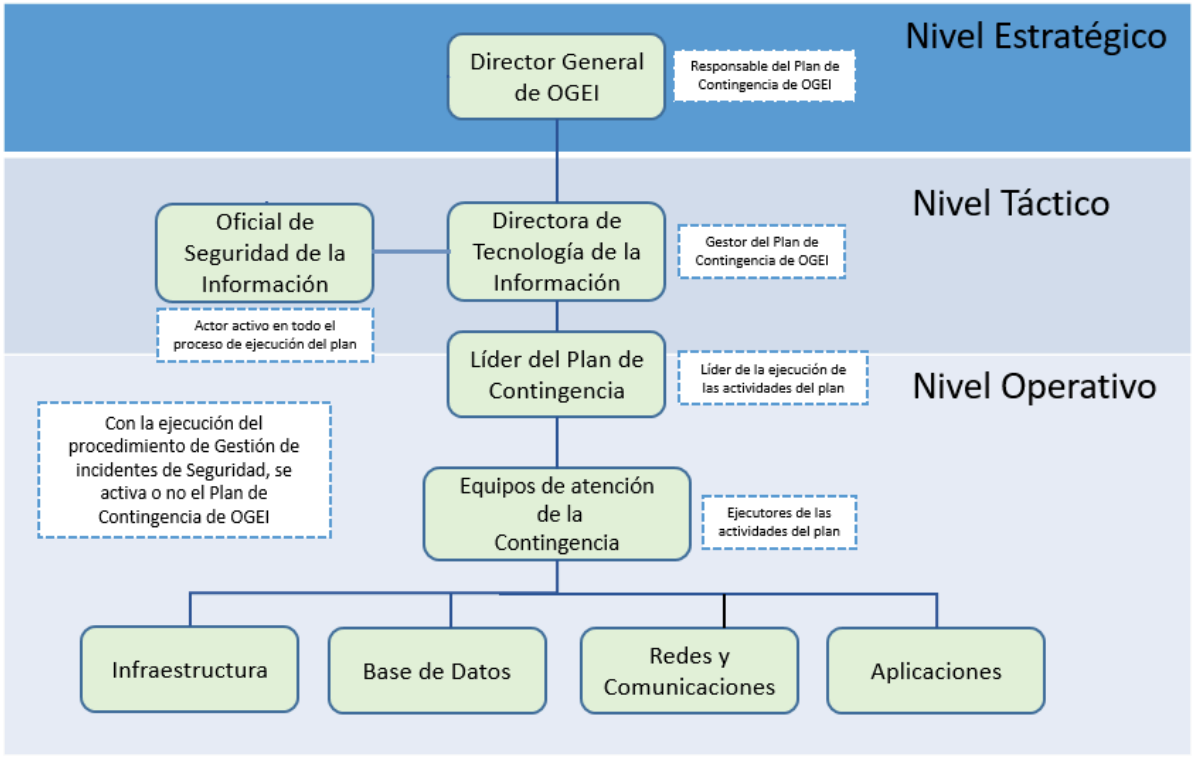
A continuación, se definen los tres niveles de gestión (estratégico, táctico y operativo) y sus responsabilidades durante una situación de contingencia de TI. El siguiente cuadro muestra las funciones y roles separando los deberes para que las tareas y áreas de responsabilidad no presenten conflicto alguno; en cada nivel se debe establecer un plan de sucesión para que en caso de no estar disponible el funcionario principal, pueda actuar su reemplazo con la misma autoridad y responsabilidad:

Nivel Estratégico: Este nivel corresponde básicamente a la planeación del logro de los objetivos del Plan de Contingencias de OGEI, se basa en decidir las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción no planeada en la entidad.

Nivel Táctico: Llevará a cabo la coordinación de las actividades que se deriven del Plan de Contingencias de OGEI, así como, la evaluación de las situaciones de interrupción y dará lineamientos para la operación de los mismos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación y brindará los insumos para la evaluación.

Nivel Operativo: Este nivel realiza la asignación de las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el Plan de Contingencias de OGEI. Se ejecuta a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

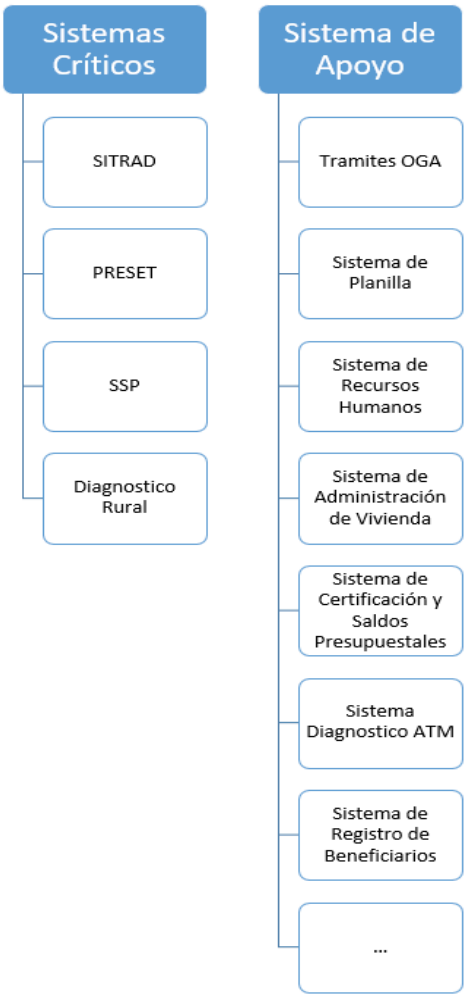
Figura 1
Organigrama de la organización del plan de contingencia de Tecnologías de la Información



4.1.2 Sistema de Información

Actualmente, los procesos se apoyan en los sistemas de información diseñados a la medida, así como en sistemas de información cedidos por medio de convenios de transferencia tecnológica por otras entidades y a los cuales el MVCS realiza las adecuaciones que considera para ajustarlo a su dinámica funcional.

Figura 2: Sistema de información del MVCS



Asimismo, la entidad cuenta con sistemas de información adquiridos a terceros y otros desarrollados internamente de acuerdo a las necesidades de los usuarios. Se cuenta con mantenimiento especialmente para los sistemas críticos, y para los demás el soporte es brindado directamente con colaboradores de la OGEI.

4.1.3 Servicios Tecnológicos

Los servicios tecnológicos que brinda la Oficina General de Estadística e Informática a través de la Oficina de Tecnología de la Información, están soportados por servidores virtualizados, los cuales están diseñados para mantener un correcto funcionamiento de la plataforma tecnológica de la entidad. Así mismo, permiten brindar una respuesta oportuna a las diferentes eventualidades que en materia de tecnologías de la información puedan afectar el funcionamiento apropiado de la red de datos, equipos tecnológicos, red de comunicaciones, entre otros servicios asociados.

Tabla 1: Descripción de los catálogos de servicios tecnológicos del MVCS

Servicio	Descripción	Alcance y Funcionalidad	Importancia para el MVCS
Impresión y digitalización	Dentro de la garantía de las máquinas comprende el mantenimiento preventivo, correctivo y garantía a las impresoras.	Este servicio va dirigido a todos los usuarios del MVCS.	Por la cobertura dentro de la entidad y complejidad que maneja en las áreas se cataloga como **ALTO**.
Conectividad WI-FI	Brindar conectividad inalámbrica a todas las oficinas del MVCS que lo necesite, facilitando el trabajo y el uso de equipos portátiles asignados por la Oficina General de Estadística e Informática a través de Oficina de Tecnologías de la Información.	Este servicio es para la sede principal, para los usuarios que realizan trabajos de despliegue en cada uno de los pisos y poder llevar a cabo su labor.	El servicio de conectividad inalámbrica para el MVCS ha sido una herramienta que se ha vuelto indispensable para funcionarios que no cuentan con cableado de red en las oficinas.
Telefonía móvil, Telefonía y Cableado Estructurado	Entrega de equipos móviles a colaboradores que lo soliciten, mantenimiento preventivo y correctivo de la Central Telefónica. Realizar cableado estructurado a las oficinas que lo requieran.	Este servicio va dirigido a todos los usuarios del MVCS.	Funcionalidad de las comunicaciones en voz y datos en las instalaciones del MVCS.
Sistema de Directorio Activo (AD)	Crea objetos como usuarios, equipos o grupos para administrar las credenciales durante el inicio de sesión de los equipos que se conectan a la red del MVCS.	Este servicio va dirigido a todos los usuarios del MVCS.	Administrar las políticas de absolutamente toda la red en la que se encuentre este servidor. Esto implica, por ejemplo, la gestión de permisos de acceso de usuarios, bandejas de correo personalizadas, etc.
Equipo de Cómputo	Comprende el mantenimiento preventivo y correctivo de los equipos de cómputo del MVCS.	Este servicio de soporte va dirigido a todos los equipos de cómputo del MVCS.	Funcionalidad del sistema operativo y demás aplicaciones instaladas en los equipos de cómputo del MVCS.
Ofimática	Conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en el MVCS para optimizar, automatizar, y mejorar los procedimientos o tareas.	Este servicio de soporte va dirigido a todos los equipos de cómputo del MVCS.	Funcionalidad de herramientas informáticas y demás aplicaciones instaladas en los equipos de cómputo del MVCS.
Recursos Audiovisuales (proyector y laptop)	Servicios de instalación y configuración de equipos de audio y video en las salas de reuniones del MVCS. Adicional se tiene un control de reservas y acompañamiento.	Este servicio de soporte va dirigido a la configuración de equipos de audio y video en la sala de reuniones del MVCS o donde se requiera.	Funcionalidad de herramientas informáticas y demás aplicaciones instaladas en los equipos de cómputo del MVCS.

Correo electrónico	Se refiere a los servicios asociados a la cuenta de correo electrónico, tales como creación y configuración de cuentas de correo, sincronización, backup, modificación y eliminación de listas de distribución, compartir contactos y calendario.	Este servicio de soporte va dirigido a la creación y configuración de usuarios que estén previamente aprobados por la OGEI.	El servicio de correo electrónico se brinda para los funcionarios CAS y Órdenes de Servicios que trabajan en el MVCS.
Servidores	Hace referencia a la administración, configuración y disponibilidad de los servidores del MVCS.	Este servicio de soporte va dirigido a los servidores que están instalados en el Centro de Datos, el cual está ubicado en el piso 4 de la sede principal del MVCS.	Dirigido para la continuidad y administración de las aplicaciones que están instaladas en estos servidores del MVCS.
Bases de Datos	Servicio para la creación, respaldo, restauración de las Bases de Datos que interactúan con las aplicaciones misionales del MVCS.	Este servicio de soporte va dirigido a las Bases de Datos de SQL Server, la cual están en los servidores que están en el Data center del MVCS.	El Servicio de las Bases de Datos es la que da la continuidad y el funcionamiento de las Aplicaciones Misionales que tiene el MVCS.
Centro de Datos	Este servicio incluye servicios de apoyo logístico, instalación de componentes, monitoreo, backups, mantenimientos.	El Centro de Datos es donde se encuentran los servidores de las aplicaciones que maneja el Ministerio, también está el Switch Core, el aire acondicionado y el sistema contra incendios.	El Centro de Datos debe estar en óptimas condiciones en cuanto al sistema eléctrico y aire acondicionado, ya que si estos dos factores no están funcionando se verán afectados los servidores.
Seguridad Informática	Actividades orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información y la plataforma tecnológica del Ministerio y sus servicios asociados.	La seguridad informática está diseñada por medio del firewall de marca Palo Alto y las políticas del Directorio Activo para usuarios, administradores y usuarios finales.	Por medio de este servicio se controla y garantiza el servicio de Internet, y el óptimo funcionamiento de las aplicaciones WEB que tiene la entidad.
Portales	Servicios asociados con los sitios WEB desarrollados y mantenidos por la OGEI con el propósito de divulgar información y ofrecer servicios de interés general para los colaboradores de la entidad o para los ciudadanos.	Está constituido por las Páginas Webs e intranet donde se ofrecen los diferentes servicios para usuarios y ciudadanos.	Por medio de este servicio se realizan publicaciones de las diferentes actividades que se realizan en el MVCS.
Internet	Administración de la disponibilidad de los servicios de Internet.	El servicio es utilizado por la Sede Principal y por las sedes de LAN extendida (Miraflores, Panamá 2, Callao y Vitrina Inmobiliaria).	Este servicio es importante para la funcionalidad de las aplicaciones Web, correo electrónico y demás actividades que realiza el MVCS con otras entidades del estado.

Gestión de Usuarios	Servicio para la creación, modificación, eliminación de usuarios y licencias.	El servicio hace referencia a las solicitudes que realizan los funcionarios para la asignación de usuarios o accesos a las aplicaciones que tiene la Entidad.	Es importante para que los funcionarios puedan ingresar a las aplicaciones y realizar las diferentes actividades que se realizan en la Entidad.

4.1.4 Infraestructura a nivel nacional

Para soportar los servicios tecnológicos que se entregan a los procesos del MVCS, tiene establecida una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos.

Adicionalmente, el MVCS cuenta con un Centro de Datos propio ubicado en las instalaciones de la sede principal del MVCS ubicada en la Av. República de Panamá Nº 3650 - San Isidro, cuarto piso y cuatro (4) sedes externas: Miraflores, San Isidro, Callao, Vitrina Inmobiliaria. Además, se cuenta con 24 Centros de Atención al Ciudadano - CAC.

Tabla 2: Ubicación de Centros de Datos y CAC

DIRECCIÓN	ELEMENTOS	CONTACTO
Local Central **Av. República de Panamá Nº 3650 - 3660 - 3664 - 3666**	Centro de Datos, equipos de cómputo, impresoras y gabinete de redes.	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234
Local Miraflores **Av. Alfredo Benavides 391 - 395 Miraflores**	Equipos de cómputo, impresoras y gabinete de redes.	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234
Local Callao **Almacén y Archivo Central** **Av. Elmer Faucett Cdra. 39 s/n. - Callao** **(Frente al Grupo Aéreo N° 8)**	Equipos de cómputo, impresoras y gabinete de redes.	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234
Local Vitrina Inmobiliaria **Jirón Camaná 199 esquina Conde Superunda- Cercado de Lima**	Equipos de cómputo, impresoras y gabinete de redes.	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234
CENTRO DE ATENCIÓN AL CIUDADANO - CAC		
CAC AMAZONAS **Jr. Ayacucho Nº 1151-1153 Chachapoyas**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 041-477001
CAC ANCASH **Jr. Esteban Castromonte N° 399 con Av. Confraternidad Internacional Este – Urb. Pedregal Medio - Huaraz**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 043-234094

CAC APURIMAC **Av. El Arco Nº 110 – Distrito Tamburco - Abancay**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 083-322031
CAC AREQUIPA **Calle República de Chile Nº 329, Urb. La Negrita, Distrito Cercado de Arequipa**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 054-315694
CAC AYACUCHO **Jr. Garcilaso de la Vega Nº 797, Urb. Banco de la Nación Mz. C. Lt. 13**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 066-314746
CAC CAJAMARCA **Jr. Baños del Inca Nº 114, 116, Urb. Ramón Castilla**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 076-770362
CAC CUSCO **Av. Huayruropata Nº 1609 – 1611, Dist. Wanchaq**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 084-223759
CAC HUANCAVELICA **Jr. Mayta Cápac Nº 101, Barrio San Cristóbal – Hvca / Esq. Con Malecón Virgen de la Candelaria**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 067-780064
CAC HUÁNUCO **Jirón Progreso Nº 320 Huánuco - Huánuco**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 062-282244
CAC ICA **Calle Los Nardos Nº 185 Urb. San Isidro - Ica**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 056-387390
CAC JUNÍN **Psje. José María Arguedas Nº 220, El Tambo, Huancayo**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 064-397530
CAC LA LIBERTAD **Jr. Diego de Almagro Nº 560 - Centro Histórico de Trujillo**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 044-228167
CAC LAMBAYEQUE **Calle Los Gladiolos Nº 398, Urb. Los Parques - Chiclayo**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 074-276564
CAC LIMA **Av. Alfredo Benavides Nº 395 (Mezanine 3) – Distrito Miraflores**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 01-2117930 6110-6111
CAC LORETO **Jirón Moore Nº 1550 – Iquitos**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 065-264789
CAC MADRE DE DIOS **Av. Fitzcarrald Nº 418 – Puerto Maldonado - Tambopata**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 082-350056
CAC MOQUEGUA **Av. Bolívar Nº 390, Mz. D Lt. 29,**	Equipos de cómputo, impresoras y router del	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234

Urb. Santa Catalina	proveedor de servicio	Oficina: 053-479102
CAC PASCO **Av. Carlos Salaverry Nº 906, San Juan Pampa, Yanacancha**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 063-280633
CAC PIURA **Av. Los Cocos N° 259, Urb. Club Grau Mz. C Lote 4**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 073-251945
CAC PUNO **Jr. Lampa N° 135 - Cercado**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 051-205001
CAC SAN MARTÏN **Jr. Oscar R. Benavides N° 329, Moyobamba**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 042-351034
CAC TACNA **Calle César Faucheaux, Mz. A Lt. 2**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 052-283296
CAC TUMBES **Calle Bolívar N° 912, Cercado de Tumbes**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 072-781797
CAC UCAYALI **Jr. Raymondi N° 386 – 394, Pucallpa**	Equipos de cómputo, impresoras y router del proveedor de servicio	mesadeservicios@vivienda.gob.pe, 2117930 - anexo 1234 Oficina: 061-281611

- Topología de red del MVCS – Interconexión sedes - anexo 5
- Diagrama de la topología de la red del MVCS - Infraestructura sede principal, anexo 6

4.1.5 Infraestructura del Centro de Datos Sede Principal

Para soportar los servicios tecnológicos que se entregan a los procesos del MVCS, se tiene establecida una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos.

Tabla 3: Infraestructura del centro de datos sede principal

CANTIDAD	DESCRIPCIÓN
7	Servidores DELL
3	Servidores HP
6	Servidores Lenovo
106	Servidores virtuales
2	Switch Core

2	UPS MODELO (GXT3-1000RT230, DELTA1100A, HP9116C10-KR-XL, URT-2K)
2	Storage
1	KVM
1	Sistema de aire acondicionado de precisión
1	Sistema de detección y extinción de incendios
2	Firewall Palo Alto

4.1.6 Acuerdos de Niveles de Servicios de Tecnologías

La Oficina General de Estadística e Informática a través de la Oficina de Tecnología de la Información ha considerado los Acuerdos de Niveles de Servicio (ANS) para la prestación de estos servicios, los cuales son definidos teniendo en cuenta el nivel de complejidad y la afectación que causa sobre la infraestructura tecnológica.

Tabla 4: Acuerdos de niveles de servicios del catálogo de servicios tecnológicos del MVCS

Servicio	Canales de Acceso	Disponibilidad de |Horarios	Horario de Soporte	Horario de uso	Requisitos para Acceder al Servicio
Impresión y digitalización	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	L a V de 8:30 am a 5:15 pm	8 x 5, los días hábiles del año.	Acceso a la red
Conectividad Wifi	Access Point	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Solicitar el servicio para hacer la habilitación respectiva del dispositivo a conectar
Telefonía y Cableado Estructurado	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Tener usuario válido para poder acceder a los equipos de cómputo
Equipo de Cómputo	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	8 x 5, los días hábiles del año	L a V de 8:30 am a 5:15 pm	8 x 5, los días hábiles del año	Tener usuario válido para poder acceder a los equipos de cómputo
Ofimática	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	8 x 5, los días hábiles del año	L a V de 8:30 am a 5:15 pm	8 x 5, los días hábiles del año	Tener usuario válido para poder acceder a los equipos de

					cómputo
Recursos Audiovisuales	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	8 x 5, los días hábiles del año	L a V de 8:30 am a 5:15 pm	8 x 5, los días hábiles del año	Tener una reserva previa para la sala de reuniones
Correo electrónico	Los usuarios acceden al servicio por web o en equipos móviles en caso de tenerlo configurado.	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Tener acceso a Internet
Servidores	Estar autorizado y tener acceso al Centro de Datos	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Tener aplicaciones en los servidores que están en el Centro de Datos del piso 4 del MVCS.
Bases de Datos	Estar autorizado y tener acceso al Centro de Datos	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Tener aplicaciones que interactúen con las Bases de Datos que están en los servidores del Centro de Datos del MVCS.
Centro de Datos	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	L a V de 8:30 am a 5:15 pm	L a V de 7:00 am a 5:00 pm	Estar autorizado para el ingreso.
Seguridad Informática	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	L a V de 8:30 am a 5:15 pm	L a V de 7:00 am a 5:00 pm	Realizar la solicitud por la Mesa de Servicios
Portales	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	24x7x365	24x7x365	Realizar la solicitud por la Mesa de Servicios
Internet	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	24x7x365	L a V de 8:30 am a 5:15 pm	24x7x365	Realizar la solicitud por la Mesa de Servicios
Gestión de Usuarios	Mesa de Servicios ● mesadeservicios @vivienda.gob.pe ● anexo 1234	L a V de 7:00 am a 5:00 pm	L a V de 8:30 am a 5:15 pm	L a V de 7:00 am a 5:00 pm	Realizar la solicitud por la Mesa de Servicios
Copias de respaldo	Solo para el personal de OGEI y por solicitud, el personal autorizado de la OGEI realiza copias de	Por cronograma definido y por demanda	Por cronograma definido y por demanda	Por cronograma definido y por demanda	Solicitud de acceso a servicios vía formulario de mesa de servicio Plan de respaldo y resguardo de datos

	seguridad según cronograma.				

4.1.7 Roles, funciones y responsabilidades dentro del Plan de Contingencia

Tabla 5: Roles y responsabilidades definidas para el Plan de Contingencia de OGEI

Roles	Antes de la interrupción	Durante la interrupción	Después de la interrupción
Director/a General de OGEI	Aprobar el Plan de Contingencia de OGEI.	Permanecer atento al desarrollo del Plan de Contingencias de OGEI.	Informar resultados de la ejecución del Plan de Contingencia de OGEI a la Alta Dirección.
Director/a de OTI	Es el canal de comunicación para la gestión del plan.	Monitorea y asegura el cumplimiento del Plan de Contingencia de OGEI.	Analiza la interrupción y participa en la toma de decisiones, dependiendo de la criticidad y afectación. Propone revisiones del Plan de Contingencia de OGEI.
	Apoyar en la toma de decisión sobre la activación del Plan de Contingencias de OGEI.	Gestionar las actividades del Plan de Contingencia de OGEI, asignando a los funcionarios de acuerdo con los perfiles de administración de hardware y software.	Programar y coordinar las pruebas del retorno a la normalidad luego que haya terminado la contingencia.
	Coordinar actividades de documentación y actualización del Plan de Contingencias de OGEI.	Mantener comunicación constante con los integrantes de los niveles estratégico y táctico sobre las actividades realizadas durante la interrupción.	Informar al Director General sobre las actividades realizadas durante y después de la interrupción.
	Asegurar que los cambios presentados se actualicen en el Plan de Contingencia de OGEI.	Realizar seguimiento a la situación durante la activación del Plan de Contingencias de OGEI.	
		Proveer soporte a los líderes y equipos de recuperación.	
	Identificar y gestionar los recursos requeridos para la operación del Plan de Contingencias de TI.	Planificar y gestionar el retorno a la normalidad.	
Oficial de Seguridad de la Información	Analizar los eventos de seguridad registrados y participar con los demás miembros del nivel estratégico y táctico, en la toma de decisión de activar o no el Plan de Contingencia de OGEI.	Permanece en comunicación activa con el Líder del Plan de Contingencias de OGEI.	Analiza las causas de la interrupción y los resultados de la ejecución del plan e informa el análisis realizado a los niveles estratégico y táctico.
	Identificar riesgos de	Participar activamente en la	Actualizar el Plan de Contingencia

	interrupción de los servicios de TI y emitir concepto para toma de decisiones	ejecución del plan.	de OGEI.
Líder del Plan de Contingencia de OGEI **Director/a de OTI**	Apoya en la toma de decisión sobre la activación del Plan de Contingencias de OGEI.	Liderar las actividades de recuperación de los servicios de TI afectados sobre equipos de infraestructura y aplicaciones.	Apoyar la actualización del Plan de Contingencias de OGEI.
	Comunicar al nivel operativo de las actividades a realizar en caso de presentarse la interrupción.	Mantener informado a nivel estratégico, sobre las actividades de ejecución del Plan de Contingencia de OGEI.	Coordinar y realizar las pruebas del retorno a la normalidad luego que haya terminado el Plan de Contingencia de OGEI.
	Coordinar y participar activamente en la ejecución de las pruebas del Plan de Contingencias de OGEI.	Ejecutar junto con los administradores de infraestructura y aplicaciones las labores de recuperación.	Informar al nivel estratégico sobre las actividades realizadas durante el evento.
		Coordinar la logística para el desarrollo de las actividades de recuperación tales como traslados de los equipos de recuperación, entre otros.	
		Informar al nivel estratégico, los recursos a adquirir necesarios de materiales, equipos, consumibles durante la recuperación.	
Equipos de atención de la Contingencia: ● **Coordinador/a de Infraestructura y Aplicaciones** ● **Coordinador/a de Desarrollo Tecnológico** ● **Administrador/a de Bases de Datos** ● **Administrador/a de servicios de redes y comunicaciones**	Realizar de forma periódica las actividades de instalación y arranque de la infraestructura de TI y la infraestructura de recuperación.	Ejecutar las actividades registradas en el Plan de Contingencias de OGEI y las que considere necesarias para la recuperación de la infraestructura, servicio y/o aplicación afectada.	Restaurar a la normalidad la infraestructura, servicios y/o aplicaciones afectadas para su puesta en producción nuevamente.
	Aplicar los procedimientos del proceso de Gestión de Tecnología de la Información.	Proveer soporte técnico según requerimientos del momento.	Documentar las lecciones aprendidas del evento de interrupción.
	Mantener (en el caso que aplique) iguales las configuraciones de los equipos de producción y de respaldo, así como de los sistemas de información y bases de datos de producción y de respaldo.	Ejecutar las actividades registradas en el Plan de Contingencia de OGEI y las que considere necesarias para la recuperación del equipo de la plataforma o del activo de información afectado.	Restaurar a la normalidad el equipo de la plataforma o el activo de información afectado para usarlo nuevamente.
	Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.	Asegurar la prestación del servicio en el menor tiempo posible, luego de la activación del Plan de Contingencia de OGEI.	Tomar medidas correctivas frente a lo ocurrido en la activación del Plan de Contingencia de OGEI para la recuperación de las actividades durante el evento.

• **Administrador/ a de Sistemas y Servidores** • **Soporte Técnico**	Ejecutar las pruebas del Plan de Contingencia de OGEI.		Revisar los informes de incidencias y consecuencias y elaborar el plan de remediación de las mismas.
	Identificar riesgos de interrupción de los servicios de TI y emitir conceptos para toma de decisiones.		Reportar los inconvenientes y oportunidades de mejora del Plan de Contingencia de OGEI.
	Participar en las actividades de continuidad (capacitaciones, divulgación, pruebas y ejecución).		
Equipo de Apoyo Logístico: • **Profesionales de las diferentes áreas que se requieran para la ejecución del Plan de Contingencia de OGEI.**	Conocer el Plan de Contingencias de OGEI.	Ejecutar actividades de logística para el desarrollo de las actividades de recuperación tales como traslados del personal y equipo de recuperación.	Reportar los inconvenientes y oportunidades de mejora del Plan de Contingencia de OGEI.
		Realizar actividades relacionadas con compras necesarias de materiales, equipos, consumibles durante la recuperación.	

4.2 FASE 2: DETERMINACIÓN DE VULNERABILIDADES

4.2.1 Identificación de riesgos

Para el Plan de Contingencias de la OGEI del MVCS se tienen en cuenta los riesgos tecnológicos identificados dentro del análisis de riesgos de seguridad de la información.

La metodología para actualizar el Plan de Contingencia de OGEI se encuentra alineada a lo establecido en el estándar internacional ISO 22301 – Sistema de Gestión de Continuidad de Negocio.

Tabla 6: Riesgos del Proceso de Gestión de Tecnología de la información

Nº	Descripción del Riesgo	Efecto	Medidas de contención
Factores Naturales o provocados por el hombre			
1	Desastres naturales (terremotos) o provocados por el hombre (incendio,	- Posible deterioro / inutilización del local del MVCS. - Incapacidad total para operar los sistemas mecanizados, las	- Entrenamiento de personal para asumir funciones alternas en caso de desastre. - Contar con sistemas de detección y extinción de incendios.

	inundación, robo, vandalismo, terrorismo, etc.)	comunicaciones y servidores. - En caso extremo inutilización total de servidores y equipos de comunicación.	- Mantener el servicio de vigilancia las 24 horas continuas. - Todos los equipos de cómputo deben estar en un nivel superior al piso, para evitar deterioros por inundaciones. - Mantenimiento periódico de instalaciones eléctricas, telefónicas.
Factor de Servicio			
2	Interrupción eléctrica	Servicio paralizado, se cuenta con grupo electrógeno sin mantenimiento.	- Se cuenta con grupo electrógeno en el MVCS - Mantenimiento de las fuentes alternas de generación eléctrica. - Instalación de lámparas de emergencia. - Señales de prevención iluminadas de salidas y puertas de emergencia. - Entrenamiento de personal para asumir funciones alternas en estos casos (apagar servidores operando con UPS).
3	Caída de circuitos de comunicaciones externas	- Imposibilidad de comunicaciones con el exterior (solo por correo electrónico en equipos móviles) - Suspensión de acceso a internet.	- Mantener actualizado la lista de contactos de los proveedores para las coordinaciones telefónicas que se tengan que realizar ante alguna eventualidad. - Contar con un enlace de internet de Backup con la empresa operadora del servicio.
Factores de Sistemas			
4	Falla en componentes de red de comunicación interna	- Falla switch principal, paralizando totalmente la red. - Falla de switch, paraliza parcialmente equipos del nodo. - Falla en un punto de la red paraliza el equipo afectado.	- Contar con contrato de mantenimiento preventivo / correctivo, que garantice el reemplazo de equipo críticos dañados en 2 horas. - Monitoreo periódico de la red de datos, verificando su performance.
5	Desperfectos en estaciones de trabajo, impresoras y otros dispositivos de cómputo	Imposibilidad de proceso y de emisión de resultados en forma oportuna o correcta.	- Contar con un plan de mantenimiento preventivo / correctivo, que garantice el buen funcionamiento de los equipos. - Monitoreo periódico de los equipos con la finalidad de actuar predictivamente, reemplazando partes antes de fallar.
6	Falla en los servidores de aplicación	Paralización total del servicio de los usuarios afectados.	- Contar con un contrato de mantenimiento preventivo / correctivo, que garantice la atención en el plazo máximo de 2 horas, durante las 24 horas del día. - Ante una falla el proveedor antes de 24 horas entregará el equipo reparado o colocará equipo temporal de reemplazo. - Mantener actualizado el Plan de Contingencia de OGEI, que permita recuperar rápidamente la información desde el Backup y actualizar información pasada la contingencia.

4.2.2 Clasificación de interrupciones y nivel de afectación a los servicios de TI

La activación o no del Plan de Contingencias de OGEI del MVCS, dependerá del resultado de la ejecución del "Procedimiento Gestión de Incidentes de Seguridad" y/o las decisiones tomadas por el nivel estratégico y táctico de este Plan de Contingencias de OGEI, frente a la situación que genere la interrupción del servicio tecnológico.

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia de OGEI, son evaluados de acuerdo con el impacto que tienen sobre la prestación del servicio tecnológico del MVCS, de acuerdo con la siguiente clasificación:

Tabla 7: Clasificación de la Interrupción

Tipo de Interrupción	Características	Ejemplos	Respuesta
TOTAL	Evento que inhabilita el Centro de Datos para prestar sus servicios. No permite que el equipo de tecnología siga laborando en las instalaciones principales de la empresa.	Terremotos. Incendio general. Orden Público. Fallo eléctrico en el sector.	No se cuenta con sede alterna de contingencia.
PARCIAL	Evento que afecta a más de un recurso informático de manera drástica ocasionando la suspensión parcial del funcionamiento del hardware o software considerados como críticos.	Fallas técnicas en equipos de servidores que alojan más de un aplicativo, bases de datos.	No se cuenta con sede alterna de contingencia.
ESPECÍFICA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de informática.	Fallas técnicas de un equipo que aloja un sistema o servicio, ausencia de personal clave.	No se cuenta con sede alterna de contingencia.

La evaluación de la afectación de los servicios de TI, se definió con base en el impacto que puede generar la materialización de alguno de los riesgos identificados en el proceso de Gestión de Tecnologías de la Información en el desarrollo de las actividades propias de cada proceso, de la siguiente manera:

Tabla 8: Niveles de afectación de los servicios de TI

Recursos Afectado	Nivel de Afectación Alto=3, Medio=2, Bajo=1	Tiempo de Respuesta a la Contingencia
Servidores	3	24 horas
Computadoras	1	72 horas
Sistemas de información y/o aplicativos	3	8 horas

Servicio de internet	3	8 horas
Correo Electrónico	2	*considerando el SLA de Google
Red de datos	3	8 horas
Impresoras y Escáner	1	48 horas
Corriente eléctrica	3	2 horas
Telefonía	1	8 horas

4.3 FASE 3: ESTRATEGIAS DEL PLAN DE CONTINGENCIA

Esta estrategia define los aspectos básicos que requieren ser probados periódicamente, a fin de medir el comportamiento integral e individual de los recursos asignados y/o los procedimientos definidos para la atención de una interrupción de un servicio de TI.

La estrategia de prueba del Plan de Contingencia de OGEI, define los aspectos básicos que requieren ser probados periódicamente, a fin de medir el comportamiento integral e individual de los recursos asignados y/o los procedimientos definidos para la atención de una interrupción de un servicio de TI.

De acuerdo a los tipos y frecuencia de pruebas, se eligió las “Pruebas Reales (Tecnológicas)” incluidas en el Plan de Contingencia de OGEI, el cual indica que son pruebas en donde se involucra la activación del Centro de Datos Principal y tendrán una periodicidad de un año de acuerdo al calendario de pruebas coordinado con la Oficina de Tecnología de la Información.

Este tipo de pruebas puede ser parcial o total, donde se prueban secciones o elementos individuales del Plan de Recuperación, como puede ser, un aplicativo o una plataforma o se prueban todos los componentes.

Con informe N° 88-2022-VIVIENDA/OGEI-GFN se alcanza el cronograma anual aprobado de pruebas de contingencias en materia de Tecnología de la Información para el año 2023 (manuales y automatizados) de acuerdo al Plan de Contingencia de OGEI (anexo N°4), el mismo que ha sido elaborado en coordinación con el personal de la Oficina de Tecnología de la Información.

4.3.1 Estrategias del Plan de Contingencia

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

4.3.1.1 Almacenamiento y respaldo

- Realización de copias de respaldo de la información almacenada y procesada en el Centro de Datos.
- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

Periodicidad: Mensual
Responsables: Especialista de Infraestructura y el Oficial de Seguridad de la Información

4.3.1.2 Entorno de réplica

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido, propios de la entidad. Y el especialista de Infraestructura, identifica un ambiente adecuado para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

Periodicidad: Mensual
Responsables: Especialista de Infraestructura y el Oficial de Seguridad de la Información

4.3.1.3 Evaluación y gestión de proveedores

Actualizar el listado de proveedores claves de servicios y recursos de TI y mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

Periodicidad: Semestral.
Responsable:Especialista de Infraestructura

4.3.1.4 Entrenamiento y personal de reemplazo

El personal de la OTI, debe entrenarse en el proceso de recuperación de los servicios de TI. El entrenamiento se evalúa para verificar que ha logrado sus objetivos.

Al inicio de cada año se debe realizar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTI, tales como soporte técnico, redes

y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.

Periodicidad: Semestral.
Responsable: Oficial de Seguridad de la Información

4.3.1.5 Renovación tecnológica

Se desarrolla la programación en el Plan Operativo Institucional que incluye acciones de renovación tecnológica.

Periodicidad: Anual
Responsables: Especialista de Infraestructura

4.3.2 Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del MVCS y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre.

A continuación, se citan las acciones que se realizarán durante una contingencia:

<u>Acciones durante la emergencia</u>

- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.
- Informar al coordinador del Plan de Contingencia sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

4.3.3 Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitarse una emergencia o desastre, a fin de recuperar la información y los servicios informáticos del MVCS para estabilizar la infraestructura tecnológica luego del evento suscitado.

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

Tabla 9: Prioridad de atención durante la restauración de TI

Prioridad de atención	Descripción
1	**Atención prioritaria:** Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios y manejen alto volumen de información. Ejemplo: Sistema de Trámite Documentaría (SITRAD), Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGA), servidores de bases de datos, entre otros.
2	**Atención normal:** Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requieren conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	**Atención baja:** Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Intranet entre otros.

Los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

4.4 FASE 4: ELABORACIÓN DEL PLAN DE CONTINGENCIA

4.4.1 Aspectos generales para la atención de una contingencia

El Plan de Contingencias de OGEI, se activa frente a una situación de interrupción de un servicio y/o infraestructura de TI o de acuerdo a lo determinado por el “Procedimiento Gestión de Incidentes de Seguridad” y/o lo que exprese el nivel estratégico o táctico del Plan de Contingencias de OGEI.

A continuación, se presentan las actividades generales que se deben tener en cuenta por los roles definidos dentro del plan, para la atención de una situación de contingencia de TI.

Tabla 10: Actividades y responsabilidades para el manejo de contingencias de OGEI

Actividad	Responsable	Acción
1	Colaboradores del MVCS	Reportar la falla en el sistema de Mesa de Servicios siguiendo el "Procedimiento de Registro y Atención de Requerimiento de Soporte a los Sistemas de Información y Equipos informáticos"
2	Responsable del Sistema de Mesa de Servicios	Analiza la falla. En caso de corresponder a un incidente de seguridad, traslada la acción al "Procedimiento de Atención de Servicio de Mesa de Servicios y Soporte a Usuarios" Si la situación no es un incidente de seguridad, pero afecta la operación de algún servicio de TI, informa a la Oficina de Tecnología de la Información para la toma de decisión.
3	Equipo de Respuestas ante Incidentes de Seguridad de la Información (CSIRT)	Evalúa y determina si el incidente corresponde a una contingencia. En este caso informa al responsable del Plan de Contingencias de OGEI.
4	Director/a de la Oficina de Tecnología de la Información	Autoriza la puesta en marcha del Plan de Contingencia de OGEI, notificando a las áreas afectadas y a los niveles estratégico y táctico del Plan de Contingencias de OGEI.
5	Oficial de Seguridad de la Información	Gestiona las actividades del Plan de Contingencia de OGEI, asignando a los funcionarios que realizarán las labores operativas de recuperación según el tipo de interrupción y los servicios y/o infraestructura afectada.
6	Equipo de atención del Plan de Contingencias de OGEI Equipos de apoyo de acuerdo a la especialidad	Ejecuta las actividades de recuperación junto con el equipo de atención e informa al Oficial de Seguridad de la Información (según lo descrito en el escenario de contingencia a solucionar). Realiza pruebas de recuperación del servicio y/o infraestructura afectada.
7	Coordinador de Infraestructura Tecnológica	Informa al Director/a de la Oficina de Tecnologías de la Información la finalización de las actividades de recuperación. Coordina las actividades para el restablecimiento de la operación normal de los servicios de TI.
8	- Especialista en Administración de servicios de Red y Telefonía - Especialista en Administración de Sistemas y Servidores - Administración de Base de Datos	Inicia las acciones pertinentes para el restablecimiento del proceso normal (según lo descrito en el escenario de contingencia a solucionar).
9	Grupo de atención del Plan de Contingencias de OGEI.	Actualiza hoja de vida del equipo, servidor o del sistema de información sobre la incidencia presentada.
10	- Director/a de la Oficina de	Realizar análisis de las fallas presentadas y de los

	Tecnología de la Información - Oficial de Seguridad de la Información - Equipo de atención del Plan de Contingencias de OGEI	indicadores del proceso. Documenta los resultados y lecciones aprendidas.
11	Director(a) de Tecnologías de la Información.	Autoriza la finalización del plan. Informar a las áreas afectadas la normalización en la prestación de los servicios de TI. Autoriza el cierre de la contingencia e informa al Director General de la OGEI la situación de contingencia atendida.

4.4.2 Sistemas de Información y Aplicaciones

4.4.2.1 Realizar inventario de los Sistemas de Información y/o Aplicativos afectados de acuerdo con las características relacionadas en el documento Plan de Contingencias de OGEI.

4.4.2.2 Preparar y configurar un equipo de cómputo de acuerdo con las características y condiciones de conectividad especificadas relacionadas en el documento del Plan de Contingencias de OGEI del Sistema de Información y/o aplicación afectada.

4.4.2.3 Restaurar copia de seguridad de la base de datos correspondiente, así como, la copia de respaldo más reciente del código fuente o del archivo de instalación o ejecutable.

4.4.2.4 Revisar permisos de acceso y cuentas de usuario del sistema de información afectado.

4.4.2.5 Verificar la conexión entre la base de datos y el sistema y/o aplicativo.

4.4.2.6 Realizar pruebas de procesamiento y transaccionalidad de datos entre los sistemas y/o aplicativos en el equipo dispuesto para la atención de la contingencia.

4.4.2.7 Paralelo a estas actividades, en el sistema afectado, se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencias de OGEI.

4.4.2.8 En caso que la contingencia se presente en un servicio, sistema de información y/o aplicativo que cuente con un soporte técnico y/o garantía, se debe informar al proveedor o contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el proveedor o contratista.

4.4.3 Recursos Tecnológicos e Infraestructura

4.4.3.1 Realizar inventario físico de la infraestructura afectada de acuerdo con las características relacionadas en el documento Plan de Contingencias de OGEI.

4.4.3.2 Determinar las características técnicas de la infraestructura física afectada.

4.4.3.3 Con la infraestructura no afectada y dependiendo de la situación presentada, realizar las actividades planteadas en los diferentes escenarios para atender la contingencia y restaurar el servicio de TI afectado.

4.4.3.4 Verificar las conexiones entre servicios de TI y la infraestructura dispuesta para la atención de la contingencia.

4.4.3.5 Realizar pruebas de transaccionalidad de datos y/o conexiones en el equipo dispuesto para la atención de la contingencia.

4.4.3.6 Paralelo a estas actividades, en la infraestructura afectada se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencias de OGEI.

4.4.3.7 En caso que la contingencia se presente en la infraestructura que cuente con un soporte técnico y/o garantía, se debe informar al proveedor o contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

Como mínimo se requiere contar con la siguiente infraestructura de TI como base, para poner en marcha cualquier estrategia de atención de contingencia de TI con una interrupción total:

SOLUCIÓN BASE

1. Dos servidores tipo cuchilla con las siguientes características por servidor:
   a. CPU: 2 procesadores Intel Xeon (20 Núcleos)
   b. RAM: 512 GB
   c. HDD: 10TB
2. Sistema Operativo Windows Server Datacenter 2019 R2
3. Base de datos SQL Server 2017 para WINDOWS SERVER 2019
4. Switch de comunicaciones de 48 puertos 1GB.
5. Canal de acceso pasivo a internet.
6. Software de virtualización VMware 7.0 o superior

4.4.4 Recursos Humanos

Los funcionarios asignados por parte de la Oficina General de Estadística e Informática, para la atención de una contingencia que afecte un servicio de TI, se presentan a continuación:

Tabla 11: Funcionarios asignados de OGEI

ROL	CARGO	ANEXO
Líder del Plan de Contingencia	Director/a de OTI	4305
Oficial de Seguridad de la Información	Especialista en Seguridad de la Información	4303
Coordinador/a de Desarrollo Tecnológico	Coordinadora de Desarrollo Tecnológico	4320
Coordinador/a de Infraestructura Tecnológica	Coordinador de Infraestructura Tecnológica	4307
Administración de servicios de Red y Telefonía	Especialista en Infraestructura Tecnológica	4308
Administración de Sistemas y Servidores	Especialista en Administración de Sistemas y Servidores	4306
Administración de Base de Datos	Especialista en Administración de Base de Datos	4307

4.4.5 Aspectos Logísticos

Cuando ocurra una situación inesperada que conlleva a la materialización de un riesgo identificado en este Plan de Contingencia de OGEI, el colaborador afectado o los colaboradores afectados deberán reportarlo de inmediato a través de la Mesa de Servicios al correo mesadeservicios@vivienda.gob.pe o al teléfono 2117930 anexo 1234 o comunicarse directamente a la Oficina General de Estadística e Informática al anexo 4303, 4320, 4305, 4306, 4307 y 4308. Una vez reportada la contingencia, se activará por parte de la Oficina de Tecnología de la Información el respectivo procedimiento para el manejo de contingencia. Adicionalmente al interior de la Dirección General se realizan las siguientes actividades de prevención de forma periódica.

4.4.5.1 Verificar el directorio telefónico de contacto de los funcionarios responsables y mantenerlo actualizado.

4.4.5.2 Verificar los procedimientos de control de copias y restauración de seguridad.

4.4.5.3 Realizar jornadas de capacitación sobre el plan, a funcionarios de las diferentes áreas sobre las actividades a seguir en el proceso de contingencia.

4.4.5.4 Habilitar el servicio de conectividad con los proveedores y correo electrónico que se tiene definido para garantizar el servicio.

4.5 FASE 5: IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA

El plan aplica las actividades necesarias para mantener en operatividad los sistemas de información y/o aplicativos y la infraestructura tecnológica que los soporta el MVCS,

para su implementación es necesario tener en cuenta los aspectos técnicos, humanos y de logística descritos en este plan, que permitan estar preparados para afrontar cualquier contingencia.

4.5.1 Escenarios del Plan de Contingencia de OGEI

La forma como se han estructurado las actividades que conforman el Plan de Contingencia de OGEI, es a través de un conjunto de actividades cronológicamente clasificadas (antes, durante, después) por cada tipo de evento, cuya ocurrencia podría paralizar las operaciones dentro de la institución.

Se han identificado tres escenarios críticos:

- Edificio no operativo
- Centro de Datos no operativo
- Centro de Datos no operativos y falla de datos de los servidores

En la matriz a continuación se detallan las actividades a realizar para cada caso:

Tabla 12: Actividades cronológicamente clasificadas

CASO Nº	ANTES	DURANTE	DESPUÉS
1. Edificio no operativo (sede central del MVCS en mal estado) con Centro de Datos Alterno	- Contar con un Centro de Datos Alterno, que cuente con todas las medidas de seguridad del caso, donde el MVCS pueda asegurar y operar sus servicios críticos como medida de contingencia ante un desastre. - Disponer el contacto autorizado del proveedor (interno o externo) del Centro de Datos Alterno. - Poseer el listado de teléfonos de contactos del personal de TI (equipo del Plan de Contingencia) a fin de convocar para acudir al Centro de Datos Alterno. - Mantener una copia de los servicios y aplicaciones del MVCS en la nube.	- Contactar al proveedor del Servicio del Centro de Datos Alterno a fin de que brinde las facilidades y acceso al personal de TI del MVCS para activar o poner en línea los servicios críticos. - Contactar al encargado de subir los backup a la nube. - Realizar la recuperación de datos e información crítica de ser necesario.	- Verificar con el equipo de contingencia de TI que los servicios y aplicativos se encuentran restablecidos. - Mantener actualizado y en línea los servicios críticos en el Centro de Datos Alterno - Prever la posibilidad de volver los servicios al Centro de Datos original. - Evaluar los daños al Centro de Datos principal a fin de estimar la posibilidad de ir restaurando sus servicios de forma progresiva.
2. Centro de Datos	- Ejercicios de pruebas, simulaciones o ejercicios de	- Contactar al personal de TI (equipo del Plan de	- Coordinar con la Oficina de

no operativo	situaciones en las que **no se cuente con el Centro de Datos Alterno.** - Mantenimiento y verificación de los sistemas de seguridad física y lógica del Centro de Datos: ➢ Sistema de detección y aviso de incendios. ➢ Sistema de videovigilancia. ➢ Sistema de control de acceso. ➢ Sistema de verificación de temperatura. ➢ Sistema de aire acondicionado de precisión. ➢ Cableado eléctrico y de datos. ➢ Luces de emergencia. ➢ Equipos de protección ante caída de fluido eléctrico (UPC). ➢ Pozos a tierra.	Contingencia) a fin de convocar para acudir al Centro de Datos - En caso de incendio o amago de incendio: Llamar al Centro de Control del MVCS. - En caso de inundación: llamar a la Oficina de Servicio General de OGA. - En caso de pérdida de información en el Centro de Datos: Contactar al encargado de subir los backup a la nube y avisar al Oficial de Seguridad de la Información.	Abastecimientos y Control Patrimonial para la verificación de la energía eléctrica en el Centro de Datos. - Verificación de las redes de comunicación por piso. - Verificación del alta de los servidores (checklist). - Recuperación de datos a través del levantamiento de backup. - Los trabajos de recuperación tendrán dos etapas: ➢ La primera: la restauración del servicio usando los recursos de la institución o local de respaldo. ➢ La segunda: volver a contar con los recursos en las cantidades y lugares propios del sistema de información debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestros sistemas e imagen institucional.
3. Centro de Datos no operativos y falla en el equipamiento de los servidores	- Realizar pruebas de recuperación de datos del Centro de Datos según cronograma en coordinación con el encargado de subir los backup a la nube. - Mantenimiento y verificación de los sistemas de seguridad física y lógica del Centro de Datos: ➢ Sistema de detección y aviso de incendios. ➢ Sistema de videovigilancia. ➢ Sistema de control de acceso. ➢ Sistema de verificación de temperatura. ➢ Sistema de aire	Todo lo descrito en el N° 2 De no lograr la recuperación de información de los servidores, se deberá realizar la recuperación de las copias de respaldo de los servidores.	Evaluar daños a fin de verificar equipos recuperables que puedan operar fuera del Centro de Datos.

	acondicionado de precisión. ➢ Cableado eléctrico y de datos. ➢ Luces de emergencia. ➢ Equipos de protección ante caída de fluido eléctrico (UPS). ➢ Pozos a tierra.		

4.5.2 Tipos y frecuencia de pruebas

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

- Programación periódica establecida con los equipos de administración de sistemas de información y plataforma tecnológica como mecanismo de control de calidad de la función de contingencia; por ejemplo, después de la terminación de un proyecto, a los tres (03) meses y posteriormente cada (06) meses.
- Cuando haya modificaciones de hardware, software y aplicativos o cuando existan cambios significativos en la plataforma tecnológica cubierta por el Plan.
- También pueden realizarse cuando se prevea el riesgo de que suceda un evento que afecte la entidad, como problemas laborales o de orden público.

Desde el punto de vista del cubrimiento o alcance, los tipos de pruebas pueden ser:

4.5.3 Pruebas de escritorio (detallada y documentada)

Se trata de un tipo de prueba programada y controlada que consiste en una revisión detallada del Plan de Contingencias de OGEI y los procedimientos implicados. Para su ejecución se verifica la existencia del plan y sus procedimientos, y se convoca a los diferentes equipos de contingencia a participar en un taller-práctico en donde se verifique paso a paso y en forma ordenada, bajo la moderación del responsable del Plan de Contingencia de OGEI, con el fin de determinar fallas y omisiones con el criterio experto de quienes participan. En este ejercicio se tienen en cuenta las dependencias de las diferentes actividades.

Es recomendable ejecutar este tipo de prueba antes de ejecutar una prueba real y una vez sea publicada alguna actualización del Plan de Contingencia.

4.5.4 Pruebas Reales (Tecnológicas)

Son pruebas en donde se realizan en el Centro de Datos principal y tendrán una periodicidad mínima de un año.

Este tipo de prueba puede ser parcial o total, donde se prueban secciones o elementos individuales del Plan de Recuperación, como puede ser, un aplicativo o una plataforma o se prueban todos los componentes.

4.5.5 Prueba General

Esta prueba consiste en verificar el desempeño de la plataforma tecnológica designada para la contingencia de OGEI en un ambiente de interrupción total, la cual consiste en realizar un simulacro donde se compruebe de manera integral la ejecución de las siguientes actividades:

- Pruebas de suministro de energía eléctrica con UPS. (corte del servicio de energía y verificación de la entrada de las UPS en funcionamiento).
- Puesta en producción de los equipos de respaldo y sistemas de información en el Centro de Datos del MVCS.
- Recuperación de la información de las copias de respaldo de información, para verificar su correcto proceso de restauración (de acuerdo a lo descrito en el “Procedimiento para la Realización y Control de Copias de Respaldo”).

Dado que este tipo de prueba implica la afectación de los servicios de TI en producción, se recomienda ejecutar en horarios no hábiles para no impactar de manera importante en caso de producirse fallas en la operación. Es importante repetir este ejercicio tantas veces como se considere necesario para adquirir un muy buen nivel de conocimiento y práctica.

El siguiente paso es ejecutar este mismo tipo de pruebas en horarios hábiles, una vez se haya determinado que los niveles de servicio de la plataforma de respaldo son aquellos establecidos en los compromisos del Plan de Contingencias de OGEI.

Una vez realizado este último tipo de ejercicio en varias oportunidades, el cual es programado y controlado, se puede pasar a la ejecución de estas pruebas en forma no programada, pero sí controlada, teniendo en cuenta seguir un protocolo como el expuesto antes: las primeras veces en horario no hábil y luego en horario hábil.

4.5.6 Prueba de UPS

Los sistemas de alimentación ininterrumpida - UPS (por sus siglas en inglés - Uninterruptible Power Supply), son el sistema que garantiza la energía eléctrica a los equipos de cómputo del Centro de Datos, cuando haya una suspensión de este servicio.

La prueba consiste en verificar la activación automática de la puesta en marcha de los UPS cuando se suspende la energía eléctrica. Adicionalmente se puede realizar una prueba de autonomía de 20 minutos que debe mantener el suministro de energía a los equipos conectados a la red eléctrica regulada.

Esta prueba se realiza manteniendo una cantidad determinada de equipos de cómputo y servidores activos, se corta el fluido eléctrico normal.

4.5.7 Prueba de puesta en producción de los equipos de respaldo

Consiste en instalar y preparar un equipo alterno en el Centro de Datos con las características requeridas de acuerdo a los servicios de la Oficina de Tecnología de la Información que se requieran con el fin de verificar el funcionamiento y puesta en producción. (No se cuenta con sede alterna de contingencia).

4.5.8 Prueba de restauración de información

Consiste en realizar una restauración de las copias de seguridad más recientes que se tienen de los sistemas de información y/o aplicativos que seleccione el responsable del Plan de Contingencias de OGEI (SITRAD, PRESET, SSP, DIAGNÓSTICO entre otros) utilizando los procedimientos existentes de restauración y verificar la comunicación entre los aplicativos y las bases de datos.

4.5.9 Evaluación de la prueba

Una vez se haya realizado la prueba y como actividad final, es necesario efectuar una evaluación o revisión de su desarrollo en la cual estén analizados los objetivos, los parámetros, los criterios establecidos, las fallas y fortalezas.

4.5.10 Etapas de la prueba

A continuación, se presentan las etapas que se deben realizar para el desarrollo de una prueba al Plan de Contingencias de OGEI.

Tabla 13: Etapas del desarrollo de las pruebas del Plan de Contingencia

Etapa	Descripción
Planeamiento de la prueba	Definir los equipos participantes, los objetivos específicos de la prueba.
Notificación de la prueba a los equipos de trabajo	Notificar a los equipos participantes la realización de la prueba y verificar que todos ellos estén enterados.
Alistamiento y habilitación de ambientes para la prueba.	Incluye contar con todos los elementos necesarios para iniciar el proceso de prueba en el Centro de Datos.
Puesta en producción del Centro de Datos para la prueba	Actividades de los equipos de recuperación tendientes a restaurar y sincronizar las aplicaciones.
Operación en el Centro de Datos para la prueba	Actividades de los equipos de recuperación tendientes a probar la operación en el Centro de Datos para la contingencia.
Limpieza de los datos después de la prueba	Borrar todos los archivos sensibles de la prueba de contingencia.
Evaluación de la prueba	Reunirse con el personal que participó en la prueba para identificar problemas y aciertos del Plan de Contingencia de OGEI.

4.5.11 Documentación de las pruebas

Para realizar el registro del antes, durante y después de la ejecución de las pruebas al Plan de Contingencias de OGEI, se utilizará el formato descrito en el Anexo 1 – “Formato de Documentación de Pruebas del Plan de Contingencias de OGEI” de este documento.

4.5.12 Actividades críticas en el marco del Plan de Continuidad Operativa del MVCS aprobado con RM N° 248-2022-VIVIENDA

Tabla 14: Actividades críticas en el marco del Plan de Continuidad Operativa

Objetivo:	Activar el equipamiento, redes críticas y servicios para trabajos remotos, que permitan la conectividad de los procesos críticos.	**Responsable:**	**Periodo Máximo Tolerable:**
		OGEI	12 horas

N°	Actividad	Rol	Responsable
1	Activar rombo y DAF	Administrativo/a	Director/a General de la Oficina General de Estadística e Informática

2	Activar el Plan de Contingencia de OGEI e informar la continuidad de servidores y medidas aplicadas	Administrativo/a	Director/a de la Oficina de Tecnología de la Información
	Procedimiento:		
	• Verificar la continuidad de los servicios en el centro de datos principal y se informa continuidad de servidores y medidas aplicadas.	Especialista Red 1	Especialista en Administración de Sistemas y Servidores
	• Informar al/a la Director/a General de OGEI los servicios que están levantados en este momento y los sistemas críticos importantes **(servicios críticos: Portal Web, Intranet, correo electrónico - 100% en la nube; SITRAD, SSP, Preset, Preset2, Trámite OGA, SIAF, SIGA, Diagnósticos de Agua y Saneamiento se deberán recuperarse).**	Especialista Gestor	Coordinador/a de Infraestructura Tecnológica
	• En caso se encuentren inoperativos los servidores, se deberá restaurar las bases de datos y aplicaciones desde el servicio de almacenamiento en la nube hacia nuevos servidores que deberán ser adquiridos, alquilados o prestados de manera temporal.	Especialista de base de datos	Especialista de base de datos
	• En caso el servicio de almacenamiento en la nube no esté disponible, informar al jefe inmediato la situación y el tiempo de restablecimiento estimado. Además, comunicar al jefe inmediato para que éste pueda coordinar con el Director/a de la OSDN, para luego informar a la OGA, Secretaría General y a los Viceministros, la sede donde los servicios serán recuperados, levantados y se mantendrán operativos.	Especialista Gestor	Coordinador/a de Infraestructura Tecnológica
3	Efectuar pruebas y reducir afectaciones a redes críticas.	Administrativo 2	Director/a de la Oficina de Tecnología de la Información
	Procedimiento:		
	• En caso de disponibilidad de conexión en las sedes del MVCS, confirmar tiempo de reconexión con el proveedor del servicio.	Especialista Red 2	Especialista en Infraestructura Tecnológica
	• En casa sede del MVCS, el responsable de OGEI deberá verificar el estado de los equipos de Red según los procedimientos y planes de OGEI.		
4	Desarrollar pruebas de conectividad y comunicaciones del COE-VIVIENDA y sala del Grupo de Trabajo de GRD del MVCS.	Especialista Red 2	Especialista en Infraestructura Tecnológica
5	Establecer las verificaciones de los equipos y accesorios del COE-VIVIENDA y sala del	Especialista Red 1	Especialista en Administración de Sistemas

	Grupo de Trabajo de GRD del MVCS.		y Servidores
6	Activar los servicios para trabajo remoto, de ser necesario, e informar la situación.	Administrativo 2	Director/a de la Oficina de Tecnología de la Información.
	Procedimiento:		
	• Activar Mesa de Servicios Virtual.	Analista 1	Soporte Técnico
	• Activar servicios de conexiones remotas mediante VPN o Google Remote Desktop para las personas que usan SIGA, SIAF, Melissa, Clarissa o trámite de planillas.	Especialista Red 2	Especialista en Infraestructura Tecnológica
	• Brindar soporte de sistemas de manera virtual.	Analista 1	Soporte Técnico
	• Activar préstamos de bienes tecnológicos a través de los directores generales de OGA y OGEI.	Especialista Gestor	Coordinador/a de Infraestructura Tecnológica
	• Activar la Mesa de Partes Virtual, de no ser posible la activación, se procede a activar la cuenta de correo: mesadepartes@vivienda.gob.pe, con la administración de la OGDA.	Especialista Red 1	Especialista en Administración de Sistemas y Servidores
	• Habilitar la cuenta abastecimiento_mvcs@vivienda.gob.pe para el tema de pago de terceros y proveedores importantes de manera virtual, con la administración de la OGA.	Especialista Red 1	Especialista en Administración de Sistemas y Servidores
	• Informar situación de los servicios activados.	Especialista Gestor	Coordinador/a de Infraestructura Tecnológica
7	Inspeccionar y registrar los equipos de tecnologías de información.	Especialista Red 1	Especialista en Administración de Sistemas y Servidores
8	Informar término de medidas y acciones conformes.	Especialista Gestor	Coordinador/a de Infraestructura Tecnológica
9	Activar servicios y control para trabajo remoto, de ser necesario.	Especialista Red 2	Especialista en Infraestructura Tecnológica

4.6 FASE 6: MONITOREO

Dado que las condiciones del inmueble del MVCS pueden variar con el tiempo, lo mismo que los bienes informáticos, incluidos los equipos informáticos del Centro de Datos, es importante que se realice una verificación del Plan de Contingencia.

Las acciones de verificación se deben realizar de manera trimestral y bajo un ambiente controlado, donde se comprueben que con las acciones definidas los bienes y servicios informáticos respondan de acuerdo a lo esperado, considerando que los procesos pueden variar y afectar la disponibilidad de los sistemas. Por lo que, es importante la ejecución de simulacros de interrupción de servicios informáticos, los cuales deben estar definidos, de forma que se pueda determinar el nivel de éxito de los mismos. Para dichos simulacros se debe considerar lo siguiente:

- Definir a los responsables del simulacro por las diferentes áreas interesadas.
- Evaluar los riesgos, validar el inventario de recursos.
- Elaborar un plan de atención del Centro de Datos.
- Se debe comunicar a todo el personal de la Institución sobre los simulacros.
- Se debe realizar una evaluación conjunta con todos los responsables definidos para el simulacro, y plasmar en un documento las mejoras que se requieren plantear.
- Comunicar a todos los interesados el resultado de la evaluación del simulacro.

En base a los resultados obtenidos se realiza la modificación y mantenimiento del presente plan, para lo cual se establecen controles formales para dichas modificaciones. Asimismo, todos los responsables mencionados en el presente plan deberán tener conocimiento de los cambios.

5. ANEXOS

Anexo 1. Formato de Documentación de Pruebas del Plan de Contingencia de OGEI: https://bit.ly/3vVEYYI

PERÚ | Ministerio de Vivienda, Construcción y Saneamiento | Secretaría General | Oficina General de Estadística e Informática

Documentación de Pruebas del Plan de Contingencias de OGEI	Versión 2023

RIESGO A EVALUAR	<Nombre del riesgo a evaluar de acuerdo a lo descrito en la sección 6 “Identificación de Riesgos” del Plan de Contingencia de OGEI Ver. 2024>
TIPO DE INTERRUPCIÓN	<Identificar el tipo de interrupción a trabajar de acuerdo a lo descrito en la sección 9 “Clasificación de interrupciones y nivel de afectación a los servicios de TI” del Plan de Contingencia de OGEI Ver. 2024>
ESCENARIO DE	<Referir el escenario de prueba que se va a simular de acuerdo

PRUEBA	a lo descrito en la sección 10.1 “Escenarios del Plan de Contingencia de OGEI” Ver. 2024>		
OBJETIVO DE LA PRUEBA	<Describir la finalidad de la prueba a realizar>		
RECURSO A PROBAR	<Nombre del sistema de información, aplicativo y/o infraestructura tecnológica y/o servicio de TI que se va a probar de acuerdo a lo descrito en la sección 6 “Inventario de servicios e infraestructura de TI” del Plan de Contingencia de OGEI Ver. 2024>		
FECHA	**DURACIÓN**	**RESPONSABLE**	**DESCRIPCIÓN**
<dd/mm/aaaa del diligenciamiento del formato>	<Tiempo estimado de la duración de la prueba>	<Responsable de la ejecución de la prueba>	<Descripción resumida de la prueba a realizar>

ALCANCE: <Describir el alcance del plan de pruebas, identificando el lugar de la prueba, los recursos, servicio, aplicativos y/o servicios que serán sometidos a pruebas y los tipos de prueba que se realizarán, de acuerdo a lo descrito en la sección 4.5.2 “Tipos y frecuencia de pruebas” del Plan de Contingencias de OGEI Ver. 2024>

REQUISITOS PARA LA PRUEBA

- **Recurso Humano:** <Especificar el recurso humano necesario para la ejecución del plan de pruebas, incluyendo los descritos en la sección 5 “Roles y responsabilidades dentro del Plan de Contingencias de OGEI” del Plan de Contingencias de OGEI Ver. 2024, así como los proveedores involucrados>
- **Requerimientos Hardware:** <Especificar los requerimientos de hardware (sistema operativo, memoria, servidor de aplicaciones, red, etc.) para la ejecución del plan de pruebas>
- **Requerimientos Software:** <Especificar los requerimientos de software y copias de respaldo para la ejecución del plan de pruebas>
- **Requerimientos de Logística:** <Especificar los requerimientos logísticos que se requieran (ejemplo: transporte, autorizaciones, entre otros) para la ejecución del plan de pruebas>

PLAN DE PRUEBAS

<Por cada tipo de prueba diligencie un cuadro>

Tipo de prueba:	<Tipo de prueba, citar el tipo de prueba a realizar de acuerdo a lo descrito en la sección 10.2 “Tipo y frecuencia de las pruebas” del Plan de Contingencias de OGEI Ver. 2024>
Identificador:	<Identificador único de la prueba, puede estar compuesta por la fecha y un número consecutivo>
Líder de la prueba:	<Nombre de la persona líder de la prueba>
Objetivo:	<Objetivo de la ejecución del tipo de prueba>
Técnica:	<Técnica empleada para ejecutar la prueba. Secuencia de pasos y condiciones que debe seguir el equipo de pruebas para ejecutarla >
Precondiciones:	<Condiciones previas para la ejecución de la prueba>
Criterios de éxito:	<Criterios para considerar que la ejecución de la prueba generó resultados satisfactorios>
Precondiciones:	<Conjunto de condiciones que deben ser ciertas o que se deben cumplir antes de iniciar la prueba>

Resultado esperado:	<Resultado que se espera obtener con la ejecución de la prueba, se debe establecer antes de ejecutar la prueba>
Secuencia de pasos para la ejecución de la prueba:	<Descripción de cada uno de los pasos que se requieren para ejecutar la prueba, teniendo como referencia lo descrito en el numeral 10.3 “Etapas de la prueba” del Plan de Contingencias de OGEI Ver. 2024>
Resultado obtenido:	<Resultado obtenido después de ejecutar la prueba. En caso de que el resultado obtenido sea diferente al resultado esperado se deben describir dichas diferencias y las posibles causas que las generaron>
Fecha ejecución:	<Fecha en la cual se ejecuta la prueba – formato dd/mm/aaaa>
Anexos:	<Relación de los anexos que complementan la ejecución de la prueba>
Observaciones:	<Observaciones adicionales de la prueba>

APROBACIÓN DE LA SOLICITUD DE PRUEBA

SOLICITADA POR
Informe N° 02-2024/OGEI-GFERNANDEZ (HT:1076-2024)
Asunto: Cronograma de pruebas de contingencia para el año 2024

APROBADA POR
Cargo: Director/a de la OTI
Nombre:
Dependencia: OTI / OGEI
Fecha:

REPORTE DE RESULTADOS DE LA PRUEBA

REALIZADA POR
Cargo:
Nombre:
Dependencia:
Fecha:

ACEPTADA POR
Cargo: Coordinador de Infraestructura Tecnológica
Nombre: kenny Rodriguez Caceres
Dependencia: OTI / OGEI
Fecha:

Anexo 2. Lista de contactos de proveedores de servicios

Nº	PROVEEDOR	SERVICIO	CONTACTO	TELEFÓNO	Correo electrónico
1	GTD	Telefonía fija	Mesa de Servicios	7430911	Clientes.GtdPeru@grupogtd.com
2	Redes y Servicios	Central Telefónica	Mesa de Servicios	7390803	soporte@red.net.pe
4	Nextnet	Servicio de internet Principal	Mesa de Servicios	6449470 op3 op1	noc@nextnet.pe

Anexo 3. Teléfonos de emergencia de San Isidro

INSTITUCIÓN	TELÉFONO
BOMBEROS	
Emergencia	116
Bomberos San Isidro 100	264 0339 - 116
Bomberos Miraflores 28	445 7447
MUNICIPALIDAD	
Serenazgo / Alerta San Isidro	319 0450
Defensa Civil	513 9000 / 2931
Central Telefónica	513 9000
POLICÍA NACIONAL	
Emergencias	105
Comisaría San Isidro	441 1275
Comisaria Orrantia	264 1932 - 264 6561
UDEX-Explosivos	433 3333
DIROVE-Robos Vehículos	328 0351 - 328 0207
DIRINCRI-Crímenes	221 1523
DINCOTE-Terrorismo	475 2995
URGENCIA - EMERGENCIAS MÉDICAS	
SAMU-Sistema atención Médica Urgencia	106
Cruz Roja Peruana	268 8109
Clínica Javier Prado	440 2000 - 211 4141
Clínica Anglo Peruana	616 8900 / 1132
Clínica Ricardo Palma	224 2224
Hospital Casimiro Ulloa	204 0900
Clínica El Golf	631 0000
Central Hospital FAP	440 2749
Emergencias médicas (ambulancia municipal)	513 9008 opción 1
AMBULANCIAS - EMERGENCIA ESSALUD STAE (Sistema de Transporte Asistido de Emergencias)	117

COMPAÑÍAS DE SEGUROS	
Pacifico	415 1515 - 513 5000
Rímac	411 1111
Mapfre	213 3333
La Positiva	211 0211
SERVICIOS	
Defensa Civil - INDECI Emergencias	115
Mensaje de voz - Emergencia por Desastre	119
INDECI - Instituto de Defensa Civil	225 9898
Luz del Sur	617 5000
EDELNOR	517 1717
CÁLIDDA -Gas Natural	614 9000 / 1808
SEDAPAL - Red de Agua y Desagüe	317 8000
Morgue - Lima	328 8204
Centro Antirrábico - San Isidro	513 9000 / 4110
Morgue-Lima	328 8204

*** Información de la página web de la Municipalidad de la San Isidro:** https://bit.ly/3irjHDl

Anexo 4. Cronograma de pruebas de contingencia 2024

OFICINA GENERAL DE ESTADISTICA E INFORMATICA

ACTA DE CONFORMIDAD

Fecha:	03/01/2024
De la unidad orgánica:	OGEI
A la unidad orgánica:	Oficina de Tecnología de la Información
Motivo:	Elaboración y coordinación del cronograma de pruebas de contingencia para el año 2024

Cronograma de pruebas de contingencia para el año 2024												
Escenarios	Horario	01	02	03	04	05	06	07	08	09	10	11	12
Caída de la Central Telefónica	Fuera del horario laboral	X									X		
Caída del Internet de los Centros de Atención a los Ciudadanos	Fuera del horario laboral							X					
Caída de Servidor de Base de datos	Fuera del horario laboral		X			X			X			X	
Caída del Directorio Activo	Fuera del horario laboral			X						X			
Caída de Firewall	Fuera del horario laboral				X						X		
Caída del Switch Core	Fuera del horario laboral					X						X	
Caída de Internet sede principal	Fuera del horario laboral						X						X

FIRMA DIGITAL Firmado digitalmente por:VASQUEZ ALDAVE Maria Isabel FAU 20504743307 soft
Motivo: Soy el autor del documento
Fecha: 2024/01/03 11:36:54-0500
VIVIENDA

Firma.....
Nombre **MARIA ISABEL VASQUEZ ALDAVE**
DNI: 07874267

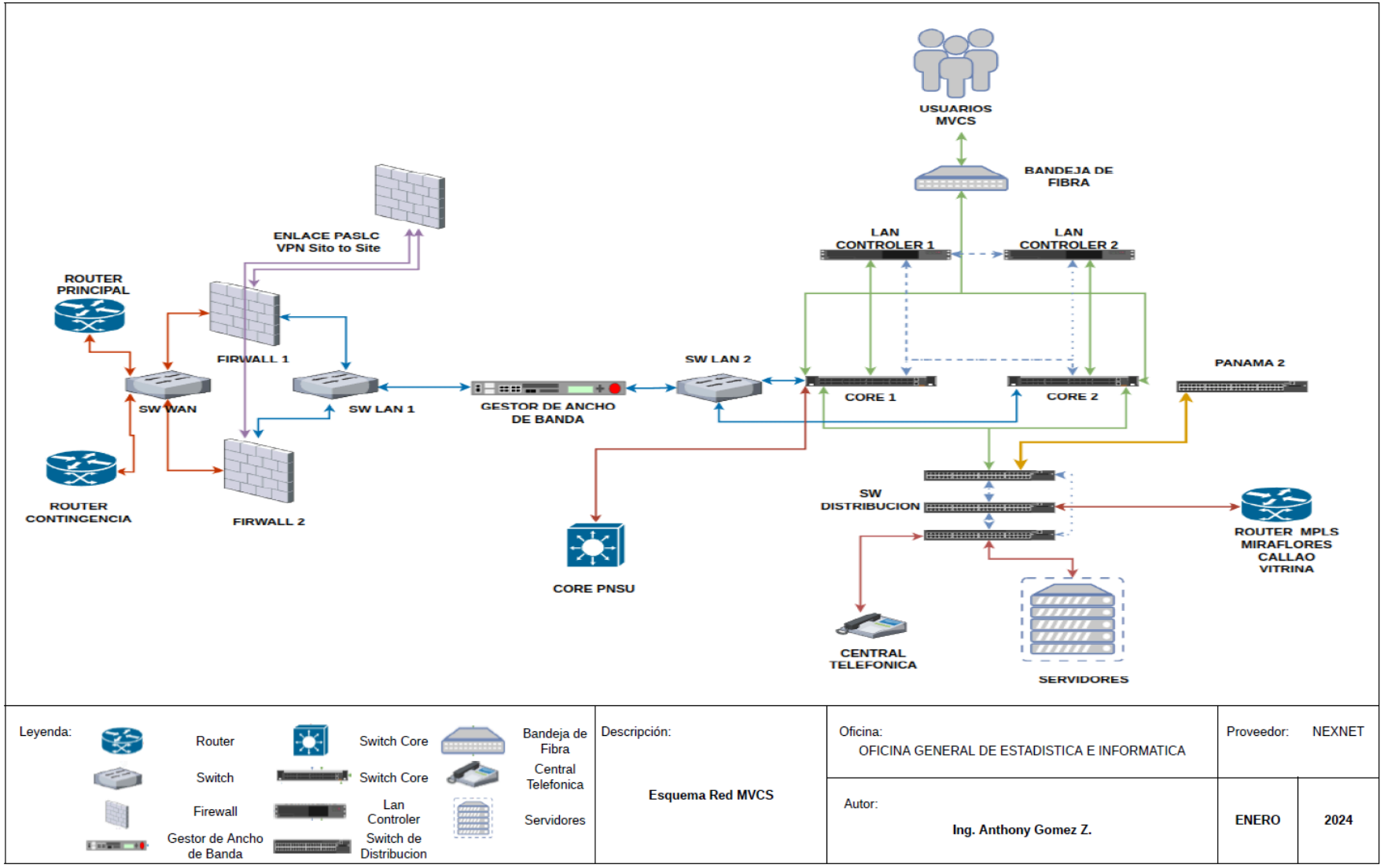
FIRMA DIGITAL Firmado digitalmente por:RODRIGUEZ CACERES Kenny Mirko FAU 20504743307 soft
Motivo: En señal de conformidad
Fecha: 2024/01/04 11:12:42-0500
VIVIENDA

Firma.....
Nombre **KENNY RODRIGUEZ CACERES**
DNI: 40235471

FIRMA DIGITAL Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft
Motivo: En señal de conformidad
Fecha: 2024/01/03 09:44:50-0500
VIVIENDA

Firma.....
Nombre **GUILLERMO FERNÁNDEZ NAMUCHE**
DNI: 25770449

Anexo 5. Topología de red del MVCS - Interconexión sedes



Anexo 6. Diagrama de la topología de la red del MVCS - Infraestructura sede principal