PERÚ | Ministerio de Vivienda, Construcción y Saneamiento | Organismo Técnico de la Administración de los Servicios de Saneamiento

PLAN

Tipo de documento normativo	Nro. Versión	Total, de páginas
PLAN	01	60

PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS DEL OTASS 2024-2025

Etapa / Responsable	Firma
Elaborado por: Pedro Jesús Quispe Castillón **Cargo:** Analista de Gestión de Servicios de Tecnologías de la Información	Firma digital Firmado digitalmente por QUISPE CASTILLON Pedro Jesus FAU 20565423372 soft Motivo: Soy el autor del documento Fecha: 07.11.2024 16:28:58 -05:00
Revisado por: Luis Andrés Canchari Cuyutupac **Cargo:** Jefe de la Unidad de Tecnologías de la Información	Firmado digitalmente por CANCHARI CUYUTUPAC Luis Andres FAU 20565423372 soft Motivo: Soy el autor del documento Fecha: 2024/11/07 16:23:36-0500
Revisado por: Katlen Pacheco Roman **Cargo:** Jefa de la Oficina de la Administración	Firmado digitalmente por PACHECO ROMAN Katlen FAU 20565423372 soft Motivo: Doy V°B° Fecha: 2024/11/07 20:52:04-0500
Revisado por: Wilians Mori Isuisa **Cargo:** Jefe de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por MORI ISUISA Wilians FAU 20565423372 soft Motivo: Soy el autor del documento Fecha: 2024/11/07 18:27:23-0500
Revisado por: Raúl Enrique Orjeda Pereda **Cargo:** Jefe de la Oficina de Asesoría Jurídica	Firmado digitalmente por ORJEDA PEREDA Raul Enrique FAU 20565423372 soft Motivo: Soy el autor del documento Fecha: 2024/11/07 18:04:07-0500

INDICE

I. PRESENTACIÓN 3
II. MARCO LEGAL 4
III. ANTECEDENTES Y ALCANCE 5
IV. DIAGNOSTICO O CARACTERIZACIÓN DE LA PROBLEMÁTICA 5
V. ARTICULACIÓN CON EL PEI Y POI 6
VI. MARCO TEÓRICO Y METODOLOGÍA 7
VII. OBJETIVOS E INDICADORES DEL PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS 30
VIII. PROGRAMACIÓN DE ACTIVIDADES DEL PLAN 31
IX. ANEXOS 35

I. PRESENTACIÓN

El Organismo Técnico de la Administración de los Servicios de Saneamiento, es un organismo público técnico especializado adscrito al Ministerio de Vivienda, Construcción y Saneamiento, con personería jurídica de derecho público interno, con autonomía funcional, económica, financiera y administrativa, con competencia a nivel nacional, que tiene como funciones: dirigir el Régimen de Apoyo Transitorio, fortalecer las capacidades de los prestadores urbanos de los servicios de saneamiento y promover la integración de los prestadores y sus procesos, para lograr su sostenibilidad.

La Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, establece que las entidades públicas usen obligatoriamente la Norma Técnica Peruana NTP-ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. El control “5.30 Preparación de las TIC para la continuidad del negocio” de la norma en mención indica que la preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad de negocio y los requisitos de continuidad de las tecnologías de información y comunicaciones.

Asimismo, la Resolución Ministerial N° 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno, señala que el Plan de Recuperación de los servicios informáticos forma parte del Plan de Continuidad Operativa, el cual busca inicialmente restaurar los servicios informáticos necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

El Organismo Técnico de la Administración de los Servicios de Saneamiento, en cumplimiento de la Resolución Ministerial N° 320-2021-PCM, mediante Resolución Directoral N° 000073-2023-OTASS-DE conformó el Grupo de Comando para la Gestión de la Continuidad Operativa del Organismo Técnico de la Administración de los Servicios de Saneamiento. Y mediante Resolución Directoral N° 000154-2023-OTASS-DE, del 27 de septiembre del 2023, aprobó el Plan de Continuidad Operativa.

En ese sentido, el Plan de Recuperación de los Servicios Informáticos del Organismo Técnico de la Administración de los Servicios de Saneamiento, es un documento técnico que contiene la planificación, evaluación de riesgos y escenarios, determinación de las estrategias, definición y ejecución del plan de pruebas, implementación del Plan Recuperación de los Servicios Informáticos y el monitoreo; cuya finalidad es la recuperación eficiente y efectiva de los servicios Informáticos del alcance establecido por la Entidad.

II. MARCO LEGAL

2.1 Ley N°29664, Ley que crea el Sistema Nacional de Gestión de Riesgos de Desastres (SINAGERD), y modificatorias.

2.2 Decreto Supremo N°006- 2019-VIVIENDA que aprueba la primera sección del Reglamento de Organización y Funciones del Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS.

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

2.4 Decreto Supremo N°115-2022-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022-2030.

2.5 Resolución Ministerial N°276-2012-PCM, que aprueba la Directiva N° 001-2012-PCM/SINAGERD "Lineamientos para la Constitución y Funcionamiento de los Grupos de Trabajo de la Gestión del Riesgo de Desastres en los Tres Niveles de Gobierno".

2.6 Resolución Directoral N°000154-2023-OTASS-DE, que aprueba el Plan de Continuidad Operativa del OTASS.

2.7 Resolución Ministerial Nº180-2013-PCM que aprueba los lineamientos para la organización, constitución y funcionamiento de las Plataformas de Defensa Civil.

2.8 Resolución Ministerial N°320-2021-PCM, que aprueba los "Lineamientos para la Gestión de Continuidad Operativa y la Formulación de los Planes de continuidad Operativa de las Entidades Públicas en los tres niveles de gobierno"; y deroga la Resolución Ministerial N°028-2015-PCM, que aprueba los "Lineamientos para la Gestión de Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno".

2.9 Resolución Directoral N°000154-2023-OTASS-DE, que aprueba el Plan de Continuidad Operativa del OTASS.

2.10 Resolución Directoral N°000010-2019-OTASS-DE, que aprueba la segunda sección del Reglamento de Organización y Funciones del Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS.

2.11 Resolución Directoral N°000103-2023-OTASS-DE, que aprueba la Directiva "Disposiciones para la Gestión de los Documentos Normativos en el Organismo Técnico de la Administración de los Servicios de Saneamiento y sus Unidades Ejecutoras" Versión 04.

2.12 Resolución de Gerencia General N° 010-2024-OTASS-GG que aprueba el Reglamento Interno de Servidores Civiles del Organismo Técnico de la Administración de los Servicios de Saneamiento.

2.13 Resolución de Gerencia General N°000033-2024-OTASS-GG, aprueba la Directiva 002-2020-OTASS-UTI, Versión 03 “Directiva que regula la gestión de accesos y uso adecuado de los equipos y servicios informáticos en el Organismo Técnico de la Administración de los Servicios de Saneamiento.

III. ANTECEDENTES Y ALCANCE

El Plan de Recuperación de Servicios Informáticos se alinea al Plan de Continuidad Operativa 2023-2025 aprobada con RD 154-2023-OTASS-DE donde busca mantener y continuar la operación de las actividades críticas del OTASS ante un evento adverso que altere su normal, adecuado y oportuno funcionamiento.

En agosto del 2022, El Organismo Técnico de la Administración de los Servicios de Saneamiento experimentó un suceso critico que afecto los servicios de Tecnologías de la Información sin poder recuperarse en el tiempo ideal y en base a un documento normativo aprobado.

El Plan de Recuperación de Servicios Informáticos, contempla dentro del alcance, los servicios y sistemas informáticos que brindan soporte a las actividades críticas del OTASS, la infraestructura tecnológica en la que se soporta los servicios y sistemas informáticos y el centro de datos ubicado en el primer piso de la sede principal del OTASS. Y así mismo los sucesos críticos que afectan los servicios informáticos como el que ocurrió en agosto del 2022, interrumpiendo varios servicios de críticos de la Entidad.

Así mismo contempla actividades, roles y responsabilidades para gestionar riesgos, eventualidades, incidentes y/o situaciones de emergencia, que atenten contra el normal funcionamiento de los servicios y sistemas informáticos que soportan los procesos misionales del OTASS y estos aplicarse solo en los usuarios de la sede central del OTASS donde solo se pueda interrumpir sus actividades por un corto tiempo según la criticidad del evento adverso.

IV. DIAGNÓSTICO O CARACTERIZACIÓN DE LA PROBLEMÁTICA

El Perú en los últimos 500 años ha sido sacudida con altos niveles de intensidad con la ocurrencia de más de 35 sismos de magnitudes iguales o mayores a 7.5 MW, que generan diversos escenarios de destrucción y muerte en cada una de las diez regiones distribuidas a lo largo de la costa. Así como la pérdida total de Centro de datos de distintas Entidades del estado.

En la sede central del Organismo Técnico de la Administración de los Servicios de Saneamiento ha tenido varias perdidas de suministro de energía eléctrica el cual ha generado inoperatividad total de los servicios informáticos del OTASS.

El centro de datos del OTASS ha tenido algunas fallas técnicas el cual ha afectado la continuidad de los servicios informáticos, y donde por cada recuperación hubo tiempo demasiado extendido para poder regresar a la normalidad.

Es por todo lo mencionado previamente, el Plan de Recuperación de Servicios Informáticos que se implementaría en el OTASS, cobra un importante valor, por tratarse de un activo crítico que debemos mantener y recuperar su oportuno funcionamiento.

Es así que se ha identificado lo siguiente:

4.1 Problema

Existe el riesgo de que los servicios y sistemas informáticos queden inoperativos para atender las operaciones críticas del OTASS, a causa de un sismo de 8.8 MW, incendio, explosión, perdida de suministro eléctrico, ataque cibernético o falla de un componente de la infraestructura tecnológica del OTASS.

4.2 Población objetivo

Los usuarios del OTASS que hacen uso de los servicios informáticos identificados como críticos en el Plan Continuidad Operativa del OTASS.

4.3 Causas del problema identificado

a) Carencia de un centro datos de contingencia para el OTASS.

b) Limitada planificación para ejecutar las actividades ante un evento adverso que afecte los servicios informáticos del OTASS.

c) Limitado número de profesionales para la ejecución del Plan de Recuperación de Servicios Informáticos del OTASS.

d) Carencia de un generador energía eléctrica de contingencia para el centro de datos del OTASS.

V. ARTICULACIÓN CON EL PEI Y POI

De acuerdo a la revisión del Plan Estratégico Institucional – PEI 2023-2027 Ampliado del OTASS, aprobado mediante Resolución Directoral N° 000045-2024-OTASS/CD, el Plan de Recuperación de Servicios Informáticos, se encuentra articulado al objetivo OEI 04: Modernizar la Gestión Institucional, y la Acción Estratégica Institucional AEI 04.1: Esquemas de transformación digital y herramientas tecnológicas implementadas; así como al Plan Operativo, Institucional (POI) Anual 2024 Versión 1 del OTASS, aprobado mediante Resolución Directoral N° 000071-2024-OTASS-DE, en las siguientes actividades operativas: AOI00158900001 Elaboración de Procedimientos y/o Planes sobre Tecnologías de

la Información y AOI00158900145 Operatividad de la Infraestructura Tecnológica del OTASS. El detalle de muestra en la Tabla 1.

Tabla 1. Articulación con el PEI y POI del OTASS

Plan Estratégico Institucional 2023-2027 ampliado del OTASS		**Plan Operativo Institucional 2024**
Objetivo Estratégico Institucional	**Acción Estratégica Institucional**	**Actividades Operativas**
Objetivo Estratégico Institucional 04: Modernizar la Gestión institucional	AEI 04.1: Esquemas de transformación digital y herramientas tecnológicas implementadas	AOI00158900001 Elaboración de Procedimientos y/o Planes sobre Tecnologías de la Información
		AOI00158900145 Operatividad de la Infraestructura Tecnológica del OTASS

VI. MARCO TEÓRICO Y METODOLOGÍA

El Plan de Recuperación de Servicios Informáticos elaborado para OTASS toma como referencia la norma ISO:22301-2012 Sistemas de gestión de la continuidad de negocio y la norma ISO/IEC 27001:2022 Sistema de gestión de la seguridad de la información. La norma ISO:22301-2012, describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos para la mejora de la preparación de las TIC para garantizar la continuidad del negocio. La norma ISO/IEC 27001 es la norma internacional para la Gestión de Seguridad de la Información (ISO 27001) y considera la continuidad de negocio como un elemento clave dentro de la gestión de la seguridad de la información. Tiene como fin, contrarrestar interrupciones en las actividades empresariales y en los procesos críticos de negocio derivados de fallos importantes en los sistemas de información y garantizar su reanudación. Esta norma indica que crear un Sistema de Gestión de Seguridad de la Información SGSI es vital para preservar la Continuidad del Negocio.

El Análisis de Impacto del Negocio BIA (Bussiness Impact Analysis), permitirá identificar los procesos críticos de la entidad, analizar el impacto con relación a la continuidad del negocio y priorizar la recuperación de servicios o sistemas informáticos. Así también se debe determinar el tiempo de inactividad inaceptable y para ello se puede usar los siguientes indicadores MTD, RTO, RPO. El Tiempo

máximo de inactividad tolerable (MTD) representa la cantidad total de tiempo que el propietario del sistema está dispuesto a aceptar para una interrupción o interrupción del proceso de negocio e incluye todas las consideraciones de impacto. El tiempo objetivo de recuperación (RTO) define la cantidad máxima de tiempo que un recurso del sistema puede no estar disponible antes de que haya un impacto inaceptable en otros recursos del sistema, procesos de negocios compatibles y el MTD. El punto objetivo de recuperación (RPO) representa el punto en el tiempo, antes de una interrupción o interrupción del sistema, en el que se pueden recuperar los datos del proceso de negocio (dada la copia de seguridad más reciente de los datos) después de una interrupción.

En este apartado del plan se mencionará y describirá los planes a realizar, así como las actividades que se ejecutaran en el transcurso de todo el desarrollo del Plan de Recuperación de Servicios Informáticos del OTASS.

Así mismo, el uso del RTO, RPO y MTD en los tiempos de recuperación mínimo y máximo de los Servicios Informáticos del OTASS ante actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

6.1 Plan de Recuperación de los Servicios Informáticos

El Plan de Recuperación de los Servicios Informáticos permite minimizar las consecuencias en caso de la ocurrencia de incidentes o situaciones de emergencia, con el fin de reanudar las operaciones en el menor tiempo posible. Las acciones de recuperación de los servicios informáticos se organizan en tres grupos de actividades: i) Actividades de prevención y reducción, ii) Actividades de ejecución, iiii) Actividades de recuperación y retorno a la normalidad

i. Actividades de Prevención y Reducción

Es el conjunto de acciones y comprobaciones orientadas a prevenir la ocurrencia de incidentes no planificados o situaciones de emergencia, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo.

Las actividades de prevención son la parte principal del Plan de Recuperación de los Servicios Informáticos porque permiten aminorar y atenuar la probabilidad de ocurrencia.

ii. Actividades de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente no planificado o la situación de emergencia, y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro de los procedimientos de ejecución deben ser completamente claras y definidas de tal forma, que sean de conocimiento y

entendimiento inequívoco del personal involucrado en atender la recuperación de los servicios informáticos.

iii. Actividades de Recuperación y retorno a la normalidad

Es el conjunto de acciones que tiene por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un incidente no planificado o situación de emergencia.

6.2 Plan de Pruebas

El plan de pruebas es un conjunto de actividades y procedimientos diseñados para evaluar la capacidad de hacer frente a incidentes no planificados o situaciones de emergencia. Estas pruebas se llevan a cabo con el fin de identificar posibles debilidades en el Plan de Recuperación de los Servicios Informáticos y garantizar que las medidas de adoptadas sean efectivas en caso de un evento adverso. Se ejecutará en el mes de enero de forma anual, con el fin de evaluar la preparación del OTASS, ante la ocurrencia de un incidente no planificado o situación de emergencia que active el Plan, y realizar los ajustes necesarios.

6.3 Metodología

De acuerdo a la ISO 22301:2022 “Sistema de Continuidad de Negocio” se propone un conjunto de actividades agrupados en siete fases: i) Fase 1 Planificación, ii) Fase 2 Gestión de Riesgos, iii) Fase 3 Análisis de Impacto del Negocio (BIA), iv) Fase 4 Actividades a realizar para la recuperación de servicios informáticos críticos del OTASS, v) Fase 5 Definición y Ejecución del Plan de Pruebas, vi) Fase 6 Implementación del Plan de Recuperación de Servicios Informáticos y vii) Fase 7 Monitoreo.

6.3.1 Fase 1: Planificación

6.3.1.1 Organización

Para la ejecución del Plan de Recuperación de Servicios Informáticos del OTASS, se propone un equipo operativo que lidere la ejecución del Plan. La Tabla 2 muestra el cargo y rol de los integrantes del equipo en mención, el equipo está conformado exclusivamente por personal de la Unidad de Tecnologías de la Información.

Tabla 2. Equipo Operativo de Servicios Informáticos del OTASS

N°	CARGO	ROL
1	Jefe de la Unidad de Tecnologías de la Información	Líder de recuperación de servicios informáticos
2	Analista de Gestión de Servicios de Tecnologías de la Información	Coordinador de infraestructura y sistemas de comunicación
3	Desarrollador de Sistemas de Información	Coordinador de servicios y sistemas Informáticos
4	Especialista de seguridad de la información	Oficial de seguridad y confianza digital
5	Gestor de Base de Datos	Coordinador de base datos

6.3.1.2 Roles y responsabilidades

El Equipo Operativo de Servicios Informáticos del OTASS tendrá los siguientes roles:

a) Líder de Recuperación de Servicios Informáticos.

1) Es el canal de comunicación entre el equipo operativo de servicios informáticos cual se transmitirán las decisiones tomadas en torno a las acciones del Plan de Recuperación de los Servicios Informáticos del OTASS.

2) Informar a la Alta Dirección los avances, resultados y estrategias adoptadas durante la recuperación de Servicios Informáticos del OTASS.

3) Autorizar la activación y puesta en marcha del Plan de Recuperación de los Servicios Informáticos del OTASS.

4) Proveer liderazgo general al equipo operativo de servicios informáticos de personas involucradas en el proceso de recuperación.

5) Guiar al personal necesario durante la situación de emergencia y supervisa los avances en la recuperación de los servicios informáticos.

6) Asegurar la provisión de esquemas de recuperación de los servicios informáticos del OTASS.

7) Dirigir las pruebas de validación del Plan de Recuperación de Servicios Informáticos del OTASS.

b) Coordinador de Infraestructura Tecnológica y Sistemas de Comunicación.

1) Informar al Líder de Recuperación de Servicios Informáticos, el estado, impacto, actividades y tiempos de recuperación durante la ocurrencia de incidentes o situaciones de emergencia.

2) Dirigir y coordinar la respuesta y recuperación de las plataformas que soportan los servicios informáticos del OTASS.

3) Mantener actualizado el inventario los equipos que conforman el Centro de datos tales como UPS, servidores, equipos de almacenamiento, switches, firewall y Router.

4) Revisar periódicamente los esquemas de recuperación de los servicios informáticos.

5) Coordinar con los proveedores del Centro Datos el mantenimiento y soporte en caso de ocurrencia de incidentes o situaciones de emergencia.

6) Monitorear la red y definir las medidas preventivas para minimizar y/o reducir las consecuencias en caso de la ocurrencia de incidentes y/o situaciones de emergencia.

7) Coordinar y supervisar que se cumplan en forma apropiada y completar los procedimientos de respaldo de los sistemas informáticos.

8) Asegurar que los respaldos de la información sean enviados fuera de la Institución como medida de seguridad.

9) Participar en las pruebas del Plan de Recuperación de Servicios Informáticos.

c) Coordinador de Servicios y Sistemas Informáticos.

1) Informar al Líder de Recuperación de Servicios Informáticos, el estatus, impacto, actividades y tiempos de recuperación de los servicios informáticos durante la ocurrencia de incidentes o situaciones de emergencia.

2) Mantener actualizado el inventario de las servicios y sistemas informáticos.

3) Mantener actualizado el repositorio de código fuente de los sistemas informáticos.

4) Mantener actualizada la documentación técnica de despliegue y/o puesta en producción de los servicios y sistemas informáticos.

5) Coordinar la recuperación de los servicios y sistemas informáticos con el Equipo de Infraestructura Tecnológica.

6) Implementar con el coordinador de infraestructura tecnológica y sistemas de comunicación los esquemas y/o procedimientos que faciliten la resolución de incidentes.

7) Participar en las pruebas del Plan de Recuperación de Servicios Informáticos.

8) Verificar el correcto funcionamiento de los servicios y sistemas informáticos durante y después de la ocurrencia de incidentes o situaciones de emergencia.

9) Coordinar e interactuar con los proveedores que brindan soporte a los servicios y sistemas informáticos.

d) Oficial de Seguridad y Confianza Digital.

1) Propiciar la aplicación metodológica del Plan de Recuperación de los Servicios Informáticos del OTASS.

2) Coordinar, supervisar y controlar las labores de ejecución del Plan de Recuperación de los Servicios Informáticos del OTASS.

3) Coordinar las pruebas de recuperación de los sistemas y servicios informáticos del OTASS.

4) Durante las pruebas tiene el rol de veedor y/o auditor de las pruebas de recuperación tecnológica, emite observaciones y revisa los informes de cada prueba realizada.

5) Propiciar las capacitaciones y entrenamientos internos a los distintos equipos de recuperación de los sistemas y servicios informáticos, con respecto a temas de continuidad y recuperación tecnológica.

6) Elaborar y emitir el informe final con el resultado de las pruebas, sus conclusiones y recomendaciones.

7) Dirigir la definición de los riesgos del plan.

e) Coordinador de Base de Datos

1) Evaluar los daños causados al entorno de la base de datos durante el incidente. Esto implica determinar el alcance de los datos perdidos o dañados, identificar cualquier problema de integridad de los datos y evaluar el impacto en la disponibilidad y el rendimiento del sistema.

2) Inventario actualizado de las bases de datos de los sistemas y servicios informáticos.

3) Información actualizada de las bases de datos de los sistemas y servicios informáticos.

4) Coordinar y llevar a cabo la restauración de los datos afectados. Esto puede implicar la recuperación de datos desde respaldos válidos, la reconstrucción de datos perdidos o dañados, y la implementación de medidas para garantizar la consistencia y la integridad de los datos restaurados.

5) Colaborar con el equipo operativo de servicios informáticos para resolver cualquier problema relacionado con la base de datos que surja como

resultado del incidente. Esto puede incluir la resolución de problemas de rendimiento, la optimización de consultas, la reparación de daños en la estructura de la base de datos y la implementación de medidas para prevenir futuros incidentes similares.

6) Realizar un análisis después del incidente para identificar las causas subyacentes del incidente y recomendar medidas preventivas para evitar que vuelva a ocurrir en el futuro.

7) Comunicar de manera efectiva con el equipo operativo de servicios informáticos sobre el estado de la recuperación de la base de datos, las acciones tomadas para resolver el incidente y las medidas preventivas implementadas para evitar incidentes futuros.

6.3.2 Fase 2: Gestión de Riesgos

6.3.2.1 Registros Vitales

Dentro de la estrategia de un esquema de recuperación, existen tres pilares básicos indispensables, siendo estos: Una sólida estructura organizacional (Personas), Planes y procedimientos documentados y los registros vitales.

Los registros vitales constituyen la información y data crítica que la Entidad necesita resguardar y recuperar en caso ocurra un incidente crítico que afecte la disponibilidad de los servicios informáticos.

Los registros vitales se pueden encontrar en formato electrónico o impreso, esta clasificación permitirá asignar los controles de seguridad necesarios para su respaldo, custodia y recuperación en una situación de indisponibilidad de los servicios informáticos.

Los registros vitales por buenas prácticas son respaldados regularmente en medios externos (cintas, discos externos, solución en la nube). El OTASS ha identificado cuatro registros vitales que se detallan en la Tabla 3.

Tabla 3. Registros Vitales de OTASS.

N°	REGISTROS VITALES	DESCRIPCIÓN
1	Bases de Datos	Esquemas, tablas e información almacenada en la Base de Datos.
2	Servidores	Información de los sistemas que se almacena en los servidores,
3	Archivos de Configuración	Archivos que contienen la configuración de los servidores, lo cual se necesita para que funcionen adecuadamente,
4	Fuentes	Código fuente, librerías, documentación, etc.

La frecuencia de respaldo de los registros vitales del OTASS debe obedecer a los requerimientos y necesidades de la Entidad, requisitos de seguridad de la información y la criticidad de la información para la continuidad de los servicios informáticos.

Los respaldos de los registros vitales deben estar ubicados y almacenados en un local remoto y a distancia suficiente para evitar los daños colaterales ante la ocurrencia de un evento o peligro.

Los registros vitales deben probarse regularmente para asegurar su integridad y fiabilidad en caso de desastre.

6.3.2.2 Identificación de recursos y/o servicios informáticos críticos

La Tabla 4 presenta las actividades críticas de los órganos del OTASS definidas en el Plan de Continuidad Operativa y se asocia con los servicios y sistemas informáticos que brinda la UTI.

Tabla 4. Actividades críticas identificados

N°	ÓRGANO O UNIDADES CRÍTICAS	ACTIVIDADES CRÍTICAS	SERVICIO INFORMÁTICO
1	Dirección de Gestión y Financiamiento	1. Gestionar las transferencias para el fortalecimiento de las capacidades de las empresas prestadoras. 2. Determinar los bienes y servicios necesarios para fortalecer las capacidades de las empresas prestadoras.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. O-Transfer 3. SIGA 4. SIAF 5. Correo Electrónico 6. Herramientas colaborativas 7. Servicio Internet
2	Dirección de Operaciones	1. Ejecutar las transferencias identificadas por la Dirección de Gestión y Financiamiento. 2. Brindar asistencia técnica a las empresas prestadoras de servicios de saneamiento y seguimiento. 3. Coordinar la continuidad de la ejecución de las estrategias y actividades que se encuentren en ejecución a la fecha de ocurrencia del evento.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. O-Transfer 3. SIGA 4. SIAF 5. O-ALCANTERNA 6. O-CARTOGRAFÍA 7. Correo Electrónico 8. Herramientas colaborativas 9. Servicio Internet
3	Dirección de Monitoreo y Evaluación	1.Monitorear las transferencias financieras para garantizar la prestación de los servicios de saneamiento. Priorizando las EPS en Emergencia de corresponder. 2. Monitorear la asistencia con las estrategias o actividades del OTASS, priorizando las que cuente con maquinarias, equipos y/o vehículos.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. SIGA 3. SIAF 4. Correo Electrónico 5. Herramientas colaborativas 6. Servicio Internet

N°	ÓRGANO O UNIDADES CRÍTICAS	ACTIVIDADES CRÍTICAS	SERVICIO INFORMÁTICO
4	Dirección de Integración	1. Realizar transferencias financieras y asistencia técnica a prestadores que se encuentren en procesos de integración a la fecha de ocurrencia del evento; o en integración territorial, de procesos o de sistemas.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. SIGA 3. SIAF 4. Correo Electrónico 5. Servicio Internet
5	Oficina de Planeamiento y Presupuesto	1. Aprobación de solicitudes de certificación presupuestales y modificación presupuestaria para la atención de las actividades críticas. 2. Formular y/o emitir opinión técnica para asignación presupuestal a través de Decretos Supremos, Decretos de Urgencia y otros mecanismos. Así como la formulación de documentos normativos que permitan la implementación de las disposiciones establecidas en los decretos de urgencia de corresponder.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. SIGA 3. SIAF 4. Correo Electrónico 5. Servicio Internet
6	Oficina de Gestión Social y Comunicaciones	1. Garantizar las comunicaciones, en las diferentes plataformas de comunicación, para dar a conocer las acciones que desarrolla el OTASS durante el evento, además de las actividades críticas con los prestadores de los servicios de saneamiento.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. SIGA 3. SIAF 4. Correo Electrónico 5. Herramientas colaborativas 6. Servicio Internet
7	Unidad de Recursos Humanos	1. Recopilar y elaborar reporte de la situación del personal del OTASS. 2. Coordinar el trabajo presencial y/o remoto. 3. Gestionar el pago de planilla. 4. Activar el seguro contra todo riesgo de ser necesario.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. SIGA 3. SIAF 4. E-STATAL 5. Correo Electrónico 6. Herramientas colaborativas 7. Servicio Internet
8	Unidad de Abastecimiento	1. Solicitar un informe sobre el estado de la estructura del edificio y las oficinas para determinar la modalidad de trabajo y uso de sede alterna. 2. Acondicionar los espacios de trabajo e instalar de ser necesario SSHH portátiles. 3. Abastecer de agua y adquirir o contratar grupo electrógeno y todo material necesario para instalaciones. 4. Brindar seguridad y vigilancia en la nueva sede. 5. Salvaguardar los bienes patrimoniales y de Almacén. 6. Priorizar contrataciones urgentes y necesarias.	1. Sistema de Gestión Documental del OTASS – O Documentos 2. O-Transfer 3. SIGA 4. SIAF 5. Correo Electrónico 6. Herramientas colaborativas 7. Servicio Internet

N°	ÓRGANO O UNIDADES CRÍTICAS	ACTIVIDADES CRÍTICAS	SERVICIO INFORMÁTICO
9	Unidad de Tecnologías de la Información	1. Identificar los componentes críticos de la infraestructura tecnológica del OTASS, como servidores, equipos de red y sistemas de almacenamiento, entre otros; evaluar los daños sufridos y determinar su estado de funcionamiento. 2. Restaurar los datos críticos a partir de los respaldos realizados previamente (Copia de seguridad custodiada externamente). 3. Restaurar la infraestructura de servidores. 4. Validar la integridad de los datos restaurados y realizar pruebas para garantizar su precisión y disponibilidad. 5. Restablecer las conexiones de red y comunicaciones internas y externas de la entidad. 6. Configurar y poner en funcionamiento los elementos de red necesarios, como routers, Switches y firewalls. 7. Verificar que los sistemas de información del OTASS se encuentren operativos y en correcto funcionamiento. 8. Verificar que los sistemas de seguridad y protección de datos estén en funcionamiento. 9. Restauración de equipos.	1. Servicio Internet 2. Plataforma de virtualización de servidores 3. Software de respaldo 4. Software de monitoreo

La Tabla 5 muestra un resumen de los servicios informáticos que soportan las actividades críticas. Estos servicios informáticos fueron identificados por el equipo de recuperación de servicios informáticos del OTASS:

Tabla 5. Servicios críticos identificados

N°	SERVICIO INFORMÁTICO CRÍTICO	NOMBRE CORTO
1	Sistema de Gestión Documental del OTASS	O-DOCUMENTOS
2	Sistema O-Transfer	O-TRANSFER
3	Sistema O-ALCANTERNA	O-ALCANTERNA
4	Sistema O-CARTOGRAFÍA	O-CARTOGRAFÍA
5	Sistema Integrado de Administración Financiera - SIAF	SIAF
6	Sistema Integrado de Gestión Administrativa - SIGA	SIGA
7	Sistema E-STATAL	E-STATAL
8	Correo Electrónico (*)	Correo
9	Herramientas colaborativas (*)	Google-Apps
10	Servicio de Internet (*)	Internet

11	Plataforma de virtualización de servidores	Virtualización servidores
12	Software de respaldo	Sistema de respaldo
13	Software de monitoreo	Monitoreo

(*) Dependen de un proveedor externo

6.3.2.3 Identificación de escenarios de riesgos

El Plan de Continuidad Operativa del OTASS, establece un conjunto de peligros que afectarían la continuidad operativa del OTASS, como son: Sismo >=8.8 MW, Pandemia o Epidemia, Incendio, Explosión o Sabotaje. La ocurrencia de uno de estos peligros o situaciones de emergencia, afectarían la operatividad de la infraestructura tecnológica de la entidad, lo que generaría la indisponibilidad de los servicios informáticos por tiempo indeterminado.

Como resultado de un análisis realizado por el equipo de recuperación de servicios informáticos del OTASS, se identificó tres escenarios de riesgo, lo que genera la necesidad de evaluar el riesgo, así como las causas y los efectos sobre las actividades críticas de la Entidad. A partir de ello se establecen procedimientos para la recuperación de los servicios informáticos identificados como críticos. Los escenarios de riesgo identificados son:

a) **Escenario**: Pérdida total del Centro de datos debido a un Sismo >=8.8 MW, Incendio o Explosión.

b) **Escenario**: Inoperatividad total de los servicios informáticos alojados en el centro de datos debido a la pérdida de suministro de energía eléctrica.

c) **Escenario:** Indisponibilidad parcial o total de los servicios informáticos debido a un ataque cibernético o falla de la infraestructura tecnológica que se encuentran dentro del centro de datos.

6.3.2.4 Análisis de riesgos de los escenarios

La Tabla 6 presenta un análisis de tres (03) escenarios de riesgo describiendo el riesgo, analizando las causas, y los efectos sobre las actividades y/u operaciones de la entidad identificadas como críticas.

Tabla 6. Escenarios de Riesgos

N°	ESCENARIO DE RIESGO	RIESGO	CAUSAS	EFECTOS
1	Pérdida total del Centro de datos debido a un Sismo >=8.8 MW, Incendio o Explosión	No se puede ingresar al centro de datos, y no se tiene acceso parcial o total a los activos que se encuentran dentro del centro de datos	1.Incendio no controlado 2.Sismo de gran magnitud. 3. Explosión.	Interrupción de las operaciones y/o actividades de los procesos críticos que dependen de los servicios informáticos
2	Inoperatividad total de los servicios informáticos alojados en el centro de datos debido a la pérdida de suministro de energía eléctrica	No se tiene acceso a los servicios informáticos que soportan las actividades críticas de la entidad	1. Corte de energía de parte de la empresa de energía eléctrica. 2. Fallas en el suministro eléctrico 3.Ausencia de un sistema de respaldo eléctrico.	Interrupción de las operaciones y/o actividades de los procesos críticos que dependen de los servicios informáticos
3	Indisponibilidad parcial o total de los servicios informáticos debido a un ataque cibernético o falla de la infraestructura tecnológica que se encuentran dentro del centro de datos	No se cuenta con servicios informáticos que brindan soporte a las operaciones críticas de la entidad	1. Ataque cibernético. 2. Falla de equipos de procesamiento y/o almacenamiento de información. 3. Falla de los equipos de comunicación y seguridad perimetral. 4. Falla de los servicios base de los sistemas informáticos. 5. Interrupción del servicio de Internet. 6. Interrupción del servicio de correo electrónico. 7. Falla en el sistema de seguridad lógica. 8. Falla en las plataformas y servicios de información externo. 9. Indisponibilidad de servicios externos contratados.	Interrupción parcial o total de las operaciones y/o actividades de los procesos críticos que dependen de los servicios informáticos

6.3.2.5 Evaluación de riesgos de los escenarios

Luego de haber identificado los posibles tres (03) escenarios de riesgo, procedemos a establecer la valoración a base de la probabilidad de ocurrencia y su impacto.

Probabilidad: Se establece los niveles de probabilidad de acuerdo a los casos presentados en el año, para cada escenario, siendo de nivel alto aquellos que tienen más de 8 casos al año o más de un caso al mes. El detalle de la evaluación se presenta en la Tabla 7.

Impacto: Se establece los niveles de impacto de acuerdo a la interrupción de la operación de uno o varios procesos de la Entidad, siendo de nivel alto, aquél que podría afectar a más de 8 procesos de la Entidad. El detalle de la Evaluación se presenta en la Tabla 8.

Tabla 7. Probabilidad

N°	DETALLE	NIVEL
1	Se podría presentar de 1 a 3 casos al año	Bajo
2	Se podría presentar de 4 a 7 casos al año	Medio
3	Se podría presentar más de 8 casos al año o más de un caso al mes	Alto

Tabla 8. Impacto

N°	DETALLE	NIVEL
1	Podría afectar de 1 a 2 actividades críticas de la Entidad	Bajo
2	Podría afectar de 3 a 4 actividades críticas de la Entidad	Medio
3	Podría afectar a más de 5 actividades críticas de la Entidad	Alto

La Tabla 9 presenta un mapa de riesgos, el mapa en mención permitirá evaluar de forma combinada la probabilidad de ocurrencia de un escenario de riesgo y el impacto negativo que el mismo escenario puede ocasionar en las actividades críticas de la entidad.

Tabla 9. Mapa de Riesgos

P3	**MEDIO**	**ALTO**	**ALTO**
P2	**BAJO**	**MEDIO**	**ALTO**
P1	**BAJO**	**BAJO**	**MEDIO**
	I1	**I2**	**I3**

La Tabla 10, presenta la evaluación del riesgo cada escenario. La valoración de cada escenario de riesgo se realizó de acuerdo a los niveles de probabilidad e impacto establecidos en la Tabla 7 y Tabla 8 respectivamente. Para determinar el nivel de riesgo cada escenario de riesgo se utilizó el mapa de riesgos establecido en la Tabla 9.

Tabla 10. Evaluación de Riesgos

Nº	ESCENARIO DE RIESGO	CLASIFICACIÓN		VALORACIÓN DEL RIESGO				
		FACTOR DE RIESGO	TIPO DE EVENTO	DESC. PROB.	NIVEL PROB.	DESC. IMPACTO	NIVEL IMPACTO	NIVEL RIESGO
1	Pérdida total del Centro de datos debido a un Sismo >=8.8 MW, Incendio o Explosión	Eventos externos	Daños irreparables de los activos que conforman el Centro Datos	Medio	P2	Alto	I3	**Alto**
2	Inoperatividad total de los servicios informáticos alojados en el centro de datos debido a la pérdida de suministro de energía eléctrica	Eventos externos Tecnología (*)	Interrupción de los servicios informáticos .	Bajo	P1	Alto	I3	**Medio**
3	Indisponibilidad parcial o total de los servicios informáticos debido a un ataque cibernético o falla de la infraestructura tecnológica que se encuentran dentro del centro de datos	Tecnología	Interrupción del Negocio / fallo en los servicios informáticos	Alto	P3	Alto	I3	**Alto**

(*) Es importante indicar que para el año 2024 el riesgo se ha reducido debido a la implementación una línea eléctrica de respaldo para el Centro de datos.

Luego de evaluar los resultados de la Tabla 10, para el presente plan se considerará únicamente los escenarios con nivel de riesgo alto. Estos escenarios son: i) Pérdida total del Centro de datos debido a un Sismo >=8.8 MW, Incendio o Explosión, y ii) Indisponibilidad parcial o total de los servicios informáticos debido a un ataque cibernético o falla de la infraestructura tecnológica que se encuentran dentro del centro de datos.

6.3.3 Fase 3: Análisis de Impacto del Negocio (BIA)

Durante esta fase se elaboró el análisis de impacto de negocio BIA, identificado los tiempos RTO, RPO y MTD para cada servicio informático crítico, en base a la opinión de expertos de la UTI. El resultado de los tiempos se detalla en la Tabla 11.

Tabla 11. RPO, RTO y MTD de los servicios informáticos críticos

N°	SERVICIO INFORMÁTICO CRÍTICO	RTO	RPO	MTD
1	Sistema de Gestión Documental del OTASS – O Documentos	48h	48h	48h
2	Sistema O-TRANSFER	48h	48h	48h
3	Sistema O-ALCANTERNA	4h	48h	24h
4	Sistema O-CARTOGRAFÍA	4h	48h	24h
5	Sistema Integrado de Administración Financiera - SIAF	4h	48h	24h
6	Sistema Integrado de Gestión Administrativa - SIGA	4h	48h	24h
7	Sistema E-STATAL	4h	48h	24h
8	Correo Electrónico (*)	4h	24h	8h
9	Herramientas colaborativas (*)	4h	24h	8h
10	Servicio de Internet (*)	8h	-	8h
11	Plataforma de virtualización de servidores	24h	48h	48h
12	Software de respaldo	24h	48h	48h
13	Software de monitoreo	8h	-	48h

(*) Dependen de un proveedor externo

6.3.4 Fase 4: Actividades a realizar para la recuperación de servicios informáticos críticos del OTASS

A continuación, se presentan las actividades de prevención y reducción, de ejecución y de recuperación y retorno a la normalidad a realizar, para la recuperación de servicios informáticos críticos del OTASS, de acuerdo a los escenarios identificados:

6.3.4.1 Escenario 1: Pérdida total del Centro de datos debido a un Sismo >=8.8 MW, Incendio o Explosión

Objetivo: Establecer las acciones que se ejecutarán a fin de restaurar la operatividad de los servicios informáticos críticos del Centro de datos del OTASS.

a) Actividades de prevención y reducción

1) Disponer del Directorio de empresas proveedoras de recursos y servicios informáticos del OTASS del Anexo 1: Directorio de empresas proveedoras de recursos y servicios informáticos del OTASS.

2) Disponer del Directorio de empresas proveedoras de emergencia del Anexo 2: Directorio de empresas proveedoras de emergencia.

3) Mantener actualizados los procedimientos e instructivos de recuperación de servicios informáticos.

4) Disponer en la sede alterna establecida en el PCO del OTASS, del equipamiento informático necesario.

5) Obtener acceso al servicio “IaaS o infraestructura como servicio” de la Plataforma Nacional de Gobierno Digital – PNGD, para contar con un Centro de datos alterno ubicado en la nube privada administrada por el Estado.

6) Instalar en la Plataforma Nacional de Gobierno Digital, el software necesario y realizar las configuraciones que correspondan para tener una réplica de nuestra plataforma de servidores del OTASS.

7) Realizar los respaldos de información, de acuerdo a la programación establecida, y tener al menos una copia de seguridad almacenada fuera del sitio o en la nube.

8) Tener un servicio contratado de traslado y custodia de cintas magnéticas que contienen las copias de respaldo de la información del OTASS.

9) Disponer de un servicio de internet en la sede alterna establecida en el PCO del OTASS.

b) Actividades de ejecución

1) Verificar el estado de los componentes del Centro de datos y la operatividad del Centro de datos, y determinar que el todo el Centro de datos no se encuentra operativo y tampoco disponible.

2) Activar el Plan de Recuperación de Servicios Informáticos.

3) Solicitar a la empresa de traslado y custodia de cintas magnéticas, el traslado de las cintas que se requieren.

4) Habilitar el servicio de internet contratado en la sede alterna establecida en el PCO del OTASS.

5) Habilitar equipos de comunicaciones en la sede alterna establecida en el PCO del OTASS.

6) Verificar que el correo electrónico y herramientas colaborativas de la Entidad se encuentren operativos.

7) Acceder a la Plataforma Nacional de Gobierno Digital – PNGD, y restaurar la información, a partir de las copias de respaldo.

8) Habilitar los servicios informáticos críticos del OTASS, de acuerdo al Anexo 10: Habilitación de los servicios informáticos críticos, considerando los RPO, RTO y MTD definidos en la Tabla 11.

c) Actividades de recuperación y retorno a la normalidad

1) Verificar que los servicios informáticos críticos se encuentren funcionando de forma correcta en la Plataforma Nacional de Gobierno Digital – PNGD. Para ello se hará uso de los siguientes Anexos:

   ANEXO 11: Verificación de la Operatividad del SIGA del OTASS.

   ANEXO 12: Verificación de la Operatividad del SIAF del OTASS.

   ANEXO 13: Verificación del Sistema de Gestión Documental O-Documentos.

   ANEXO 14: Verificación del Sistema O-Transfer del OTASS.

   ANEXO 15: Verificación de los Servicios GIS de la Plataforma GIS Corporativa.

   ANEXO 16: Verificación del Sistema E-STATAL

   ANEXO 17: Verificación del Software de Monitoreo del OTASS.

2) Comunicar a la Alta Dirección, que los servicios informáticos críticos se encuentran operativos desde la Plataforma Nacional de Gobierno Digital – PNGD.

3) Comunicar a los usuarios del Centro de datos alterno del OTASS, que los servicios informáticos críticos se encuentran operativos desde la Plataforma Nacional de Gobierno Digital – PNGD.

4) Emitir un informe con el detalle de todo lo realizado, detallando las razones que lo ocasionaron, las actividades realizadas y las lecciones aprendidas.

6.3.4.2 Escenario 2: Indisponibilidad parcial o total de los servicios informáticos de la Entidad debido a un ataque cibernético o falla de la infraestructura tecnológica que se encuentran dentro del centro de datos

Objetivo: Establecer las acciones que se ejecutarán a fin de mantener operativos los servicios informáticos de la Entidad.

a) Actividades de prevención y reducción

1) Disponer del Directorio de empresas proveedoras de recursos y servicios informáticos del OTASS del Anexo 4: Directorio de empresas proveedoras de recursos y servicios informáticos del OTASS.

2) Mantener actualizados los procedimientos e instructivos de recuperación de servicios informáticos.

3) Ejecutar de forma regular, el mantenimiento preventivo de los servidores del OTASS.

4) Realizar los respaldos de información, de acuerdo a la programación establecida; y establecer como estrategia, la regla de las copias de seguridad 3-2-1 la cual indica tener al menos tres copias, dos de ellas se almacenan en diferentes tipos de medios, y al menos una copia de seguridad se almacena fuera del sitio o en la nube.

5) Actualizar los parches de seguridad del sistema operativo de los servidores, de forma mensual.

6) Realizar periódicamente análisis de vulnerabilidades a los servidores del OTASS.

7) Disponer de una herramienta de monitoreo que reporte el estado de los servidores, equipos de comunicaciones, aplicaciones, servicios y tráfico en la red.

b) Actividades de ejecución

<u>Indisponibilidad Total de los servicios informáticos críticos del OTASS</u>

1) Verificar la disponibilidad de cada uno de los servicios informáticos críticos del OTASS y determinar que todos los servicios informáticos críticos no están disponibles.

2) Activar el Plan de Recuperación de Servicios Informáticos.

3) Verificar que el servicio de internet, correo electrónico y herramientas colaborativas de la Entidad se encuentren operativos.

4) Identificar el motivo de la inoperatividad total de los servicios informáticos críticos.

5) Si el motivo es debido a un corte de energía eléctrica, lo comunicará a la Unidad de Abastecimiento, y una vez restablecida la energía eléctrica en el centro de datos, se procede a realizar lo indicado en el Anexo 6: Procedimiento de restablecimiento de energía eléctrica del Centro de datos.

6) Si el motivo es debido a fallas o problemas técnicos con los equipos de comunicaciones del Centro de datos, el coordinador de infraestructura y sistemas de comunicación verificará inicialmente el equipo para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del equipo. Finalmente realizar el encendido de los equipos

de comunicaciones del Centro de datos, de acuerdo al Anexo 7: Procedimiento de encendido de los equipos de comunicaciones del Centro de datos.

7) Si el motivo es debido a fallas o problemas técnicos con los servidores y almacenamiento, el coordinador de infraestructura y sistemas de comunicación verificará inicialmente el equipo para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del equipo. Finalmente realizar el encendido de los servidores y almacenamiento, de acuerdo al Anexo 8: Procedimiento de encendido de los servidores y almacenamiento.

8) Si el motivo es debido a denegación de servicios por ataque informático, el coordinador de infraestructura y sistemas de comunicación realizará un primer diagnóstico de lo que ocurre y de requerirse, deberá restaurar información a partir de las copias de respaldo, las cuáles se obtienen del equipo de Backup ubicado en el centro de datos. De considerarlo necesario, solicitar a la empresa de traslado y custodia de cintas magnéticas, el traslado de las cintas que se requieren. Luego, acceder a los servidores físicos del Centro de datos, instalar el software necesario y realizar las configuraciones que correspondan para restablecer la plataforma de virtualización de los servidores del OTASS, a partir de las copias de respaldo.

9) Habilitar los servicios informáticos críticos del OTASS, considerando los RPO, RTO y MTD definidos en la Tabla 10, de acuerdo al Anexo 10: Procedimiento de habilitación de los servicios informáticos críticos.

<u>Indisponibilidad Parcial de los servicios informáticos críticos del OTASS</u>

1) Verificar la disponibilidad de cada uno de los servicios informáticos críticos del OTASS y determinar qué servicio(s) informático(s) crítico(s) no está(n) disponible(s).

2) Activar el Plan de Recuperación de Servicios Informáticos.

3) Si el motivo es debido a fallas o problemas técnicos con la infraestructura Oracle, el coordinador de base datos verificará inicialmente el equipo para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del equipo. Finalmente realizar el encendido de la

infraestructura Oracle, de acuerdo al Anexo 9: Procedimiento de encendido de la infraestructura Oracle.

4) Si el motivo es debido a fallas o problemas técnicos en la operatividad del SIGA, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el SIGA, la base de datos y los servicios para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución, el coordinador de infraestructura y sistemas de comunicación indicará al administrador del SIGA del OTASS, que se comunique con el residente del MEF para indicarle lo encontrado y a partir de ahí, realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del sistema.

5) Si el motivo es debido a fallas o problemas técnicos en la operatividad del SIAF, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el SIAF, la base de datos y los servicios para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución, el coordinador de infraestructura y sistemas de comunicación indicará al administrador del SIAF del OTASS, que se comunique con el residente del MEF para indicarle lo encontrado y a partir de ahí, realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del sistema.

6) Si el motivo es debido a fallas o problemas técnicos en la operatividad del Sistema de Gestión Documental - O Documentos, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el Sistema de Gestión Documental - O Documentos, la base de datos y los servicios para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del Sistema de Gestión Documental - O Documentos.

7) Si el motivo es debido a fallas o problemas técnicos en la operatividad del Sistema O-Transfer, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el Sistema O-Transfer, la base de datos y los servicios para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del Sistema O-Transfer.

8) Si el motivo es debido a fallas o problemas técnicos en la operatividad de los Servicios GIS de la Plataforma GIS Corporativa, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena los Servicios GIS de la Plataforma GIS Corporativa, la base de datos para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total de los Servicios GIS de la Plataforma GIS Corporativa.

9) Si el motivo es debido a fallas o problemas técnicos en la operatividad del Sistema E-STATAL, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el Sistema E-STATAL, la base de datos y los servicios para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del Sistema E-STATAL.

10) Si el motivo es debido a fallas o problemas técnicos en la operatividad del Software de Monitoreo del OTASS, el coordinador de infraestructura y sistemas de comunicación verificará el equipo donde se almacena el Software de Monitoreo del OTASS para realizar un primer diagnóstico de lo que ocurre, y de ser posible, solucionará el problema. En caso no se encuentre la solución de forma rápida se comunicará con el proveedor para indicarle lo encontrado y a partir de ahí, el proveedor realice un diagnóstico más profundo, indicando el motivo de la falla y brinde solución al problema. Se deberá hacer seguimiento hasta la operatividad total del Software de Monitoreo del OTASS.

11) Habilitar el (los) servicio(s) informático(s) crítico(s) afectado(s), considerando los RPO, RTO y MTD definidos en la Tabla 11, de acuerdo al Anexo 10: Procedimiento de habilitación de los servicios informáticos críticos.

c) Actividades de recuperación y retorno a la normalidad

<u>Indisponibilidad Total de los servicios informáticos críticos del OTASS</u>

1) Verificar que los servicios informáticos se encuentren funcionando de forma correcta. Para ello se hará uso de los siguientes Anexos:

   ANEXO 11: Procedimiento de verificación de la Operatividad del SIGA.

   ANEXO 12: Procedimiento de verificación de la Operatividad del SIAF.

ANEXO 13: Procedimiento de verificación del Sistema de Gestión Documental - O Documentos.

ANEXO 14: Procedimiento de verificación del Sistema O-Transfer.

ANEXO 15: Procedimiento de verificación de los Servicios GIS de la Plataforma GIS Corporativa.

ANEXO 16: Procedimiento de verificación del Sistema E-STATAL.

ANEXO 17: Procedimiento de verificación del Software de Monitoreo del OTASS.

2) Comunicar por los medios establecidos a los usuarios del OTASS, que los servicios informáticos críticos se encuentran operativos.

3) Emitir un informe con el incidente ocurrido, detallando las razones que lo ocasionaron, las actividades realizadas y las lecciones aprendidas.

Indisponibilidad Parcial de los servicios informáticos críticos del OTASS

1) Verificar que el (los) servicio(s) informático(s) crítico(s) se encuentra(n) operativo(s). Para ello se hará uso de alguno de los siguientes Anexos:

ANEXO 11: Procedimiento de verificación de la Operatividad del SIGA.

ANEXO 12: Procedimiento de verificación de la Operatividad del SIAF.

ANEXO 13: Procedimiento de verificación del Sistema de Gestión Documental - O Documentos.

ANEXO 14: Procedimiento de verificación del Sistema O-Transfer.

ANEXO 15: Procedimiento de verificación de los Servicios GIS de la Plataforma GIS Corporativa.

ANEXO 16: Procedimiento de verificación del Sistema E-STATAL.

ANEXO 17: Procedimiento de verificación del Software de Monitoreo del OTASS.

2) Comunicar por los medios establecidos a los usuarios del OTASS, que el (los) servicio(s) informático(s) crítico(s) se encuentra(n) operativo(s).

3) Emitir un informe con el incidente ocurrido, detallando las razones que lo ocasionaron, las actividades realizadas y las lecciones aprendidas.

6.3.5 Fase 5: Definición y Ejecución del Plan de Pruebas

El plan de pruebas está enfocado a simular situaciones de recuperación de servicios informáticos, de acuerdo a los escenarios de pruebas definidos, en caso de incidencias producidas sobre equipos, información y procesos, manejados en

situaciones reales y cuyos respaldos pueden ser empleados y replicados en una hipotética situación de emergencia.

Se diseñará un conjunto de casos de pruebas funcionales, que serán realizados por el personal de la UTI, el cual probará, verificará y observará cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el Plan de Pruebas.

El Plan de Pruebas tendrá la siguiente estructura:

a) Título de la prueba

b) Objetivo

c) Servicio informático

d) Descripción de la prueba a efectuarse.

e) Áreas afectadas / personal involucrado.

f) Resultados esperados.

Las pruebas se deberán realizar al menos una vez por semestre, en los meses de junio y noviembre, con el fin de evaluar la preparación de la Entidad, ante la ocurrencia de incidentes no planificados o situaciones de emergencia y realizar los ajustes necesarios.

6.3.6 Fase 6: Implementación del Plan de Recuperación de Servicios Informáticos

La implementación del presente Plan se realizará luego de su aprobación y estará dirigido por el Oficial de Seguridad y Confianza Digital del OTASS quien realizará las siguientes actividades:

a) Revisar y supervisar el cumplimiento de las actividades de prevención y reducción.

b) Establecer procedimientos de seguridad en los escenarios en los cuáles pueden ocurrir los problemas y que generan la necesidad de recuperación de los servicios informáticos del OTASS.

c) Definir, Planificar y ejecutar el plan de pruebas.

d) Participar en las pruebas y simulacros de desastres.

6.3.7 Fase 7: Monitoreo

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Cada vez que se realice un cambio en la infraestructura tecnológica, debemos de realizar la actualización respectiva.

a) A continuación, se enumeran las actividades principales a realizar:

b) Actualización permanente de la documentación del Plan.

c) Revisión del sistema de copias de respaldo.

d) Actualización de procedimientos para encendido, verificación de servicios.

e) Establecer umbrales para los servicios informáticos definidos en la Tabla 5.

VII. OBJETIVOS E INDICADORES DEL PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS

7.1 Objetivo General

Restaurar los servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

7.2 Objetivos Específicos

a) Contar con servicios informáticos implementados en el espacio de la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de "IaaS Infraestructura como Servicio"
b) Documentar procedimientos adecuados que permitan recuperar la operatividad de los servicios informáticos del OTASS.
c) Ejecutar pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.
d) Fortalecer la composición de los servicios y equipos de la infraestructura tecnológica para una adecuada recuperación de servicios y sistemas informáticos.

7.3 Indicadores

Tabla 12. Metas e indicadores

OBJETIVO	DESCRIPCIÓN	INDICADOR	META	
			2024	2025
General	OBJ.G Restaurar los servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.	Porcentaje de los servicios informáticos restaurados en el tiempo optimo de restauración RTO necesarios para ejecutar las actividades y/o procesos críticos de la Entidad.	ND	100%

OBJETIVO	DESCRIPCIÓN	INDICADOR	META	
			2024	2025
Específicos	OBJ.01 Contar con servicios informáticos implementados en el espacio de la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de "IaaS Infraestructura como Servicio"	Porcentaje de avance de implementación del espacio en la Plataforma Nacional de Gobierno Digital de la PCM para implementar un Centro de datos de contingencia bajo el esquema de "IaaS Infraestructura como Servicio"	ND	43%
	OBJ.02 Documentar procedimientos adecuados que permitan recuperar la operatividad de los servicios informáticos del OTASS.	Porcentaje de procedimientos desarrollados que permitan recuperar la operatividad de los servicios informáticos del OTASS.	100%	100%
	OBJ.03 Ejecutar pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	Número de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	ND	2
	OBJ.04 Fortalecer la composición de los servicios y equipos de la infraestructura tecnológica para una adecuada recuperación de servicios y sistemas informáticos.	Porcentaje de bienes y/o servicios implementados que permitan recuperar la operatividad de los servicios informáticos del OTASS. (*)	10%	100%

(*) Acumulado

VIII. PROGRAMACIÓN DE ACTIVIDADES DEL PLAN

El presente Plan tiene programado

a) Descripción de actividades

Tabla 13. Actividades del Objetivo Especifico OBJ.01

N°	Actividad	Unidad de medida	CRONOGRAMA							META	RESPONSABLE
			2024	2025							
				Abr	Ma	Jun	Jul	Ag	Set		
1	Implementación de los bienes y servicios necesarios en el Plan de Recuperación de Servicios Informáticos.	Informe		X	X	X	X	X	X	6	UTI-OSCD

Tabla 14. Actividades del Objetivo Especifico OBJ.02

N°	Actividad	Unidad de medida	CRONOGRAMA		META	RESPONSABLE
			2024	2025		
				Mar		
1	Revisión y validación de los procedimientos del Plan de Recuperación de Servicios Informáticos.	Procedimiento		X	1	OSCD

Tabla 15. Actividades del Objetivo Especifico OBJ.03

N°	Actividad	Unidad de medida	CRONOGRAMA			META	RESPONSABLE
			2024	2025			
			Nov	Ene	Jun		
1	Elaboración de Plan de trabajo interno para ejecutar las pruebas de recuperación de servicios.	Informe	X			1	UTI-OSCD
2	Realización de las pruebas del el Plan de Recuperación de Servicios Informáticos.	Actas		X	X	2	UTI-OSCD
3	Capacitación al equipo operativo sobre los procedimientos previstos en el Plan de Recuperación de Servicios Informáticos.	Actas		X	X	2	UTI-OSCD

Tabla 16. Actividades del Objetivo Especifico OBJ.04

N°	Actividad	Unidad de medida	CRONOGRAMA			META	RESPONSABLE
			2024	2025			
			Dic	Ene	Jun		
1	Formulación de las EETT y TDR para la adquisición de los bienes y servicios necesarios para el Plan de Recuperación de Servicios Informáticos.	Documento técnico	X	X		9	UTI-OSCD

N°	Actividad	Unidad de medida	CRONOGRAMA			META	RESPONSABLE
			2024	2025			
			Dic	Ene	Jun		
2	Actualización del Plan de Recuperación de Servicios Informáticos.	Documento			X	1	OSCD

b) Costeo a nivel de especifica de gasto

Tabla 17. Costeo y programación anual de gasto del Plan de Recuperación de Servicios Informáticos del OTASS 2024-2025

PLAN DE RECUPERACION DE SERVICIOS INFORMATICOS			
Objetivo Estratégico Institucional 04: Modernizar la Gestión Institucional			
AEI 04.1: Esquemas de transformación digital y herramientas tecnológicas implementadas			
ACTIVIDAD OPERATIVA INSTITUCIONAL	ESPECIFICA DE GASTO	PROGRAMACIÓN DE GASTO	
		2024	2025
AOI00158900001 Elaboración de Procedimientos y/o Planes sobre Tecnologías de la Información AOI00158900145 Operatividad de la Infraestructura Tecnológica del OTASS	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE DE BASE DATOS SQL		S/ 80,000
	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE DE BASE DATOS ORACLE		S/ 140,000
	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE DE RESPALDO		S/ 92,500
	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE DE MONITOREO		S/ 34,500
	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE BASE PARA SERVIDORES (SISTEMA OPERATIVO)		S/ 80,000
	2.6.6.1.3.2. ADQUISICION DE LICENCIA DE SOFTWARE OPENKM		S/ 250,000
	2.3.2.7.4.99. CONTRATACION DE SERVICIO DE TRASLADO Y CUSTODIA DE COPIAS DE RESPALDO	S/ 8,000	S/ 48,000
	2.3.2.2.2.3. CONTRATACION DE UN SISTEMA DE CONEXIÓN A INTERNET PARA EL CENTRO DE OPERACIÓN DE CONTINGENCIA		S/ 2,000
SUB TOTAL		S/ 8,000	S/ 727,000

c) Financiamiento

Las actividades programadas en el Plan de Recuperación de Servicios Informáticos del OTASS para el periodo 2024 se encuentra financiado con cargo a la Meta Presupuestal 047 de la Unidad de Tecnologías de la Información; dicho Plan se encuentra vinculada a las siguientes actividades operativas: AOI00158900145: OPERATIVIDAD DE INFRAESTRUCTURA TECNOLOGICA DEL OTASS y

AOI00158900001: ELABORACION DE PROCEDIMIENTOS Y/O PLANES SOBRE TECNOLOGIAS DE LA INFORMACION. Las actividades programadas para el año 2025 se ejecutará ajustándose a la asignación presupuestaria que se autorice en las metas presupuestarias de la Unidad de Tecnologías de la Información.

Por otro las acciones de prevención / reducción, recuperación de servicios informáticos y ejecución, serán abordados por el personal de la Entidad.

d) Cronograma de Ejecución

Las actividades del Plan de Recuperación de Servicios Informáticos en el OTASS 2024-2025 se ejecutarán de acuerdo al siguiente cronograma:

Tabla 18. Cronograma de ejecución de actividades

<table>
<tr><th colspan="9">CRONOGRAMA DE EJECUCION DE ACTIVIDADES</th></tr>
<tr><td colspan="9">Objetivo general: Restaurar los servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.</td></tr>
<tr><th rowspan="3">N°</th><th rowspan="3">Actividad</th><th colspan="7">CRONOGRAMA</th></tr>
<tr><th rowspan="2">2024</th><th colspan="6">2025</th></tr>
<tr><th>Abr</th><th>May</th><th>Jun</th><th>Jul</th><th>Ago</th><th>Set</th></tr>
<tr><td colspan="9">Objetivo específico 1: Contar con servicios informáticos implementados en el espacio de la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de “IaaS Infraestructura como Servicio”</td></tr>
<tr><td>A.1.1</td><td>Implementación de los bienes y servicios necesarios en el Plan de Recuperación de Servicios Informáticos.</td><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><th rowspan="3">N°</th><th rowspan="3">Actividad</th><th colspan="7">CRONOGRAMA</th></tr>
<tr><th rowspan="2">2024</th><th colspan="6">2025</th></tr>
<tr><th colspan="6">Mar</th></tr>
<tr><td colspan="9">Objetivo específico 2: Documentar procedimientos adecuados que permitan recuperar la operatividad de los servicios informáticos del OTASS.</td></tr>
<tr><td>A.2.1</td><td>Revisión y validación de los procedimientos del Plan de Recuperación de Servicios Informáticos.</td><td></td><td colspan="6">X</td></tr>
<tr><th rowspan="3">N°</th><th rowspan="3">Actividad</th><th colspan="7">CRONOGRAMA</th></tr>
<tr><th>2024</th><th colspan="6">2025</th></tr>
<tr><th>Nov</th><th colspan="3">Ene</th><th colspan="3">Jul</th></tr>
<tr><td colspan="9">Objetivo específico 3: Ejecutar pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.</td></tr>
<tr><td>A.3.1</td><td>Elaboración de Plan de trabajo interno para ejecutar las pruebas de recuperación de servicios.</td><td>X</td><td colspan="3"></td><td colspan="3"></td></tr>
</table>

A.3.2	Realización de las pruebas del el Plan de Recuperación de Servicios Informáticos.			X
A.3.3	Capacitación al equipo operativo sobre los procedimientos previstos en el Plan de Recuperación de Servicios Informáticos.		X	X
N°	**Actividad**	**CRONOGRAMA**		
		2024	**2025**	
		Dic	**Ene**	**Jun**
Objetivo específico 4: Fortalecer la composición de los servicios y equipos de la infraestructura tecnológica para una adecuada recuperación de servicios y sistemas informáticos.				
A.4.1	Formulación de las EETT y TDR para la adquisición de los bienes y servicios necesarios para el Plan de Recuperación de Servicios Informáticos.	X	X	
A.4.2	Actualización del Plan de Recuperación de Servicios Informáticos.			X

e) Seguimiento y Evaluación

El proceso de seguimiento y evaluación del Plan de Recuperación de Servicios Informáticos del OTASS, se realiza en el marco de la norma ISO:22301-2012 Sistemas de gestión de la continuidad de negocio y la norma ISO/IEC 27001:2022 Sistema de gestión de la seguridad de la información, a cargo del Comité de Gobierno y Transformación Digital del OTASS. Para ello, el Oficial de Seguridad y Confianza Digital, una vez de aprobado el presente Plan, formulará un informe semestral indicando el avance del Plan a la Gerencia General.

Asimismo, la máxima autoridad administrativa de la Entidad es la responsable de informar semestralmente al Titular de la Entidad sobre los avances del PRSI.

IX. ANEXOS

ANEXO 1: Siglas y definiciones

ANEXO 2: Matriz de articulación de metas e indicadores del Plan de Recuperación de Servicios Informáticos.

ANEXO 3: Ficha de indicadores

ANEXO 4: Directorio de empresas proveedoras de recursos y servicios informáticos del OTASS.

ANEXO 5: Directorio de empresas proveedoras de emergencia.

ANEXO 6: Procedimiento de restablecimiento de energía eléctrica del centro de datos.

ANEXO 7: Procedimiento de encendido de los equipos de comunicaciones del centro de datos.

ANEXO 8: Procedimiento de encendido de los servidores y almacenamiento.

ANEXO 9: Procedimiento de encendido de la infraestructura Oracle.

ANEXO 10: Procedimiento de habilitación de los servicios informáticos críticos.

ANEXO 11: Procedimiento de verificación de la Operatividad del SIGA.

ANEXO 12: Procedimiento de verificación de la Operatividad del SIAF.

ANEXO 13: Procedimiento de verificación del Sistema de Gestión Documental - O Documentos.

ANEXO 14: Procedimiento de verificación del Sistema O-Transfer.

ANEXO 15: Procedimiento de verificación de los Servicios GIS de la Plataforma GIS Corporativa.

ANEXO 16: Procedimiento de verificación del Sistema E-STATAL.

ANEXO 17: Procedimiento de verificación del Software de Monitoreo del OTASS.

ANEXO 1
SIGLAS Y DEFINICIONES

Siglas:

i. **RPO:** Objetivo de Punto de Recuperación.

ii. **OTASS**: Organismo Técnico de la Administración de los Servicios de Saneamiento.

iii. **RTO:** Tiempo Objetivo de Recuperación.

iv. **UTI:** Unidad de Tecnologías de la Información.

v. **SGSI:** Sistema de Gestión de la Seguridad de la Información.

vi. **MTD:** Tiempo máximo de recuperación.

vii. **IIS:** Servicio de Información de Internet.

Definiciones de términos:

i. **Acceso**: Atributo que determina si un usuario tiene permiso para y hacer uso de un determinado equipo o servicio informático.

ii. **Activación**: Acto de declarar que las disposiciones sobre continuidad del negocio de la organización se deben poner en marcha con objeto de continuar suministrando los productos y servicios principales.

iii. **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización.

iv. **Aplicación**: programa o conjunto de programas diseñados para realizar una tarea específica en una computadora o dispositivo electrónico.

v. **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

vi. **Análisis** de impacto en el negocio: Proceso de analizar las actividades y el efecto que una interrupción del negocio puede tener sobre éstas.

vii. **Base de Datos**: Conjunto de datos recopilados, organizados y almacenados sistemáticamente en estructuras que permiten su consulta, procesamiento, crecimiento, actualización, modificación, eliminación y control de acceso.

viii. **Centro de datos**: Espacio donde se alojan los recursos necesarios para el procesamiento de la información de la Entidad. En este grupo también se consideran los equipos de comunicaciones de los diferentes pisos del OTASS.

ix. **Centro de datos Alterno**: Espacio de contingencia donde se concentran los recursos informáticos necesarios para el procesamiento de la información de una organización.

x. **Confidencialidad**: Es la propiedad de la información de no ponerse a disposición o no ser revelada a individuos, entidades o procesos no autorizados.

xi. **Control**: Mecanismo de gestión de riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

xii. **Datos**: Hechos, eventos, valores de atributos o cifras que han sido identificados o registrados y que requiere de un análisis y contexto para tener significado.

xiii. **Disponibilidad**: Es la propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo o una entidad autorizada.

xiv. **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias.

xv. **Gestión del Riesgo**: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

xvi. **Impacto**: Es el conjunto de consecuencias que origina un riesgo de llegar a presentarse.

xvii. **Incidente**: Situación que podría darse, o podría dar lugar a, una interrupción, pérdida, emergencia o crisis.

xviii. **Información**: Es un activo importante de la entidad, la cual puede estar en formato electrónico, impresa en papel o almacenada en un soporte informático.

xix. **Integridad**: La información debe ser consistente, fiable y no propensa a alteraciones no deseadas o modificadas como consecuencia de un evento o incidente no deseado.

xx. **Peligro o Amenaza**: Probabilidad de que un fenómeno físico, potencialmente dañino, de origen natural o inducido por la acción humana, se presente en un lugar específico, con una cierta intensidad y en un periodo de tiempo y/o frecuencia definidos.

xxi. **Probabilidad**: Posibilidad de que un evento o incidente suceda.

xxii. **Proceso crítico**: Aquel proceso considerado indispensable para la continuidad de las operaciones y servicios, cuya falta o ejecución deficiente, puede producir un impacto negativo en la operatividad e incumplimiento de metas u objetivos de la Entidad.

xxiii. **Respaldo**: Se refiere a una copia de seguridad de los datos originales que se realiza con el propósito de contar con una manera de recuperarlos en caso de que se pierdan.

xxiv. **Riesgo**: Efecto de la incertidumbre sobre la consecución de los objetivos

xxv. **Punto de recuperación Objetivo**: Está relacionado a la copia de respaldo de información, puesto que está definido por el periodo de la posible pérdida de información desde la última copia de respaldo hasta la caída de los servicios informáticos.

xxvi. **Tiempo de Recuperación Objetivo**: Periodo de tiempo posterior a un incidente, en el cual un producto o una actividad se debe reanudar o en el cual los recursos se deben recuperar.

xxvii. **Servicio informático**: Es el conjunto recursos computacionales y tecnología informática que se pone a disposición de los usuarios para brindar soporte a las operaciones y procesos de la entidad, son evaluados por acuerdos de nivel de servicios.

xxviii. **Sistema informático**: Es el componente lógico de un sistema de información que usa tecnología informática y recursos computacionales para recoger, procesar, almacenar y distribuir información.

xxix. **Servicio informático base**: Es el conjunto de servicios informáticos que brindan soporte a la operación de la infraestructura tecnológica de la entidad.

xxx. **Servicios de información externo**: Es el conjunto de servicios informáticos que no depende la infraestructura tecnológica, servicios o sistemas informáticos de la entidad.

xxxi. **Sistema de continuidad eléctrica**: Es el sistema que permite mantener con energía eléctrica a la infraestructura tecnológica.

xxxii. **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

ANEXO 2

MATRIZ DE ARTICULACIÓN DE METAS E INDICADORES DEL PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

METAS E INDICADORES DEL PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS																
PEI		POI	Objetivo General	Objetivos específicos	Indicador	Línea base		Logros esperados Años		Responsable	Actividad		Unidad de medida	Meta física Años		Responsable
OEI	AEI	AOI				Valor	Año	2024	2025		Código actividad	Actividad		2024	2025	
Objetivo Estratégico Institucional 04: Modernizar la Gestión institucional	AEI 04.1: Esquemas de transformación digital y herramientas tecnológicas implementadas	AOI00158900001 Elaboración de Procedimientos y/o Planes sobre Tecnologías de la Información AOI00158900145 Operatividad de la Infraestructura Tecnológica del OTASS	Restaurar los servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.		Porcentaje de los servicios informáticos restaurados en el tiempo optimo de restauración RTO necesarios para ejecutar las actividades y/o procesos críticos de la Entidad.	ND		ND	100%	OSCG-CGTD-UTI	A.1.1.	Ejecución de las restauraciones de servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones	Acta	ND	100%	OSCD/UTI
											A.1.2.	previas a su ocurrencia. Informe de la ejecución de las restauraciones de servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.	Informe	ND	100%	OSCD/UTI

METAS E INDICADORES DEL PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS															
PEI		POI	Objetivo General	Objetivos específicos	Indicador	Línea base		Logros esperados Años		Responsable	Actividad		Unidad de medida	Meta física Años		Responsable
OEI	AEI	AOI				Valor	Año	2024	2025		Código actividad	Actividad		2024	2025	
				OBJ.01 Contar con un espacio en la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de "IaaS Infraestructura como Servicio"	Porcentaje de implementación de servicios informáticos en la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de "IaaS Infraestructura como Servicio"	ND		ND	43%	OSCG-CGTD-UTI	A.2.1.	Ejecución de avance de implementación del espacio en la Plataforma Nacional de Gobierno Digital de la PCM para implementar un Centro de datos de contingencia bajo el esquema de "IaaS Infraestructura como Servicio"	Acta	ND	43%	OSCD/UTI
											A.2.2.	Informe de avance de implementación del espacio en la Plataforma Nacional de Gobierno Digital de la PCM para implementar un Centro de datos de contingencia bajo el esquema de "IaaS Infraestructura como Servicio"	Informe	ND	43%	OSCD/UTI
				OBJ.02 Documentar procedimientos adecuados que permitan recuperar la operatividad de	Porcentaje de procedimientos desarrollados que permitan recuperar la operatividad de los servicios	100%		100%	100%	OSCG-CGTD-UTI	A.3.1.	Elaboración de procedimientos desarrollados que permitan recuperar la operatividad de los servicios	Documento	100%	100%	OSCD/UTI

METAS E INDICADORES DEL PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS															
PEI		POI	Objetivo General	Objetivos específicos	Indicador	Línea base		Logros esperados Años		Responsable	Actividad		Unidad de medida	Meta física Años		Responsable
OEI	AEI	AOI				Valor	Año	2024	2025		Código actividad	Actividad		2024	2025	
				los servicios informáticos del OTASS.	informáticos del OTASS.						A.3.2.	informáticos del OTASS. Informe de la elaboración de procedimientos desarrollados que permitan recuperar la operatividad de los servicios informáticos del OTASS.	Informe	100%	100%	OSCD/UTI
				OBJ.03 Ejecutar pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	Número de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	ND		ND	2	OSCG-CGTD-UTI	A.4.1.	Ejecución de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	Acta	ND	2	OSCD/UTI
											A.4.2.	Informe de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.	Informe	ND	2	OSCD/UTI
				OBJ.04 Fortalecer la composición de los servicios y equipos de la infraestructura tecnológica para una adecuada recuperación de servicios y sistemas informáticos.	Porcentaje de bienes y/o servicios implementados que permitan recuperar la operatividad de los servicios informáticos del OTASS.	10%		10%	100%	OSCG-CGTD-UTI	A.5.1.	Contratación de bienes y/o servicios implementados que permitan recuperar la operatividad de los servicios informáticos del OTASS.	Documento	10%	100%	OSCD/UTI

ANEXO 3
FICHAS DE INDICADORES

Ficha Técnica del Indicador de OBJ.G

Ficha técnica del indicador			
OG	OBJ.G Restaurar los servicios informáticos necesarios para ejecutar las actividades y/o procesos críticos de la Entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.		
Nombre del indicador	Porcentaje de los servicios informáticos restaurados en el tiempo optimo de restauración RTO necesarios para ejecutar las actividades y/o procesos críticos de la Entidad.		
Justificación	Medir el porcentaje de servicios informáticos restaurados en el tiempo óptimo de restauración RTO necesarios para ejecutar las actividades y/o procesos críticos de la Entidad.		
Responsables	OSCD-UTI		
Limitaciones para la medición del indicador	Ninguna		
Método de cálculo	V01= (Número servicios informáticos críticos restaurados en el tiempo óptimo de restauración RTO) /(Número servicios informáticos críticos) * 100 V01= Porcentaje de servicios informáticos críticos restaurados en el tiempo óptimo de restauración.		
Sentido esperado del indicador	Ascendente		
Fuente y base de datos	Registros administrativos de las restauraciones de servicios informáticos críticos en el OTASS.		
Proceso de recolección y análisis	• Registrar hora de incidente, hora de inicio de restauración y hora de disponibilidad del sistema informático. • Recuperar datos del registro de eventos de cada servicio (hora incidente, hora de disponibilidad) • Medición de tiempos de restauración de los servicios informáticos críticos. • Recuperar datos del sistema de monitoreo • Coordinar con los especialistas de la UTI.		
	Línea base	**Metas**	
Año		**2024**	**2025**
Valor en absoluto	ND	0	13
Valor en relativo	ND	0%	100%

Ficha Técnica del Indicador de OBJ.01			
Ficha técnica del indicador			
OE	OBJ.01 Contar con servicios informáticos implementados en el espacio de la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de “IaaS Infraestructura como Servicio”		
Nombre del indicador	Porcentaje de implementación de servicios informáticos en la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de “IaaS Infraestructura como Servicio”		
Justificación	Mostrar la implementación de los servicios informáticos en el espacio de la Plataforma Nacional de Gobierno Digital de la PCM bajo el esquema de “IaaS Infraestructura como Servicio”.		
Responsables	OSCD-UTI		
Limitaciones para la medición del indicador	No contar con espacio suficiente para poder implementar los servicios en la Plataforma Nacional De Gobierno Digital PNGD.		
Método de cálculo	V01: Número de servicios informáticos implementados en la PNGD-PCM.		
	V02: Número de servicios informáticos planificados en la PNGD-PCM.		
	(V01/V02) *100		
Sentido esperado del indicador	Ascendente		
Fuente y base de datos	Registros administrativos de los espacios implementados del espacio en la Plataforma Nacional de Gobierno Digital de la PCM		
Proceso de recolección y análisis	• Reporte de la implementación de los servicios informáticos en la PNGD.		
	• Coordinar con los especialistas de la UTI y PCM.		
	• Registrar las implementaciones de servicios informáticos, en formatos que serán almacenados en la carpeta compartida del PRSI.		
	Línea base	**Metas**	
Año		**2024**	**2025**
Valor en absoluto	ND	0	3
Valor en relativo	ND	0%	43%

Ficha Técnica del Indicador de OBJ.02

Ficha técnica del indicador			
OE	OBJ.02 Documentar procedimientos adecuados que permitan recuperar la operatividad de los servicios informáticos del OTASS.		
Nombre del indicador	Porcentaje de procedimientos desarrollados que permitan recuperar la operatividad de los servicios informáticos del OTASS.		
Justificación	Evidenciar el cumplimiento de la documentación de procedimientos adecuados que permitan recuperar la operatividad de los servicios informáticos del OTASS.		
Responsables	OSCD-UTI		
Limitaciones para la medición del indicador	Errores en la descripción de las actividades de los procedimientos.		
Método de cálculo	V01: Número de procedimientos desarrollados. V02: Número de procedimientos programados. (V01/V02) *100		
Sentido esperado del indicador	Ascendente		
Fuente y base de datos	Registros administrativos de los procedimientos desarrollados que permitan recuperar la operatividad de los servicios informáticos del OTASS.		
Proceso de recolección y análisis	• Desarrollo de los procedimientos adecuados. • Coordinar con los especialistas de la UTI. • Registrar el desarrollo de los procedimientos de la UTI, en formatos que serán almacenados en la carpeta compartida del PRSI.		
	Línea base	**Metas**	
Año		**2024**	**2025**
Valor en absoluto (*)	ND	12	12
Valor en relativo	ND	100%	100%

(*) La medición del indicador es acumulativo

Ficha Técnica del Indicador de OBJ.03				
Ficha técnica del indicador				
OE	OBJ.03 Ejecutar pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.			
Nombre del indicador	Número de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.			
Justificación	Evidenciar las pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.			
Responsables	OSCD-UTI			
Limitaciones para la medición del indicador	Falta de personal profesional para ejecutar las pruebas de recuperación.			
Método de cálculo	V01: ∑(Número de pruebas de recuperación ejecutadas)			
	V01: Número de pruebas de recuperación de la operatividad de los servicios informáticos del OTASS.			
Sentido esperado del indicador	Ascendente			
Fuente y base de datos	Registros administrativos de las pruebas ejecutadas.			
Proceso de recolección y análisis	• Ejecución de las pruebas de recuperación.			
	• Coordinar con los especialistas de la UTI y proveedores de servicio.			
	• Registrar las pruebas de recuperación por los especialistas de la UTI, en formatos que serán almacenados en la carpeta compartida del PRSI.			
	Línea base	**Metas**		
Año		**2024**	**2025**	
Valor en absoluto	ND	0	2	
Valor en relativo	ND	0%	100%	

Ficha Técnica del Indicador de OBJ.04

Ficha técnica del indicador			
OE	OBJ.04 Fortalecer la composición de los servicios y equipos de la infraestructura tecnológica para una adecuada recuperación de servicios y sistemas informáticos.		
Nombre del indicador	Porcentaje de bienes y/o servicios implementados que permitan recuperar la operatividad de los servicios informáticos del OTASS.		
Justificación	Mostrar el cumplimiento de la composición de los servicios y equipos de la infraestructura tecnológica.		
Responsables	OSCD-UTI		
Limitaciones para la medición del indicador	Falta de presupuesto para adquirir y contratar los bienes y/o servicios.		
Método de cálculo	V01: Número de servicios y equipos contratados V02: Número de servicios y equipos planificados (V01/V02) *100		
Sentido esperado del indicador	Ascendente		
Fuente y base de datos	Registros administrativos de los servicios y equipos implementados		
Proceso de recolección y análisis	• Implementación de servicios y equipos de infraestructura tecnológica. • Coordinar con los especialistas de la UTI y Abastecimiento. • Registrar la composición de servicios y equipos por los especialistas de la UTI, en formatos que serán almacenados en la carpeta compartida del PRSI.		
	Línea base	**Metas**	
Año		**2024**	**2025**
Valor en absoluto (*)	ND	1	9
Valor en relativo	ND	10%	100%

(*) La medida del indicador es acumulativo

ANEXO 4

DIRECTORIO DE EMPRESAS PROVEEDORAS DE RECURSOS Y SERVICIOS INFORMÁTICOS DEL OTASS

N°	ORGANIZACIÓN	NOMBRE DEL SERVICIO
1	Telemática S.A.	Plataforma GIS
2	Domain Consulting S.A.C.	Soporte
3	Xertica Labs S.A.C.	Correo Electrónico
4	GTD PERU S.A.C.	Internet
5	Innova Tecnología S.A.C.	Antispam
7	OTECH Consulting S.A.C.	Soporte
8	S3 Perú S.A.C.	Control de accesos

ANEXO 5

DIRECTORIO DE EMPRESAS PROVEEDORAS DE EMERGENCIA

N°	INSTITUCIÓN	CONTACTO/ DESCRIPCIÓN	MEDIO DE COMUNICACIÓN
1	Comisaría PNP	Policía Nacional del Perú	Central 105
2	Sistema de Atención Médica de Urgencia	S.A.M.U.	Central 117
3	Cruz Roja Peruana	Cruz Roja	265-8783 / 266-0481 / 470-0606
4	Instituto Nacional de Defensa Civil	INDECI	225-9898 / Central 115
5	Bomberos	Central de Bomberos	Central 116

ANEXO 6

	FORMATO	Código	FOR-UTI-005
	PROCEDIMIENTO DE RESTABLECIMIENTO DE ENERGÍA ELÉCTRICA DEL CENTRO DE DATOS	Versión	1

Objetivo	Restablecer la energía eléctrica del Centro de datos
Tiempo estimado	15 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con energía eléctrica en la sede del OTASS
Postcondiciones	Tener encendido el equipamiento de comunicaciones, servidores y almacenamiento
Actividad	**Descripción de la actividad**
1	Identificar la llave térmica del tablero eléctrico del piso 1.
2	Levantar la llave térmica del tablero electico del piso 1.
3	Identificar la llave térmica del tablero eléctrico del piso 5.
4	Levantar la llave térmica del tablero electico del piso 5.
5	Identificar las llaves térmicas del tablero de transferencia alterna dentro del Centro de datos.
6	Levantar las llaves térmicas del sistema de refrigeración y UPS.

ANEXO 7

	FORMATO	Código	FOR-UTI-006
	PROCEDIMIENTO DE ENCENDIDO DE LOS EQUIPOS DE COMUNICACIONES DEL CENTRO DE DATOS	Versión	1

Objetivo	Encender los equipos de comunicaciones del Centro de datos
Tiempo estimado	30 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con energía eléctrica en el Centro Datos
Postcondiciones	Tener encendido los equipos de comunicaciones
Actividad	**Descripción de la actividad**
1	Encender el Router de Internet.
2	Encender el PBX de Telefonía IP.
3	Encender el equipo de seguridad perimetral – Firewall.
4	Encender el Switch Core.
5	Encender los Switches de borde del Centro de datos.
6	Encender los Switches de borde de todos los pisos que pertenecen al OTASS.

ANEXO 8

	FORMATO	Código	FOR-UTI-007
	PROCEDIMIENTO DE ENCENDIDO DE LOS SERVIDORES Y ALMACENAMIENTO	Versión	1

Objetivo	Encender la infraestructura tecnológica del Centro de datos.
Tiempo estimado	2 horas
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con energía eléctrica en el Centro Datos
Postcondiciones	Tener encendido los equipos de servidores y almacenamiento
Actividad	**Descripción de la actividad**
1	Encender la infraestructura física del servidor de almacenamiento donde está alojado toda la información de los servidores del OTASS.
2	Ingresar a la consola del servidor para verificar el estado de todos los componentes.
3	Ingresar a la consola del equipo de almacenamiento y verificar que todos los componentes del equipo estén operativos.
4	Encender la infraestructura física del bastidor principal.
5	Ingresar a la consola de administración del bastidor principal.
6	Verificar que la infraestructura se encuentra operativa.
7	Encender los servidores, lo cual se realiza desde la consola de administración.
8	Ingresar a los hosts de los servidores de procesamiento para poder encender los servidores virtuales.
9	Encender el servidor de Directorio Activo y DNS para que los sistemas una vez que se enciendan, puedan encontrar sus nombres respectivos.
10	Encender el servidor de tiempo, para que cuando se enciendan los sistemas informáticos, puedan sincronizarse automáticamente con este servicio.
11	Encender la plataforma de virtualización para gestionar de forma centralizada todos los servidores virtuales.
12	Ingresar a la consola de administración de virtualización para ejecutar las tareas correspondientes.
13	Encender el resto de los servidores virtuales del OTASS.

ANEXO 9

	FORMATO	Código	FOR-UTI-008
	PROCEDIMIENTO DE ENCENDIDO DE LA INFRAESTRUCTURA ORACLE	Versión	1

Objetivo	Encender la infraestructura de Oracle
Tiempo estimado	40 minutos
Responsable	Coordinador de base datos
Precondiciones	Validación eléctrica y acceso al ILOM del servidor.
Postcondiciones	Revisión de las aplicaciones en estado activo por parte de los especialistas.
Actividad	**Descripción de la actividad**
1	Ingresar al ILOM del SERVIDOR NODO 0 y encender el servidor (interfaz remota para gestionar el hardware del servidor).
2	Ingresar al ILOM del SERVIDOR NODO 1 y encender el servidor (interfaz remota para gestionar el hardware del servidor).
3	Revisar que el Hipervisor este encendido en ambos nodos (validado con un ping).
4	Iniciar el encendido de la base de datos DBQA NODO 0.
5	Iniciar el encendido de la base de datos DBQA NODO 1.
6	Encendido del repositorio de máquinas virtuales (ODA BASE).
7	Encendido de las máquinas virtuales que componen la infraestructura de ORACLE.

ANEXO 10

	FORMATO	Código	FOR-UTI-009
OTASS ORGANISMO TÉCNICO DE LA ADMINISTRACIÓN DE LOS SERVICIOS DE SANEAMIENTO	PROCEDIMIENTO DE HABILITACIÓN DE LOS SERVICIOS INFORMÁTICOS CRÍTICOS	Versión	1

Objetivo	Habilitar los servicios críticos del Centro de datos
Tiempo estimado	30 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con la infraestructura tecnológica encendida.
Postcondiciones	Contar con los servicios críticos habilitados.
Actividad	**Descripción de la actividad**
1	Habilitar los servicios de firmador, OPENKM, tiempo y las instancias de base datos del O-Documentos
2	Habilitar los servicios de seguridad, OPENKM y bachero del O-Transfer.
3	Habilitar los componentes GIS y base datos que componen el O-Alcanterna.
4	Habilitar los componentes GIS y base datos que componen el O-Cartografía.
5	Habilitar las instancias del motor de base datos del servidor SIAF.
6	Habilitar las instancias del motor de base datos del servidor SIGA.
7	Habilitar las instancias del motor de base datos del servidor e-STATAL.
8	Habilitar los hipervisores de la Plataforma de virtualización de servidores.
9	Habilitar los servicios que componen el Software de respaldo.
10	Habilitar los servicios que componen el Software de monitoreo.

ANEXO 11

	FORMATO	Código	FOR-UTI-010
	PROCEDIMIENTO DE VERIFICACIÓN DE LA OPERATIVIDAD DEL SIGA	**Versión**	**1**

Objetivo	Verificar el acceso al SIGA
Tiempo estimado	10 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con la infraestructura tecnológica encendida.
Postcondiciones	Contar con el servicio SIGA habilitado.
Actividad	**Descripción de la actividad**
1	Ingresar al servidor del aplicativo SIGA.
2	Verificar que las aplicaciones del servicio se han iniciado.
3	Coordinar con el responsable de la administración de la aplicación del SIGA para que verifique su operatividad.
4	Verificar con el personal administrativo el ingreso al SIGA del OTASS.

ANEXO 12

	FORMATO	Código	FOR-UTI-011
	PROCEDIMIENTO DE VERIFICACIÓN DE LA OPERATIVIDAD DEL SIAF	Versión	1

Objetivo	Verificar el acceso al SIAF
Tiempo estimado	10 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con la infraestructura tecnológica encendida.
Postcondiciones	Contar con el servicio SIAF habilitado.
Actividad	**Descripción de la actividad**
1	Ingresar al servidor del aplicativo SIAF.
2	Verificar que las aplicaciones del servicio se han iniciado.
3	Coordinar con el responsable de la administración de la aplicación del SIAF para que verifique su operatividad.
4	Verificar con los administrativos el ingreso al SIAF del OTASS.

ANEXO 13

	FORMATO	Código	FOR-UTI-012
	PROCEDIMIENTO DE VERIFICACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL O - DOCUMENTOS	Versión	1

Objetivo	Verificar los componentes del Sistema de Gestión Documental O-Documentos
Tiempo estimado	20 minutos.
Responsable	Coordinador de servicios y sistemas Informáticos
Precondiciones	Contar con la infraestructura tecnológica restablecida
Postcondiciones	Contar con el servicio O-Documentos habilitado
Actividad	**Descripción de la actividad**
1	Acceder al enlace de la plataforma http://e-gesdoc.otass.gob.pe/e-gesdoc/
2	Verificar conexión del cliente del SGD.
3	Verificar carga de datos de dependencias en la página de acceso para validar conexión a Base de Datos del SGD.
4	Verificar acceso a la plataforma donde se muestra la página principal de la aplicación con las bandejas asignadas por perfil de usuario.
5	Registrar documento administrativo.
6	Verificar carga de anexo.
7	Generar documento a partir de la plantilla.
8	Cargar documento.
9	Firmar documento.
10	Verificar acceso a la Mesa de Partes Virtual Ciudadano.
11	Verificar acceso a la plataforma de Validación.
12	Verificar acceso al O-Firma.
13	Verificar fecha de documentos generados para validar sincronización con servidor de tiempo institucional NTP.

ANEXO 14

	FORMATO	Código	FOR-UTI-013
	PROCEDIMIENTO DE VERIFICACIÓN DEL SISTEMA O-TRANSFER	Versión	1

Objetivo	Verificar los componentes del sistema O-Transfer
Tiempo estimado	15 minutos.
Responsable	Coordinador de servicios y sistemas Informáticos
Precondiciones	Contar con el Sistema de Gestión Documental restablecido
Postcondiciones	Contar con el servicio O-Documentos habilitado
Actividad	**Descripción de la actividad**
1	Acceder al enlace de la plataforma https://pub.otass.gob.pe/Fichaweb
2	Iniciar sesión con las credenciales de acceso con el usuario y la contraseña valida.
3	Verificar que los servicios se encuentren operativos en el IIS del servidor
4	Acceder al servidor de procesos en lotes
5	Ingresar al programador de tareas y ubicamos el O-Transfer.
6	Verificar que el servicio de proceso de saldo este operativo.

ANEXO 15

	FORMATO	Código	FOR-UTI-014
	PROCEDIMIENTO DE VERIFICACIÓN DE LOS SERVICIOS GIS DE LA PLATAFORMA GIS CORPORATIVA	**Versión**	**1**

Objetivo	Verificar los componentes de los servicios GIS de la plataforma GIS corporativa
Tiempo estimado	15 minutos.
Responsable	Analista de Sistema de Información Geográfica
Precondiciones	Contar con los servidores y almacenamiento encendidos que componen la Plataforma GIS
Postcondiciones	Contar con el servicio GIS habilitado
Actividad	**Descripción de la actividad**
1	Ingresar al enlace de la plataforma GIS.
2	Iniciar sesión como administrador de la plataforma GIS.
3	Verificar la conexión de la base de datos geográfica corporativa y la plataforma GIS.
4	Verificar los servicios de los componentes de la plataforma GIS.
5	Finalmente, verificar que los aplicativos alojados en la plataforma GIS se encuentran operativos.

ANEXO 16

	FORMATO	Código	FOR-UTI-015
	PROCEDIMIENTO DE VERIFICACIÓN DEL SISTEMA E-STATAL DEL OTASS	Versión	1

Objetivo	Verificar los accesos del sistema E-STATAL
Tiempo estimado	10 min
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con la infraestructura tecnológica encendida.
Postcondiciones	Contar con el servicio de E-STATAL habilitado.
Actividad	**Descripción de la actividad**
1	Ingresar al servidor del E-STATAL y validar que las aplicaciones se han iniciado.
2	Coordinar con el responsable de la administración de la aplicación E-STATAL para que valide su operatividad.
3	Verificar con el equipo de recursos humanos el ingreso al E-STATAL del OTASS.

ANEXO 17

	FORMATO	Código	FOR-UTI-016
	PROCEDIMIENTO DE VERIFICACIÓN DEL SOFTWARE DE MONITOREO DEL OTASS	Versión	1

Objetivo	Verificar los accesos al software de monitoreo
Tiempo estimado	15 minutos
Responsable	Coordinador de infraestructura y sistemas de comunicación
Precondiciones	Contar con la infraestructura tecnológica encendida.
Postcondiciones	Contar con el servicio de software de monitoreo habilitado
Actividad	**Descripción de la actividad**
1	Ubicar el link URL del software de monitoreo.
2	Ingresar el usuario y contraseña del software de monitoreo.
3	Verificar la operatividad de los recursos y componentes del software de monitoreo.
4	Verificar el consumo de recursos de los nodos agregados al software de monitoreo.