PLAN DE CONTINUIDAD OPERATIVA DEL ORGANISMO NACIONAL DE SANIDAD PESQUERA PLA-009-2024-SANIPES-GG-PE-01.04

Elaborado por:
Unidad Funcional de Seguridad y Defensa Nacional y Gestión de Riesgo de Desastres
Gerente General

Revisado por:
Unidad de Planeamiento y Modernización
Oficina de Planeamiento, Presupuesto y Modernización
Oficina de Asesoría Jurídica

SANIPES Organismo Nacional de Sanidad Pesquera
Firmado digitalmente por ARRIOLA ESCALANTE Maeg Alberto FAU 20565429656 soft
Motivo: Doy V° B°
Fecha: 31.05.2024 19:48:26 -05:00

SANIPES Organismo Nacional de Sanidad Pesquera
Firmado digitalmente por BRAVO CASTILLO Jose Rosendo FAU 20565429656 soft
Motivo: Doy V° B°
Fecha: 31.05.2024 19:52:02 -05:00

FIRMA DIGITAL
Firmado digitalmente por: FALCONI CANEPA Julio Americo FAU 20565429656 soft
Motivo: Soy el autor del documento
Fecha: 31/05/2024 20:00:09-0500

Aprobado por:
Presidencia Ejecutiva

SANIPES Organismo Nacional de Sanidad Pesquera
Firmado digitalmente por: SAAVEDRA CHUMBE Monica Patricia FAU 20565429656 soft
Motivo: Soy el autor del documento
Fecha: 31/05/2024 20:36:25-0500

Índice

Índice de Figuras

Índice de Tablas

I. INFORMACIÓNGENERAL

1.1 Generalidades

El SANIPES es un organismo técnico especializado adscrito al Ministerio de la Producción, encargado de normar, supervisar y fiscalizar las actividades de sanidad e inocuidad pesquera, acuícola y de piensos de origen hidrobiológico, en el ámbito de su competencia.

El SANIPES tiene por objeto lograr una eficaz administración que establezca aspectos técnicos, normativos y de vigilancia en materia de inocuidad y de sanidad de los alimentos y de piensos de origen pesquero y acuícola, con la finalidad de proteger la salud pública.

El SANIPES tiene competencia para normar, supervisar y fiscalizar los servicios de sanidad e inocuidad pesquera, acuícola y de piensos de origen hidrobiológico, en el ámbito nacional, así como de aquellos complementarios y vinculados que brinden los agentes públicos o privados relacionados con el sector de la pesca, enmarcados en las medidas y normas sanitarias y fitosanitarias internacionales.

Entiéndase que se encuentra comprendido dentro del ámbito del SANIPES el procesamiento pesquero, las embarcaciones, la infraestructura pesquera, el embarque y otros bienes y actividades vinculados a la Ley N°30063, Ley de creación del SANIPES y sus modificatorias.

En el Plan Estratégico Institucional - PEI 2021 – 2027 se estable que la misión institucional es: “Asegurar la sanidad e inocuidad en toda la cadena productiva pesquera y acuícola, para proteger la vida y salud pública de los productores y consumidores, con instrumentos preventivos y correctivos que permiten aplicar prácticas regulatorias e incorporan el enfoque de riesgo.”

SANIPES cuenta con catorce (14) Oficinas Sanitarias Desconcentradas en las regiones de Chimbote, Camaná, Callao, Pisco, Huancayo, Iquitos, Medre de Dios, Ilo, Paita, Sechura, Puno, Tarapoto, Tacna, Tumbes; cuatro Laboratorios ubicados en: Ventanilla, Puno, Sechura y Tumbes; tres (03) puestos de vigilancia ubicados en las zonas fronterizas de Iñapari (Madre de Dios), Desaguadero (Puno) y en Aguas Verdes (Tumbes), cuatro (04) puntos de control ubicados en Pucusana, Huánuco, Lambayeque y Pucallpa.

La Sede Central del Organismo Nacional de Sanidad Pesquera, se encuentra ubicado Calle Amador Merino Reyna 267 Piso 12 San Isidro, Lima-Perú.

A Continuación, se detalla la dirección de las Oficinas Sanitarias Desconcentradas, de los Laboratorios, de los Puestos de Frontera y los Puntos de Control:

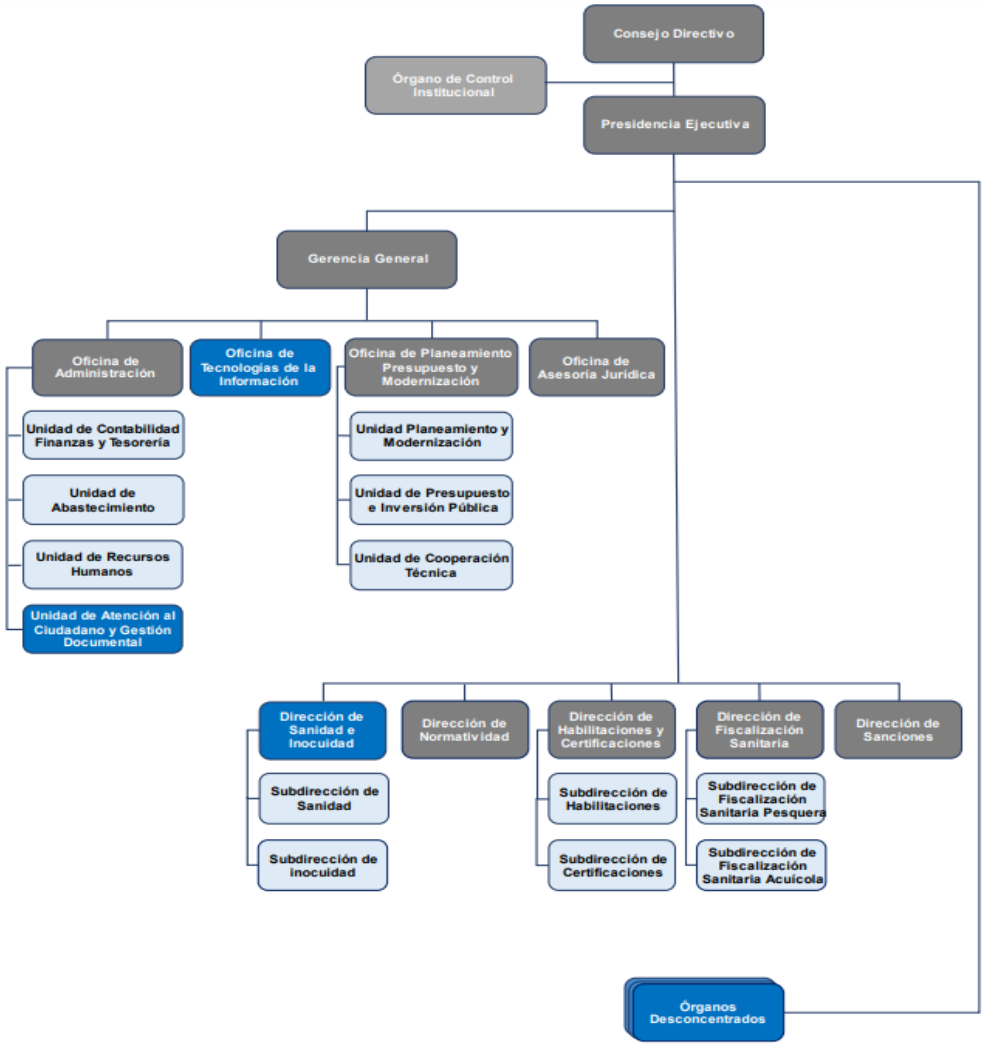
Tabla N°01: Lista de Sedes de las Oficinas Sanitarias Desconcentradas, Puestos de fronteras, Puntos de Control y Laboratorios

N°	Oficinas Sanitarias Desconcentradas, Laboratorios, Puestos de fronteras, Puntos de Control	Dirección
1	**OSD 1 Chimbote**	Jirón Hualcan 330 Urbanización Buenos Aires, distrito Nuevo Chimbote, provincia Santa - Ancash
2	**OSD 2 Camaná**	Av. Mariscal Castillo 243 – Camaná – Arequipa
3	**OSD 3 Callao**	Jr. Grau 267- 275 Bellavista - Callao
4	**OSD 4 Pisco**	Av. Las Américas 906, urb. Las Palmeras - Pisco - Ica
5	**OSD 5 Huancayo**	Psje. Las Orquídeas 133 Urb. Los Jardines de San Carlos Mz D Lote 13 Junín
6	**OSD 6 Iquitos**	Calle Tacna 133 Iquitos - Loreto
7	**OSD 7 Madre de Dios**	Jr. 28 de Julio 467 Lote 4 Mz 3Y - Puerto Maldonado – Madre de Dios

N°	Oficinas Sanitarias Desconcentradas, Laboratorios, Puestos de fronteras, Puntos de Control	Dirección
8	**OSD 8 Ilo**	Calle Brasil I-103 (2° piso) Urb. Garibaldi -Ilo - Moquegua
9	**OSD 9 Paita**	Mz. B Lote 34 – Urb. Isabel Barreto II Etapa - distrito y provincia de Paita, Piura
10	**OSD 10 Sechura**	A.H Vicente chunga Aldana Mz B2 Lote 18-B distrito y provincia de Sechura, Piura
11	**OSD 11 Puno**	Jr. Santiago Giraldo 177- Puno
12	**OSD 12 Tarapoto**	Urb. Baltazar Martínez de Compagnon Mz A Lote 3 Tercer Piso – Morales, San Martín
13	**OSD 13 Tacna**	Calle Arica 429-B - Tacna
14	**OSD 14 Tumbes**	Calle Grau 724 - Tumbes
N°	**Laboratorios**	**Dirección**
01	**Laboratorio Ventanilla**	Av. Carretera a Ventanilla Km. 5200 Ventanilla - Callao
02	**Laboratorio de Sanidad Acuícola sede Puno**	Carrera Panamericana Sur, Km. 17 - Chucuito, Puno Chucuito Puno
03	**Laboratorio Sechura**	A.H Vicente chunga Aldana Mz B2 Lote 18-B distrito y provincia de Sechura, Piura
04	**Laboratorio Tumbes**	Calle Grau 724 - Tumbes
N°	**Puestos de frontera**	**Dirección**
01	**Puesto de frontera Iñapari**	Av. Alberto Cardoso S/N – Local Puesto Fronterizo, Madre de Dios
02	**Puesto de frontera Desaguadero**	Carretera Desaguadero-Moquegua KM 3, Comunidad Lupaca Lote 01, Distrito de Desaguadero, Provincia Chucuito (CEBAF) - Puno
03	**Puesto de frontera Tumbes**	Caserío Pocitos Km 1293 – Eje Vial N°1 – Distrito de Aguas Verdes – Zarumilla, Tumbes
N°	**Punto de Control**	**Dirección**
01	**Punto de Control Lambayeque**	Av. Ramón Castilla S/N cuadra 7 – Distrito de Santa Rosa – Chiclayo (Oficina del Centro Comunitario Pesquero Artesanal de Santa Rosa CECOPAR)
02	**Punto de control Pucusana**	Malecón San Martín 100 – 102 Pucusana (Oficina del Gremio de Pescadores de Pucusana) - Lima
03	**Punto de Control Huánuco**	Jr. Constitución 408 – Huánuco (Oficina de la Dirección Regional de Producción de Huánuco)
04	**Punto de Control Pucallpa**	Jr. Tacna 826, Pucallpa (Oficina de la Dirección Regional de Producción de Ucayali)

Fuente: Oficinas Sanitarias Desconcentradas

Figura N°01: Organigrama



Fuente: Resolución de Presidencia Ejecutiva N°053-2021-SANIPES-PE

1.2 Definiciones

Para la aplicación del presente Plan, se toma como referencias las definiciones establecidas en el numeral 5.1 de los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno", que a continuación se describen:

a) Actividades críticas: Están constituidas por las actividades que la entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias y atribuciones señaladas en las normas sobre la materia.
b) Gestión de la Continuidad Operativa del Estado: Proceso continuo que debe formar parte de las operaciones habituales de la Entidad Pública con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones.
c) Unidad orgánica a cargo de la gestión de la continuidad operativa: Designada por el titular de la entidad. Responsable de articular y coordinar la Gestión de Continuidad Operativa en la Entidad, y de prestar el soporte y apoyo para asegurar la participación de todo el personal en la continuidad operativa.
d) Grupo de Comando: Es el conjunto de profesionales que se encarga de la elaboración del Plan de Continuidad Operativa de la entidad y de la toma de decisiones respecto a la implementación de dicho plan.

e) Plan de Continuidad Operativa: Instrumento a través del cual se implementa la continuidad operativa, tiene como objetivo garantizar que la entidad ejecute las actividades críticas identificadas previamente. Contiene la identificación de riesgos y recursos, acciones para la continuidad operativa y el cronograma de ejercicios.

f) Plan de Recuperación de los servicios Informáticos: Documento que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo se toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 2007 1:2014.

g) Sede alterna de la entidad pública: Espacio físico o infraestructura segura y accesible, determinada con anterioridad y de disponibilidad inmediata, que permite la ejecución de los servicios o actividades críticas señaladas en el Plan de Continuidad Operativa de la entidad. Para ello, cuenta con el equipamiento necesario y servicios básicos indispensables, que opera con autonomía energética y de conectividad. La sede alterna se ocupa cuando la sede principal de la entidad ha colapsado o su condición de operatividad ha sido afectada y pone en riesgo la seguridad del personal, pudiéndose establecer sedes alternas compartidas, que albergan a dos o más entidades públicas.

1.3 Siglas

CO : Continuidad Operativa.
COE : Centro de Operaciones de Emergencia.
DFS : Dirección de Fiscalización Sanitaria.
DHC : Dirección de Habilitaciones y Certificaciones.
DN : Dirección de Normatividad.
DS : Dirección de Sanciones.
DSI : Dirección de Sanidad e Inocuidad.
GCO : Gestión de Continuidad Operativa.
GCCO : Grupo de Comando de Continuidad Operativa.
GG : Gerencia General.
GRD : Gestión del Riesgo de Desastres.
GTGRD-SANIPES: Grupo de Trabajo para la Gestión del Riesgo de Desastres del Organismo Nacional de Sanidad Pesquera - SANIPES.
INDECI : Instituto Nacional de Defensa Civil.
OA : Oficina de Administración.
OAJ : Oficina de Asesoría Jurídica.
OD : Órganos Desconcentrados.
OP : Orden Público.
OPPM : Oficina de Planeamiento, Presupuesto y Modernización.
OSD : Oficina Sanitaria Desconcentrada.
OTI : Oficina de Tecnología de la Información.
PCM : Presidencia del Consejo de Ministros.
PCO : Plan de Continuidad Operativa.
PEI : Plan Estratégico Institucional.
PESEM : Plan Estratégico Sectorial Multianual.
POI : Plan Operativo Institucional.
PRODUCE : Ministerio de la Producción.
SDC : Subdirección de Certificaciones.
SDH : Subdirección de Habilitaciones.
SDI : Subdirección de Inocuidad.
SDS : Subdirección de Saneamiento.
SFSP : Subdirección de Fiscalización Sanitaria Pesquera.
SFSA : Subdirección de Fiscalización Sanitaria Acuícola
SINAGERD : Sistema Nacional de Gestión del Riesgo de Desastres
UFSDNYGRD: Unidad Funcional de Seguridad y Defensa Nacional y Gestión del Riesgo de Desastres
UO : Unidad Orgánica.
UOGCO : Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa.
URH : Unidad de Recursos Humanos.

II. BASE LEGAL

2.1 Ley N°29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) su reglamento y modificaciones.
2.2 Ley N°30063, Ley de Creación del Organismo Nacional de Sanidad Pesquera - SANIPES, modificada por el Decreto Legislativo N°1402.
2.3 Decreto Supremo N°0115-2022-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres - PLANAGERD 2022-2030.
2.4 Resolución Ministerial N°046-2013-PCM, que aprueba los "Lineamientos que define el Marco de Responsabilidades de Gestión del Riesgo de Desastres de las entidades del Estado en los tres niveles de Gobierno".
2.5 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"
2.6 Resolución de Presidencia Ejecutiva Nº053-2021-SANIPES/PE, que aprueba el Texto Integrado del Reglamento de Organización y Funciones del Organismo Nacional de Sanidad Pesquera (en adelante, ROF de SANIPES).
2.7 Decreto Supremo N°022-2021-PRODUCE, que aprueba la Sección Primera del Reglamento de Organización y Funciones del Organismo Nacional de Sanidad Pesquera (SANIPES).
2.8 Resolución de Presidencia Ejecutiva N°050- 2021-SANIPES-PE, que aprueba la Sección Segunda del Reglamento de Organización y Funciones del Organismo Nacional de Sanidad Pesquera (SANIPES).
2.9 Resolución de Gerencia General N.°081-2023-SANIPES/GG, que dispone de la creación de la Unidad funcional denominada "Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres", dependiente de la Gerencia General del Organismo Nacional de Sanidad Pesquera (SANIPES).
2.10 Resolución de Presidencia Ejecutiva N°095-2022-SANIPES/PE, que conforma el Grupo de Trabajo de la Gestión del Riesgo de Desastres del Organismo Nacional de Sanidad Pesquera (SANIPES).
2.11 Resolución de Presidencia Ejecutiva N°039-2024-SANIPES/PE, que aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera - SANIPES y designa a la Gerencia General como el órgano responsable de la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera – SANIPES.

III. OBJETIVOS

3.1 Objetivo General

Fortalecer la capacidad de respuesta del SANIPES, ante la ocurrencia de un evento o desastre de gran magnitud que pudiera interrumpir prolongadamente sus operaciones, garantizando que SANIPES ejecute las actividades criticas asociadas al cumplimiento de su misión institucional.

3.2 Objetivos Específicos

- Determinar actividades criticas indispensables para el SANIPES.
- Establecer procedimientos necesarios para implementar la Gestión de la Continuidad Operativa en SANIPES.

IV. IDENTIFICACIÓN DE RIESGOS Y RECURSOS

4.1 Matriz de Riesgo

Para la identificación de riesgos, se siguieron los pasos para identificación de peligros y riesgos, según lo señalado en el Anexo 2, de la Resolución Ministerial N° 320- 2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los planes de Continuidad Operativa de la Entidades Públicas de los tres niveles de gobierno".

Tabla N° 02: Matriz de Riesgo

Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
P / V	Vulnerabilidad Baja	Vulnerabilidad Media	Vulnerabilidad Alta	Vulnerabilidad Muy Alta

Fuente: Resolución Ministerial N°320-2021-PCM

Descripción de peligros identificados

Se han considerado los eventos adversos que pudieran generar interrupción de los servicios, afectar la infraestructura, recursos y vida humana, y que tengan alta probabilidad de ocurrir en las localidades donde se encuentran ubicada la Sede Central, las catorce (14) Oficinas Sanitarias Desconcentradas, los cuatro (04) Laboratorios, los tres (03) Puestos de Frontera y los cuatro (04) Puntos de Control.

En ese sentido, se identificaron los siguientes peligros:

4.1.1 Sismo de gran magnitud seguido de tsunami

En el Perú se tiene definido como escenario principal de afectación la ocurrencia de un sismo de gran magnitud, un evento de esta dimensión indefectiblemente generaría problemas en los servicios esenciales de suministros, como energía, red de agua y saneamiento, además de las vías de comunicación para la accesibilidad, generando el desabastecimiento de diferentes recursos. Esto sin mencionar el daño a la infraestructura de la sede central del Organismo Nacional de Sanidad Pesquera, se tendría complicaciones visibles y otras de análisis necesario que podrían llevar a determinar su inhabitabilidad para continuar con las operaciones propias de la entidad.

4.1.2 Movimientos en masa

Los movimientos en masa consisten en la movilización lenta o rápida, que son causados por el exceso de agua en el suelo o por la fuerza de gravedad. Asimismo, existen tipos de movimiento en masa: caídas, deslizamientos, flujos, entre otras. La ocurrencia de este evento ocasionaría una afectación en las infraestructuras del SANIPES, así como la seguridad y bienestar del personal, por lo que es necesario la activación del PCO.

4.1.3 Inundación

Las inundaciones se producen cuando las lluvias intensas sobrepasan el nivel del caudal del cauce de un río, el volumen máximo del río es superado que tiende a desbordarse afectando a la población y las actividades socioeconómicas ubicadas en las llanuras de inundación. En ese sentido, una posible inundación generaría afectaciones a la vida y salud del personal de la entidad; así como, las infraestructuras.

4.1.4 Incendio

La ocurrencia de un incendio puede afectar a la infraestructura y a la prestación de servicios en su interior, además de los trabajadores por la exposición directa al fuego, y otros daños producto de la inhalación, intoxicación y asfixia por humo. La ocurrencia de un evento de magnitud que comprometa la integridad de toda la sede, conlleva a ejecutar la continuidad de operaciones del Organismo Nacional de Sanidad Pesquera en una sede alterna, mientras se ejecutan los trabajos de rehabilitación y/o reconstrucción.

4.1.5 Alteración del Orden Público

En concordancia con el Plan Continuidad Operativa del Ministerio de la Producción, se considera probables eventos de agitación violenta de carácter social o político, realizado por parte de colectivos sociales fuera de control, con el fin de alterar el orden y la normalidad de las actividades realizadas en la entidad, tomando el espacio público e instalaciones para la atención de sus demandas.

Este tipo de evento es considerado una amenaza para las operaciones y actividades que se realizan para la atención de la ciudadanía, ya que el SANIPES se encuentra vulnerable de huelgas, concentraciones públicas, por parte de diversos grupos humanos, tales como gremios y sindicatos, grupos políticos, entre otros, que instiguen la agitación y generar acciones violentas, que vulneren la seguridad de las instalaciones y el personal, como afectación a la salud de las personas, daños materiales, hurto, sabotaje de sistema eléctrico, interrupción de las comunicaciones y de los servicios informáticos, vandalismo y otros delitos.

4.1.6 Epidemia o Pandemia

En el caso de emergencia sanitaria declarado por la autoridad máxima del Estado, se seguirán los protocolos declarados por el Gobierno, y con motivo de frenar la propagación del virus, se paralizan las actividades y operaciones normales de la entidad, interrumpiendo procesos y actividades que por la naturaleza de la función deben ser llevados de manera presencial, debiendo restringir el acceso al recinto laboral, y convocar solo la asistencia de funcionarios, directivos y Alta Dirección que están a cargo de la toma de decisiones, tomándose medidas de seguridad biológica que dispongan las Autoridades Sanitarias; así como las medidas que determine el Ministerio de Trabajo y Promoción del Empleo para el cumplimiento de las actividades del personal que laborará en modalidad de teletrabajo, permitiendo asegurar disponibilidad y acceso a los servicios de información para dar continuidad a los servicios que brinda el SANIPES en el ámbito de su competencia.

Determinación del Riesgo

Para la determinación del riesgo, el SANIPES ha considerado aquellos eventos que ocasionarían la interrupción de los servicios en forma total o parcial afectando la infraestructura, recursos y la vida humana sobre todo a las principales actividades que soportan el cumplimiento de la misión de la institución, como se puede observar a continuación:

Tabla N°03: Matriz de Riesgos SANIPES

Peligros de Origen Natural y/o Peligros por acción humana	Sede Central/Oficinas de Sanidad Desconcentrada/Laboratorios/Puntos de Control/Puestos de Frontera																						
	Ancash	Arequipa	Callao		Huánuco	Ica	Junín	Lambayeque	Lima		Loreto	Madre de Dios		Moquegua	Piura		Puno			San Martin	Tacna	Tumbes		Ucayali
	OSD Chimbote	OSD Camaná	Laboratorio Ventanilla	OSD Callao	Punto de Control Huánuco	OSD Pisco	OSD Huancayo	Punto de control Lambayeque	Pucusana	Sede Central	OSD Iquitos	Puesto de Frontera Iñapari	OSD Madre de Dios	OSD Ilo	OSD Sechura	OSD Paita	Puesto de Frontera Desaguadero	Laboratorio Puno	OSD Puno	OSD Tarapoto	OSD Tacna	Puesto de Frontera Tumbes	OSD Tumbes	Punto de Control Pucallpa
Sismo de gran magnitud seguido de Tsunami																							
Movimiento en masa																							
Inundación																							
Incendio																							

Peligros de Origen Natural y/o Peligros por acción humana	Sede Central/Oficinas de Sanidad Desconcentrada/Laboratorios/Puntos de Control/Puestos de Frontera																						
	Ancash	Arequipa	Callao		Huánuco	Ica	Junín	Lambayeque	Lima		Loreto	Madre de Dios		Moquegua	Piura		Puno			San Martin	Tacna	Tumbes		Ucayali
	OSD Chimbote	OSD Camaná	Laboratorio Ventanilla	OSD Callao	Punto de Control Huánuco	OSD Pisco	OSD Huancayo	Punto de control Lambayeque	Pucusana	Sede Central	OSD Iquitos	Puesto de Frontera Iñapari	OSD Madre de Dios	OSD Ilo	OSD Sechura	OSD Paita	Puesto de Frontera Desaguadero	Laboratorio Puno	OSD Puno	OSD Tarapoto	OSD Tacna	Puesto de Frontera Tumbes	OSD Tumbes	Punto de Control Pucallpa
Pandemia																							
Alteración del orden público																							

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres.

4.2 Determinación del Nivel de Impacto

Consiste en estimar el impacto que tendría una interrupción prolongada de los procesos que soportan el cumplimiento de la misión del SANIPES. Al respecto, en el presente Plan de Continuidad Operativa, este impacto se ha determinado sobre aquellas edificaciones que serían afectadas o impactadas por los peligros. En la siguiente Tabla se observa la estimación del nivel de impacto que afectaría a la institución relacionando el peligro con variables de operatividad determinados para el presente plan:

Tabla N°04: Matriz de Impacto

Peligro / Estimación del nivel de impacto*	Sismo de gran magnitud	Movimiento en masa	Inundación	Incendio	Pandemia	Alteración del Orden Público
Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**	Riesgo muy Alto	Riesgo muy Alto	Riesgo muy Alto	Riesgo muy Alto	Riesgo muy Alto	Riesgo muy Alto
Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto
Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**	Riesgo Medio	Riesgo Medio	Riesgo Medio	Riesgo Medio	Riesgo Medio	Riesgo Medio
No afecta la infraestructura, **no requiere evacuación**	Riesgo Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Bajo

**Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres. Se toma como referencia el criterio para la estimación del impacto de PCO – INDECI aprobado en la Resolución Jefatural N°266-2023-INDECI/JEF INDECI*

De acuerdo con la tabla anterior, correspondería determinar el nivel de impacto que tendría cada uno de las infraestructuras de la entidad frente a los peligros identificados, como se muestra a continuación:

Tabla N° 05: Matriz de Impacto SANIPES

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
1	OSD Chimbote	-Sismo de gran magnitud seguido de tsunami -Incendio -Pandemia -Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Movimiento en masa	Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
		- Inundación	Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
2	OSD Camaná	-Sismo de gran magnitud - Incendio - Pandemia - Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Movimiento en masa	Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
		- Inundación	Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
3	Laboratorio Ventanilla	-Sismo de gran magnitud seguido de tsunami -Incendio -Pandemia -Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Movimiento en masa	Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
		- Inundación	Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
4	OSD Callao	-Sismo de gran magnitud seguido de tsunami -Incendio -Pandemia -Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Inundación	Riesgo Alto	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Movimiento en masa	Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
5	Punto de Control Huánuco	-Incendio -Pandemia -Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		-Sismo de gran magnitud seguido de tsunami -Movimiento en masa - Inundación	Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
6	OSD Pisco	- Sismo de gran magnitud seguido de tsunami - Incendio - Pandemia - Alteración del Orden Público	Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Inundación	Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
7	OSD Huancayo	-Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Movimiento en masa	- Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Sismo de gran magnitud seguido de tsunami -Inundación	-Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
8	Punto de control Lambayeque	-Inundación - Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
9	Pucusana	- Sismo de gran magnitud seguido de tsunami -Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Inundación	-Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
10	Sede Central	- Sismo de gran magnitud seguido de tsunami -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Incendio	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Inundación	-Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
11	OSD Iquitos	- Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Sismo de gran magnitud seguido de tsunami - Movimiento en masa - Inundación	-Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
12	Puesto de Frontera Iñapari	- Inundación - Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami - Movimiento en masa	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
13	OSD Madre de Dios	- Inundación - Incendio -Pandemia -Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de Gran Magnitud - Movimiento en masa	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
14	OSD Ilo	- Incendio - Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Inundación	- Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
15	OSD Sechura	- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Inundación	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
16	OSD Paita	- Inundación - Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
17	Puesto de Frontera Desaguadero	- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami - Movimiento en masa - Inundación	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
18	Laboratorio Puno	- Incendio -Pandemia - Alteración del Orden Público - Movimiento en masa	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami - Inundación	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
19	OSD Puno	- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Sismo de gran magnitud seguido de tsunami - Movimiento en masa - Inundación	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
20	OSD Tarapoto	- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Inundación	- Riesgo Medio	Afectación de la infraestructura y de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
21	OSD Tacna	- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Inundación	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**
22	Puesto de Frontera Tumbes	- Incendio -Pandemia - Alteración del Orden Público - Inundación	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**

Nro.	Infraestructura	Peligro Identificado	Nivel de Impacto	
		- Movimiento en masa	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
23	OSD Tumbes	- Inundación - Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
24	Punto de Control Pucallpa	-- Incendio -Pandemia - Alteración del Orden Público	-Riesgo Muy Alto	Colapso total de la infraestructura y servicios básicos del local **que requieren evacuación**
		- Inundación	- Riesgo Alto	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Sismo de gran magnitud seguido de tsunami	-Riesgo Medio	Colapso parcial de la infraestructura y afectación de los servicios básicos del local, **que pueden requerir evacuación**
		- Movimiento en masa	- Riesgo Bajo	No afecta la infraestructura, **no requiere evacuación**

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

4.3 Identificación de recursos

Con la determinación de los peligros y los niveles de impacto que ocasionaría algún evento disruptivo es necesario precisar que el SANIPES cuenta con recursos para la respuesta que permitirá responder ante una situación de emergencia o desastre, y en caso amerite la evacuación del local, ser trasladados con el equipamiento o en su defecto prever contar con equipamiento para la Sede Alterna. En tal sentido, se identifica los recursos humanos y recursos materiales disponibles con los que cuenta la entidad.

4.3.1 Identificación de los recursos humanos disponibles del SANIPES

Tabla N° 06: Recursos Humanos de SANIPES

UNIDAD ORGANICA	SEDE	CANT.	TOTAL
PRESIDENCIA EJECUTIVA	CENTRAL - SAN ISIDRO	5	5
GERENCIA GENERAL	CENTRAL - SAN ISIDRO	16	16
OFICINA DE ADMINISTRACION	CENTRAL - SAN ISIDRO	8	8
UNIDAD DE ATENCION AL CIUDADANO	SAN ISIDRO	7	8
	VENTANILLA	1	
UNIDAD DE CONTABILIDAD, FINANZAS Y TESORERIA	CENTRAL - SAN ISIDRO	11	11
UNIDAD DE ABASTECIMIENTO	CENTRAL - SAN ISIDRO	26	49
	VENTANILLA	14	
	CENTRAL - SAN ISIDRO	1	
	BELLAVISTA	8	
UNIDAD DE RECURSOS HUMANOS	CENTRAL - SAN ISIDRO	13	13
OFICINA DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACION	CENTRAL - SAN ISIDRO	19	19
OFICINA DE ASESORIA JURIDICA	CENTRAL - SAN ISIDRO	6	6
OFICINA DE TECNOLOGIAS DE LA INFORMACION	CENTRAL - SAN ISIDRO	20	20
DIRECCION DE FISCALIZACION SANITARIA	SECHURA	1	26
	CENTRAL - SAN ISIDRO	19	
	CHIMBOTE	1	
	PALMERAS	1	
	PISCO	1	
	SAN ISIDRO/VENTANILLA	1	
	TARAPOTO	1	
	VENTANILLA	1	
SUBDIRECCION DE FISCALIZACIÓN PESQUERA	HUANCAYO	3	39
	TUMBES	4	
	CENTRAL - SAN ISIDRO	12	
	PAITA	2	
	CAMANA	2	
	CALLAO	5	
	BELLAVISTA	2	
	CHIMBOTE	4	
	ILO-MOQUEGUA	2	

UNIDAD ORGANICA	SEDE	CANT.	TOTAL
	PISCO	2	
	PUNO	1	
SUBDIRECCION DE FISCALIZACIÓN SANITARIA ACUICOLA	ILO	2	62
	IQUITOS	4	
	NARCONA	1	
	SECHURA	6	
	TARAPOTO	2	
	PUNO	2	
	MADRE DE DIOS	2	
	CENTRAL - SAN ISIDRO	18	
	BELLAVISTA	2	
	CALLAO	4	
	CHIMBOTE	5	
	PAITA	7	
	PISCO	1	
	TACNA	2	
	TUMBES	2	
	VENTANILLA	2	
DIRECCION DE SANIDAD E INOCUIDAD	PUNO	1	43
	TUMBES	2	
	SECHURA	3	
	CENTRAL - SAN ISIDRO	13	
	PIURA	1	
	VENTANILLA	23	
SUBDIRECCION DE SANIDAD	CALLAO	11	13
	CENTRAL - SAN ISIDRO	2	
SUBDIRECCION DE INOCUIDAD	CENTRAL - SAN ISIDRO	4	4
DIRECCION DE HABILITACIONES Y CERTIFICACIONES	CENTRAL - SAN ISIDRO	6	6
SUBDIRECCIÓN DE HABILITACIÓNES	CENTRAL - SAN ISIDRO	21	24
	PUNO	1	
	CHIMBOTE	1	
	SECHURA	1	
SUBDIRECION DE CERTIFICACIONES	CENTRAL - SAN ISIDRO	15	16

UNIDAD ORGANICA	SEDE	CANT.	TOTAL
	PUNO	1	
DIRECCION DE NORMATIVIDAD	CENTRAL - SAN ISIDRO	10	10
DIRECCION DE SANCIONES	CENTRAL - SAN ISIDRO	5	5
OFICINA DESCONCENTRADA SANITARIA	CENTRAL - SAN ISIDRO	3	29
	CAMANA	1	
	CALLAO	2	
	CHIMBOTE	3	
	HUANCAYO	1	
	ILO	1	
	IQUITOS	1	
	MADRE DE DIOS	1	
	PAITA	2	
	PISCO	3	
	PUNO	2	
	SECHURA	3	
	PIURA	1	
	TACNA	2	
	TARAPOTO	1	
	TUMBES	2	
Total			432

Fuente:

- *INFORME N°379 -2024-SANIPES/OA-URH (fecha de corte 12.04.2024)*
- *INFORME N°323 -2024-SANIPES/OA-UA (fecha de corte 05.04.2024)*

4.3.2 Identificación de Recursos Materiales disponibles del SANIPES

Tabla N°07: Recursos Materiales SANIPES

NOMBRE DEL RECURSO	CANTIDAD
GRUPOS ELECTROGENOS OPERATIVOS	
VENTANILLA	1
OSD TUMBES	2
EQUIPOS DE PROTECCION PERSONAL	
CASCOS	50
EQUIPOS MÉDICOS OPERÁTIVOS	
BALON DE OXIGENO	7
EQUIPO DE OXIGENOTERAPIA	1
MEDIDOR DE OXIGENO	1

NOMBRE DEL RECURSO	CANTIDAD
OXIMETRO DE PULSOS	1
TENSIOMETRO	2
TERMOMETRO INFRARROJO	43
COMPUTADORAS Y LAPTOS OPERATIVAS	
COMPUTADORA PERSONAL PORTATIL	132
UNIDAD CENTRAL DE PROCESO - CPU	400
VEHICULOS OPERATIVOS	
AUTOMOVIL	
SAN ISIDRO / CALLAO	1
CAMIONETA	
CHIMBOTE	2
PISCO	2
TACNA	1
MADRE DE DIOS	1
TUMBES	2
SECHURA	2
PAITA	1
SAN ISIDRO / CALLAO	3

Fuente: INFORME N°323 -2024-SANIPES/OA-UA (fecha de corte 05.04.2024)

V. ACCIONES PARA LA CONTINUIDAD OPERATIVA

5.1 Determinación de las Actividades Críticas

Las actividades críticas son aquellas identificadas como indispensables en la entidad, las que no deben detenerse ante situaciones de crisis operativa o de desastre para continuar brindando los servicios prioritarios, a fin de cumplir con la misión de la entidad.

Estas actividades han sido definidas con base en los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno. En el anexo N°01 se describe la metodología utilizada para la determinación de las actividades críticas.

En la Gestión de la Continuidad Operativa las actividades críticas, son aquellas que no deben detenerse o deben recuperarse en primera instancia, dentro de las primeras horas de iniciada la crisis operativa o desastre. Mientras que el resto de las actividades se reestablecen progresivamente en una segunda fase.

En la siguiente tabla se detalla las actividades con mayor prioridad, las cuales se considerarán como actividades críticas para el presente Plan de Continuidad Operativa (PCO).

Tabla N°08: Actividades Críticas SANIPES

Nro.	Procesos Misionales/Servicios	Unidad Orgánica	Proveedores y/o Clientes Internos Críticos	Proveedores y/o Clientes Externos Críticos
1	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias	DHC	- SDH - SDC - UACGD	Usuario/Administrado

Nro.	Procesos Misionales/Servicios	Unidad Orgánica	Proveedores y/o Clientes Internos Críticos	Proveedores y/o Clientes Externos Críticos
2	PM-01 Gestión de investigación en inocuidad y sanidad	DSI	- SDI - SDS	- Organización Mundial de Sanidad Animal - Ministerio de la Producción - Administrado
3	PM-03 Gestión de fiscalización	DFS	- SDFSP - SDFSA - OSD - UAEEI	- Entidad de Acreditación Mexicana-EMA - Administrado

Fuente: Elaborador por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres. Se toma como referencia los MAPROS vigentes.

5.2 Aseguramiento del Acervo Documentario

La Unidad de Atención al Ciudadano y Gestión Documental es responsable de ejecutar y monitorear los procesos de gestión documentaria y archivo de la entidad. En ese sentido, en coordinación con la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres, la UACGD elaboró el Protocolo de actuación y/o respuesta ante la ocurrencia de eventos que afecten la Gestión Documental, remitido a través del INFORME N°076-2024-SANIPES/OA-UACGD.
En el Anexo N°02, se adjunta dicho protocolo a fin de asegurar el acervo documentario.

5.3 Aseguramiento de la base de datos mediante la ejecución del plan de recuperación de los servicios informáticos

La Oficina de Tecnologías de la Información es el órgano encargado de planificar, implementar y gestionar los sistemas de información, infraestructura tecnológica de cómputo; así como de establecer los mecanismos que aseguren la disponibilidad, integridad y confidencialidad de la información del SANIPES. De modo, que en coordinación con la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres, la OTI elaboró el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicación del SANIPES, el cual fue aprobado mediante el INFORME N°53-2024-SANIPES/OTI.
En el Anexo N°03, se adjunta dicho plan a fin de asegurar la base de datos.

5.4 Roles y responsabilidades para el desarrollo de las actividades críticas

El Grupo de Comando para la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera – SANIPES, conformado mediante la Resolución de Presidencia Ejecutiva N° 039-2024-SANIPES/PE es el encargado de activar el Plan de Contingencia, ante la ocurrencia de un evento adverso. En ese sentido, una vez identificadas las dependencias responsables de la Continuidad Operativa, se han definido las responsabilidades para cada una de ellas a fin de tener establecidas las acciones a ejecutar ante situaciones de crisis.

Tabla N°09: Roles y Responsabilidades

N°	MIEMBROS	RESPONSABILIDADES
1	**Titular de la Entidad** Líder de la Continuidad Operativa	Liderar la Gestión de la Continuidad Operativa de su entidad.
		Disponer que los funcionarios de la Alta Dirección participen personalmente en la Gestión de la Continuidad Operativa y asuman responsabilidades directas en su implementación, seguimiento y monitoreo.
		Garantizar y facilitar las acciones relacionadas a la implementación de la Gestión de la Continuidad Operativa

N°	MIEMBROS	RESPONSABILIDADES
		Designar la unidad orgánica que será responsable de la Gestión de la Continuidad Operativa
		Aprobar la conformación del Grupo de Comando, a propuesta de la unidad orgánica responsable de la Gestión de la Continuidad Operativa.
		Disponer que cada unidad de organización sea de línea, de apoyo o de asesoramiento, designe un representante encargado de las coordinaciones con la unidad orgánica a cargo de la Gestión de la Continuidad Operativa.
		Garantizar y facilitar las acciones relacionadas a la implementación de la Gestión de la Continuidad Operativa.
		Establecer los mecanismos que propicien la participación de todo el personal y permitan lograr una Gestión de la Continuidad Operativa eficiente
		Asegurar y priorizar los recursos humanos, operativos y económicos.
		Integrar la Gestión de la Continuidad Operativa a la cultura organizacional
2	Presidente del GCCO-SANIPES Titular U.O. a cargo de C.O. **Gerencia General**	Proponer los procedimientos y metodologías apropiados para la Gestión de la Continuidad Operativa en la Entidad.
		Proponer la conformación del Grupo de Comando al Titular de la Entidad.
		Elaborar el cronograma de implementación de la Gestión de Continuidad Operativa y presentarlo a la Alta Dirección para su aprobación y ejecución.
		Realizar las coordinaciones con las áreas competentes, con la finalidad de determinar el estado de la infraestructura de la sede principal de la Entidad, así como del centro de cómputo y recomendar la ejecución de medidas correctivas correspondientes.
		Mantener actualizada la documentación que sustente las actividades desarrolladas como parte de la Continuidad Operativa, la misma que será parte del acervo documentario durante los procesos de transferencia.
		Remitir el Plan de Continuidad Operativa aprobado al Instituto Nacional de Defensa Civil, para su seguimiento.
		Difundir el Plan de Continuidad Operativa y publicarlo en la sede digital de la entidad
		Coordinar y ejecutar los ejercicios para validar el funcionamiento del Plan de Continuidad Operativa e informar sobre los resultados alcanzados.
		Integrar la Gestión de la Continuidad Operativa a la cultura organizacional
3	Oficina de Planeamiento, Presupuesto y Modernización	Disponer la Implementación de las decisiones adoptadas por el Grupo de Comando para la Continuidad Operativa.

N°	MIEMBROS	RESPONSABILIDADES
		Establecer las modificaciones del presupuesto para responder a las necesidades de la crisis operativa.
		Asegurar la disponibilidad de presupuesto para la ejecución de las actividades críticas y de apoyo.
		Realizar las coordinaciones para la implementación del presupuesto para la implementación del Plan de Continuidad Operativa.
		Realizar las actividades que le sean asignadas por el Presidente del GCCO-SANIPES durante la declaración de crisis operativa.
4	Unidades Orgánicas cuya actividad ha sido identificada como crítica (**DSI, DFS, DHC**)	Evaluar y gestionar la cantidad de personal necesario para el apoyo a la ejecución de las Actividades Críticas de su competencia.
		Asegurar el equipo y material necesario para apoyar la ejecución de las Actividades Críticas.
		Realizar las actividades que le sean asignadas por el Presidente del GCCO-SANIPES durante la declaración de crisis operativa.
5	**Oficina de Administración**	Coordinar el suministro de elementos esenciales relacionados a transporte, recursos de infraestructura, materiales, equipos y otros que sean necesarios acorde a las evaluaciones realizadas.
		Gestionar la consecución y adecuación de la sede alterna o centros alternos para la continuidad operativa acorde a los órganos afectados según evento adverso acontecido.
		Velar por la seguridad del personal que actúa en la sede alterna y en el área del evento.
		Establecer las coordinaciones correspondientes con la Policía Nacional para garantizar la seguridad externa de las instalaciones alternas y de las afectadas.
		Apoyar en la evacuación de los activos y recursos que garanticen la continuidad operativa.
		Gestionar la adecuación de la sede alterna.
		Realizar la implementación de la Sede Alterna para la continuidad operativa en coordinación con las unidades orgánicas responsables.
		Coordinar con las entidades prestadoras de servicios para el restablecimiento de los servicios de agua, luz e internet en la sede alterna.
		Realizar el diagnóstico del estado y los riesgos de la infraestructura de la sede principal del Organismo Nacional de Sanidad Pesquera, sede alterna, centro de cómputo, en coordinación con las unidades orgánicas responsables.
		Realizar las actividades que le sean asignadas por el Presidente del GCCO-SANIPES durante la declaración de crisis operativa.

N°	MIEMBROS	RESPONSABILIDADES
6	**Unidad de Recursos Humanos**	Asegurar la disponibilidad de recursos humanos para la ejecución de actividades críticas y de apoyo.
		Facilitar protocolos para el trabajo remoto de las actividades no críticas.
		Realizar la convocatoria del personal clave de la continuidad operativa.
		Disponer que personal establezca los procedimientos de seguridad en las áreas funcionales.
		Establecer la doble asignación de funciones en coordinación con la Unidad de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres.
		Realizar las actividades que le sean asignadas por el Presidente del GCCO-SANIPES durante la declaración de crisis operativa.
7	**Oficina de Tecnologías de Información**	Liderar la recuperación tecnológica, basada en las estrategias de continuidad implementadas.
		Identificar los posibles riesgos de aspectos tecnológicos que afectarían la continuidad de las operaciones
		Asegurar la disponibilidad de los aplicativos y medios informáticos para el soporte en la ejecución de las actividades críticas y de apoyo.
		Determinar la estructura alterna de tecnologías de la información y centros de respaldo de la información.
		Mantener actualizado el denominado Plan de Recuperación de los servicios informáticos
		Realizar las actividades que le sean asignadas por el Presidente del GCCO-SANIPES durante la declaración de crisis operativa.

Fuente:

- *Se toma como referencia las funciones establecidas en la Resolución Ministerial N°320-2021-PCM.*
- *Se toma como referencia el Reglamento Interno de las Unidades de Organización que conforman la Grupo Comando para la Gestión de la Continuidad Operativa*

5.5 Requerimientos

5.5.1 Requerimientos de Personal

Para determinar la relación nominal y personalizada del personal prioritario, mínimo e indispensable, para asegurar el Plan de Continuidad Operativa del SANIPES ante un evento adverso, es necesario comprender que no está referido a todo el personal de las unidades de organización, sino el mínimo que se necesita en esas condiciones.

El alcance del personal priorizado en el SANIPES se ha identificado en base a la necesidad de cada unidad de organización; entendiéndose que ha de desarrollar su priorización de actividades a fin de mantener la continuidad de la Entidad. En lo posible debe considerarse doble asignación de funciones.

Tabla N°10: Requerimiento Personal de las Unidades de Organización Críticas

Unidad de Organización Crítica	Cantidad
Dirección de Sanidad e Inocuidad	4
Dirección de Fiscalización Sanitaria	3

Unidad de Organización Crítica	Cantidad
Dirección de Habilitaciones y Certificaciones	4
Total	**11 personas**

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

Tabla N°11: Requerimiento de Personal de los Órganos de Apoyo y Asesoramiento

Unidad Orgánica de Apoyo y Asesoramiento	Cantidad
Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres	(02 personas)
Oficina de Administración	(05 personas)
Unidad de Recursos Humanos	(02 personas)
Oficina de Planeamiento, Presupuesto y Modernización	(02 personas)
Oficina de Tecnologías de la Información	(03 personas)
Total	**14 personas**

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

5.5.2 Requerimiento de material y equipo

Los órganos y unidades orgánicas involucrados en el PCO SANIPES cuentan con el equipamiento mínimo indispensable (equipos y mobiliarios) para facilitar al PCO ante un evento, en condiciones que impliquen una reubicación, reacondicionamiento de espacios o de desplazamiento a la sede alterna.

La Oficina de Administración asumirá el rol de determinar el estado de los equipos y materiales disponibles después de la emergencia, y determinar junto a las direcciones con actividades críticas, los materiales necesarios en la sede alterna, de acuerdo a lo determinado por el Grupo de Comando para la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera - SANIPES.

5.5.3 Requerimiento de Recursos Informáticos

La Oficina de Tecnología de la Información asumirá el rol de determinar el estado del Centro de Datos, así como el número de los equipos disponibles después de la emergencia e implementará la cantidad de equipos informáticos necesarios en la sede alterna, según lo determinado por el Grupo de Comando para la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera - SANIPES.

5.5.4 Requerimiento Presupuestal

El Plan de Continuidad Operativa del Organismo Nacional de Sanidad Pesquera - SANIPES será financiado íntegramente con cargo a los recursos presupuestales previstos en la meta presupuestal de la UFSDNYGRD consignado en el Plan Operativo Institución del año en que se activa el PCO; por consiguiente, su ejecución no demandará recursos adicionales.

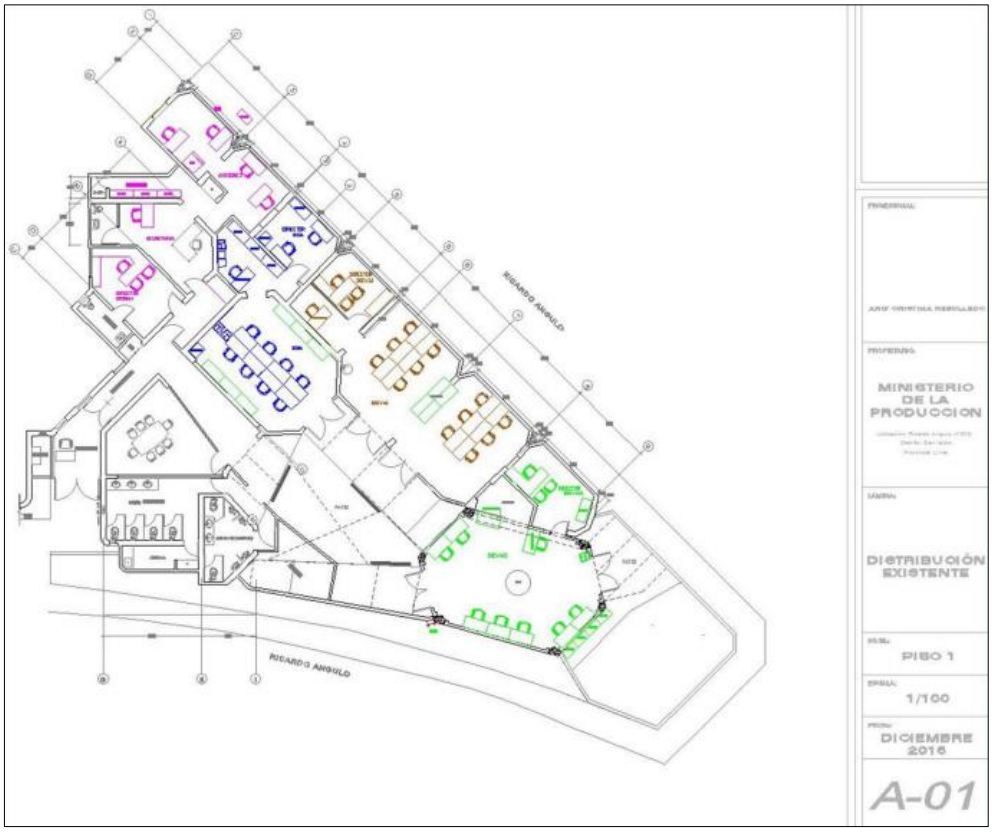
5.6 Determinación de la Sede Alterna de Trabajo

Con el fin de asegurar la Continuidad Operativa del SANIPES, y en virtud del punto “g. Sede alterna de la entidad pública” del numeral “5.1 Definiciones” de la Resolución Ministerial N°320-2021-PCM, la misma que dispone la posibilidad de establecer sedes alternas compartidas, que albergan a dos o más entidades, se solicitó a la Oficina de Seguridad y Defensa Nacional del Ministerio de la Producción, evaluar la posibilidad de poder establecer como sede alterna del SANIPES.

En ese sentido, mediante Oficio N°121-2024-PRODUCE/OSDN, la OSDN-PRODUCE, dispuso su conformidad para establecer un espacio físico de la OSDN-PRODUCE como sede alterna del SANIPES.

Dicha sede alterna se encuentra ubicada en Av. Ricardo J. Angulo R. 816 - San Isidro, infraestructura que se considera estable en su estructura, afecta a normas técnicas de construcción sismorresistente, sin evidencia de fisuras ni daños en su estructura, presenta un solo nivel y cuenta con un aforo de más de 40 personas.

Figura N°02: Distribución de la sede Ricardo Angulo del Ministerio de la Producción



Fuente: Plan de Continuidad Operativa del Ministerio de la Producción aprobado mediante Resolución Ministerial N°00410-2020-PRODUCE

5.7 Activación del Plan de Continuidad Operativa

La activación del Plan de Continuidad Operativa del SANIPES se realiza ante la ocurrencia de desastre o evento adverso a fin de continuar con los servicios y actividades de la institución. A continuación, se detallan las acciones para la activación del PCO:

Tabla N°12: Fases y actividades del PCO

FASE	ACTIVIDADES
FASE PREVIA	Gestionar la disposición de recursos económicos a fin de implementar lo señalado en el Plan de Continuidad Operativa.
	Asegurar la disposición y/o adquisición de los requerimientos indicados para la gestión de la continuidad operativa.
FASE DE ACTIVACIÓN	Evaluación inicial y reporte de afectaciones
	Activación del PCO determinada por el Titular de la Entidad y/o a propuesta del Grupo Comando.
	Convocatoria del personal involucrado en la ejecución de actividades críticas.

FASE	ACTIVIDADES
	Traslado de personal a la sede alterna y/o trabajo remoto de personal designado.
	Coordinación con entidades de saneamiento y servicios básicos a fin de asegurar la operatividad de las actividades críticas.
	Asegurar el funcionamiento y disponibilidad de recursos para la óptima ejecución de actividades críticas y de apoyo.
	Coordinaciones con COES-PRODUCE, PNP, Bomberos, Serenazgo, Municipalidad
FASE DE DESACTIVACIÓN	Desactivación del Plan de Continuidad Operativa

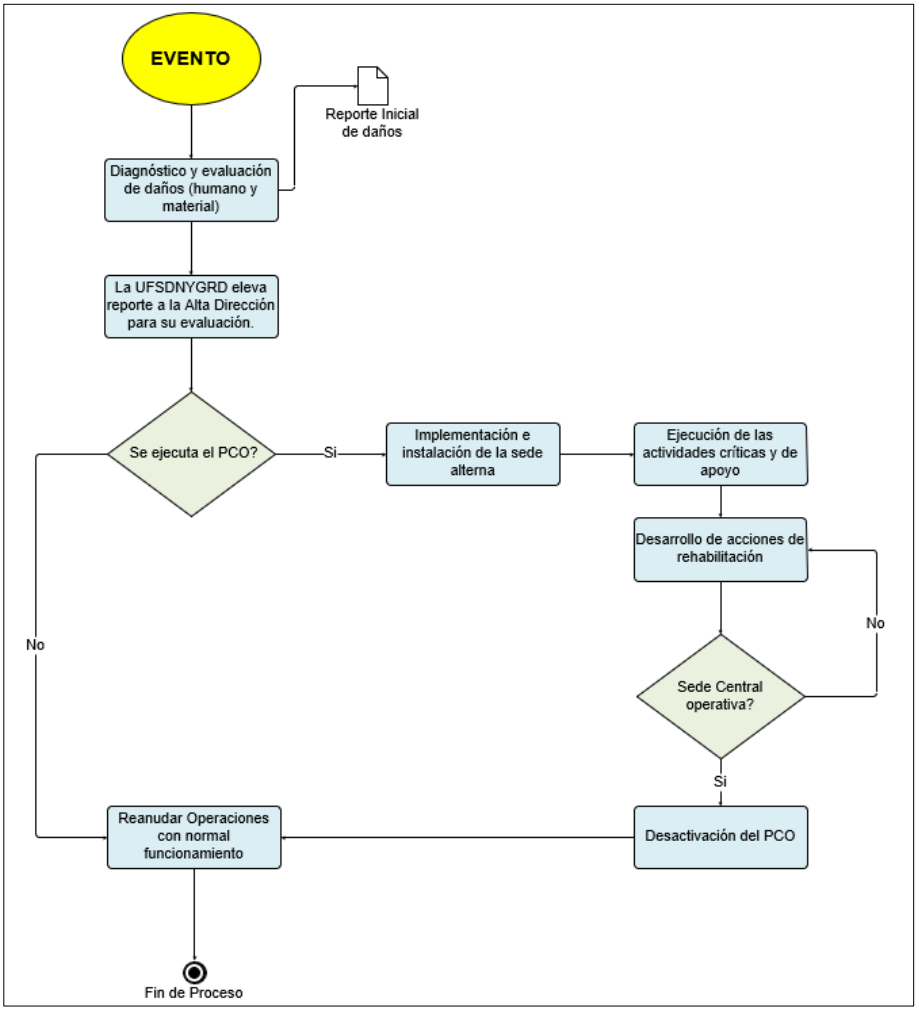
Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

5.8 Activación y desactivación de la sede alterna

La Gerencia General como la unidad orgánica encargada de la Gestión de Continuidad Operativa del Organismo Nacional de Sanidad Pesquera presidente del Grupo de Comando, por lo que le corresponde proponer a la Titular de la Entidad, la activación del PCO y de una sede alterna, de corresponder. En ese sentido, una vez autorizado la activación del PCO, el Grupo de Comando inicia con los procedimientos de convocatoria al personal esencial.

A continuación, se muestra el flujo de la activación y desactivación de la sede alterna:

Figura N°03: Flujograma de activación y desactivación de la sede alterna



Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres.

5.9 Desarrollo de las actividades críticas

Con el fin de asegurar el desarrollo de las Actividades Críticas, el Grupo de Comando debe realizar el seguimiento y monitoreo correspondiente, para tal efecto se deberá utilizar la matriz de Seguimiento y Monitoreo de la ejecución de las Actividades Críticas del Plan de Continuidad Operativa establecida en el Anexo 4 de la R.M. N°320-2021-PCM.

Tabla N°13: Matriz de Seguimiento y Monitoreo de las actividades Críticas

Actividad Crítica	Responsable	Actividades desarrolladas	Personal Asignado	Material Asignado	Equipo Asignado	Presupuesto Asignado	Fecha de Actualización	Observaciones
PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias	DHC							
PM-01 Gestión de investigación en inocuidad y sanidad	DSI							
PM-03 Gestión de fiscalización	DFS							

Fuente: Resolución Ministerial N°320-2021-PCM

VI. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

A fin de cumplir con los ejercicios de activación del Plan de Continuidad Operativa, se deberá integrar la Gestión de Continuidad Operativa a la cultura organizacional de la Entidad fortaleciendo el conocimiento de los servidores mediante capacitaciones sobre la implementación del Plan de Continuidad Operativa, así como los requerimientos necesarios para ello. De modo, que se define el siguiente cronograma de ejercicios posterior a la aprobación mediante Resolución de Presidencia Ejecutiva del Plan de Continuidad Operativa. En el Anexo 08, se detalla el cronograma de la implementación de la Continuidad Operativa.

Tabla N°14: Cronograma de Ejercicios PCO

Ejercicio PCO	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre
Pruebas del Sistema de Continuidad Operativa: Ante desastres naturales		X								X		
Pruebas del Sistema de Continuidad Operativa: Ante desastres no naturales			X									X
Simulación por sismo seguido de tsunami y/o desastre de gran magnitud*				X							X	
Simulacro Nacional Multipeligro*					X			X			X	

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

Cabe mencionar que, lo detallado en la tabla anterior se ha considerado las simulaciones y simulacros programados según normativa vigente.

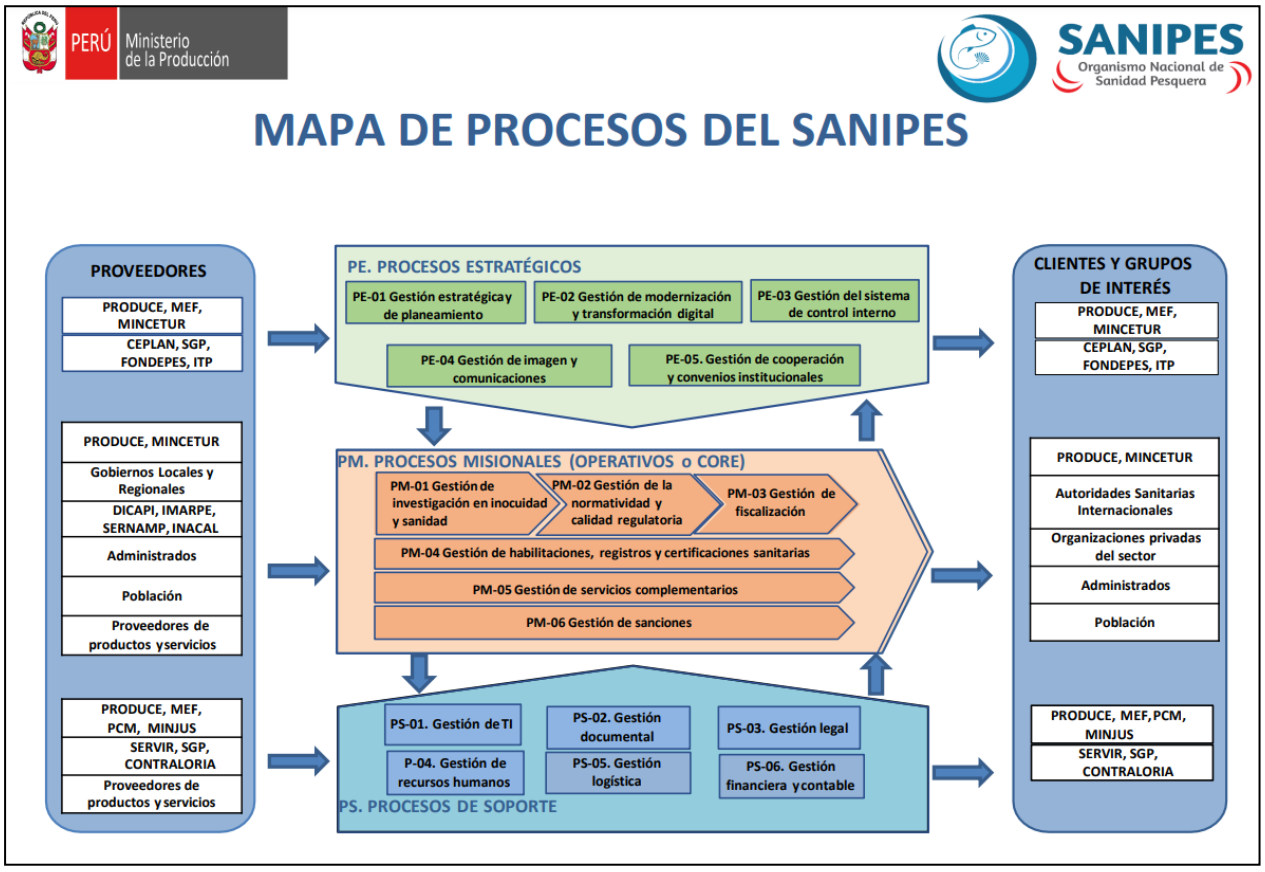
VII. ANEXOS

Anexo N°01: Determinación de actividades críticas
Anexo N°02: Protocolo de actuación y/o respuesta ante la ocurrencia de eventos que afecten la Gestión Documental
Anexo N°03: Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones del SANIPES
Anexo N°04: Procedimiento para la convocatoria del personal involucrado en la ejecución de actividades críticas
Anexo N°05: Directorio del Grupo Comando
Anexo N°06: Organización para el desarrollo de actividades críticas
Anexo N°07: Sistema de Comunicaciones de Emergencia
Anexo N°08: Cronograma de implementación de la Gestión de la Continuidad Operativa

ANEXO N°01: DETERMINACIÓN DE ACTIVIDADES CRÍTICAS

Primer criterio. – Determinación de los procesos estratégicos, misionales y de soporte.
El mapa de procesos de la entidad muestra que se cuenta con cinco (5) procesos estratégicos, seis (6) procesos misionales y seis (6) proceso de soporte.

Figura N°04: Mapa de Procesos SANIPES



Fuente: Resolución de Gerencia General N.°009-2021-SANIPES-GG

Los procesos estratégicos definen la orientación hacia donde deben operar los procesos operativos o misionales, de acuerdo con la cadena de valor de la entidad, los cuales necesitan a los procesos de apoyo o soporte para cumplir con sus objetivos.

De acuerdo con los Lineamientos para la Gestión de la Continuidad Operativa, las actividades críticas están enfocadas en aquellas que afecten al cumplimiento de la misión de la entidad, resultando estos los siguientes procesos:

Tabla N°15: Procesos Misionales SANIPES

N°	Procesos Misionales
1	PM-01 Gestión de investigación en inocuidad y sanidad
2	PM-02 Gestión de la normatividad y calidad regulatoria
3	PM-03 Gestión de fiscalización
4	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias
5	PM-05 Gestión de servicios complementarios
6	PM-06 Gestión de sanciones

Fuente: Resolución de Gerencia General N°009-2021-SANIPES-GG

Segundo criterio. – Determinación de los productos priorizados en el SCI

Los procesos misionales son la secuencia de actividades que transforman insumos en un bien o servicio y, por tanto, están contenidos en las cadenas de valor. El SANIPES optimiza sus procesos a fin de producir los bienes o servicios que valora la población de manera eficaz y eficiente siendo sus principales los siguientes:

Tabla N°16: Productos Priorizados en el SCI

N°	Productos Priorizados en el Sistema de Control Interno
1	Habilitaciones y registros sanitarios
2	Asistencia técnica y capacitación en buenas prácticas pesqueras, calidad sanitaria e inocuidad.
3	Resolución de expedientes del procedimiento administrativo sancionador
4	Fiscalización sanitaria de las actividades pesqueras en toda la cadena productiva
5	Fiscalización sanitaria de las actividades acuícolas en toda la cadena productiva
6	Plan Oficial de Vigilancia de enfermedades de los recursos hidrobiológicos
7	Alertas en materia de sanidad e inocuidad pesquera y acuícola
8	Informe técnico de análisis de riesgos en materia de sanidad e inocuidad en alimentos pesqueros y acuícolas.
9	Certificaciones oficiales sanitarias

Fuente: Informe N°061-2024-SANIPES/OPPM

Vinculación con los procesos misionales:

Se realizó la vinculación de los principales productos identificados con los procesos misionales de la entidad, obteniéndose lo siguiente:

Tabla N°17: Vinculación Productos Priorizados con Procesos Misionales

N°	Principales Productos SANIPES	Proceso Misional
1	Habilitaciones y registros sanitarios	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias
2	Asistencia técnica y capacitación en buenas prácticas pesqueras, calidad sanitaria e inocuidad.	PM-02 Gestión de la normatividad y calidad regulatoria
3	Resolución de expedientes del procedimiento administrativo sancionador	PM-06 Gestión de sanciones
4	Fiscalización sanitaria de las actividades pesqueras en toda la cadena productiva	PM-03 Gestión de fiscalización
5	Fiscalización sanitaria de las actividades acuícolas en toda la cadena productiva	PM-03 Gestión de fiscalización
6	Plan Oficial de Vigilancia de enfermedades de los recursos hidrobiológicos	PM-01 Gestión de investigación en inocuidad y sanidad
7	Alertas en materia de sanidad e inocuidad pesquera y acuícola	PM-01 Gestión de investigación en inocuidad y sanidad
8	Informe técnico de análisis de riesgos en materia de sanidad e inocuidad en alimentos pesqueros y acuícolas.	PM-01 Gestión de investigación en inocuidad y sanidad
9	Certificaciones oficiales sanitarias	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

A partir de lo observado anteriormente, se desarrolló un cuadro resumen, a fin de medir el impacto de cada proceso misional respecto los principales productos que brinda el SANIPES.

Tabla N°18: Análisis Procesos Misionales según Productos Priorizados

N°	Procesos Misionales	Cantidad de Productos Vinculados	Prioridad
1	PM-01 Gestión de investigación en inocuidad y sanidad	3	1
2	PM-02 Gestión de la normatividad y calidad regulatoria	1	3

3	PM-03 Gestión de fiscalización	2	2
4	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias	2	2
5	PM-05 Gestión de servicios complementarios	0	4
6	PM-06 Gestión de sanciones	1	3

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

Tercer criterio. – Valor Presupuestal de los productos priorizados en el SCI
Se realizó la vinculación del presupuesto asignado según producto priorizado, obteniéndose lo siguiente:

Tabla N°19: Presupuesto por Producto Priorizados

N°	Principales Productos SANIPES	Presupuesto de Productos Priorizados (S/.)
1	Habilitaciones y registros sanitarios	3 435 361.96
2	Asistencia técnica y capacitación en buenas prácticas pesqueras, calidad sanitaria e inocuidad.	2 233 110.60
3	Resolución de expedientes del procedimiento administrativo sancionador	915 398.46
4	Fiscalización sanitaria de las actividades pesqueras en toda la cadena productiva	15 307 252.03
5	Fiscalización sanitaria de las actividades acuícolas en toda la cadena productiva	15 222 616.45
6	Plan Oficial de Vigilancia de enfermedades de los recursos hidrobiológicos	1 255 087.83
7	Alertas en materia de sanidad e inocuidad pesquera y acuícola	232 788.55
8	Informe técnico de análisis de riesgos en materia de sanidad e inocuidad en alimentos pesqueros y acuícolas.	232 788.55
9	Certificaciones oficiales sanitarias	2 730 429.80

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

Vinculación con los procesos misionales:

De igual modo, se procedió a vincular el presupuesto asignado con los procesos misionales, en base al producto priorizado correspondiente por cada proceso, como se observa a continuación:

Tabla N°20: Análisis Procesos Misionales según Presupuesto

N°	Procesos Misionales	Presupuesto Asignado		Prioridad
		Monto (S/.)	Porcentaje (%)	
1	PM-01 Gestión de investigación en inocuidad y sanidad	1 720 664.93	4.14	3
2	PM-02 Gestión de la normatividad y calidad regulatoria	2 233 110.6	5.37	3
3	PM-03 Gestión de fiscalización	30 529 868.5	73.45	1

N°	Procesos Misionales	Presupuesto Asignado		Prioridad
		Monto (S/.)	Porcentaje (%)	
4	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias	6 165 791.76	14.83	2
5	PM-05 Gestión de servicios complementarios	0	0	4
6	PM-06 Gestión de sanciones	915 398.46	2.20	3

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

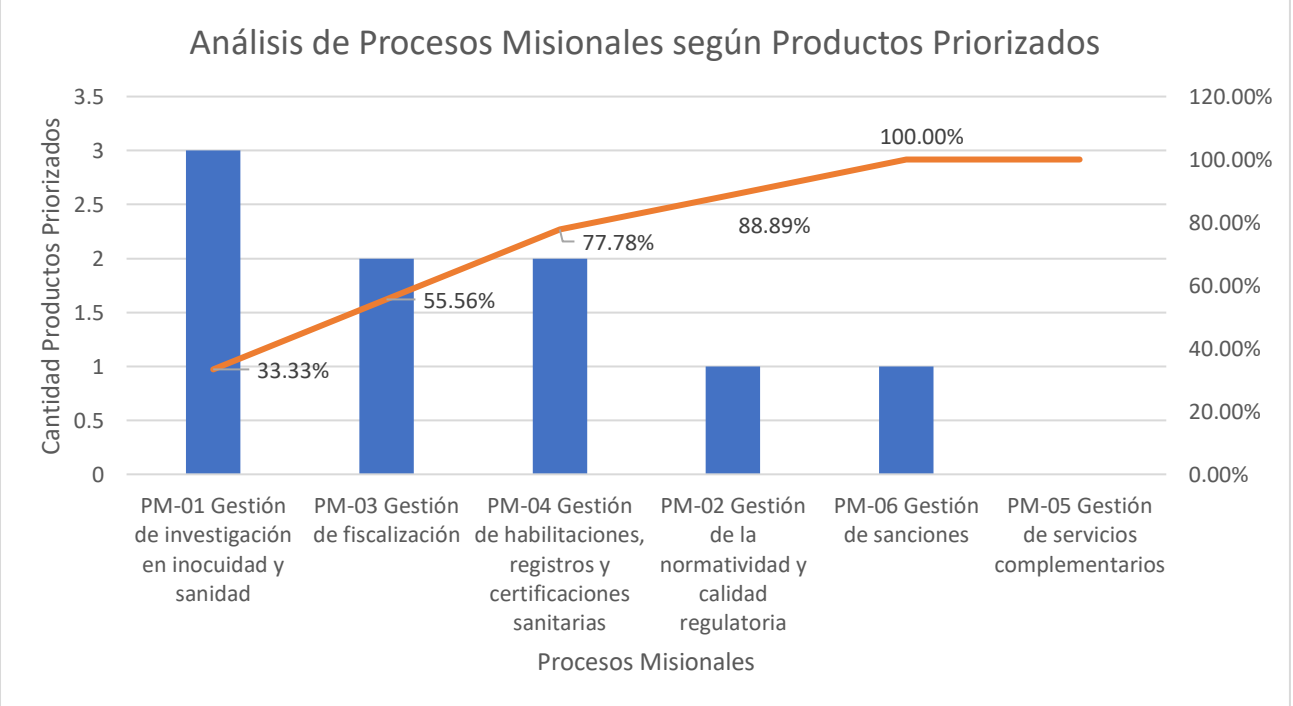
A partir de los criterios expuestos, se realizó el siguiente análisis:

Tabla N°21: Análisis Global de los Procesos Misionales

N°	Procesos Misionales	Prioridad por Criterio		Prioridad
		Productos Priorizados SCI	Presupuesto Asignado	
1	PM-01 Gestión de investigación en inocuidad y sanidad	1	3	2
2	PM-02 Gestión de la normatividad y calidad regulatoria	3	3	3
3	PM-03 Gestión de fiscalización	2	1	2
4	PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias	2	2	2
5	PM-05 Gestión de servicios complementarios	4	4	4
6	PM-06 Gestión de sanciones	3	3	3

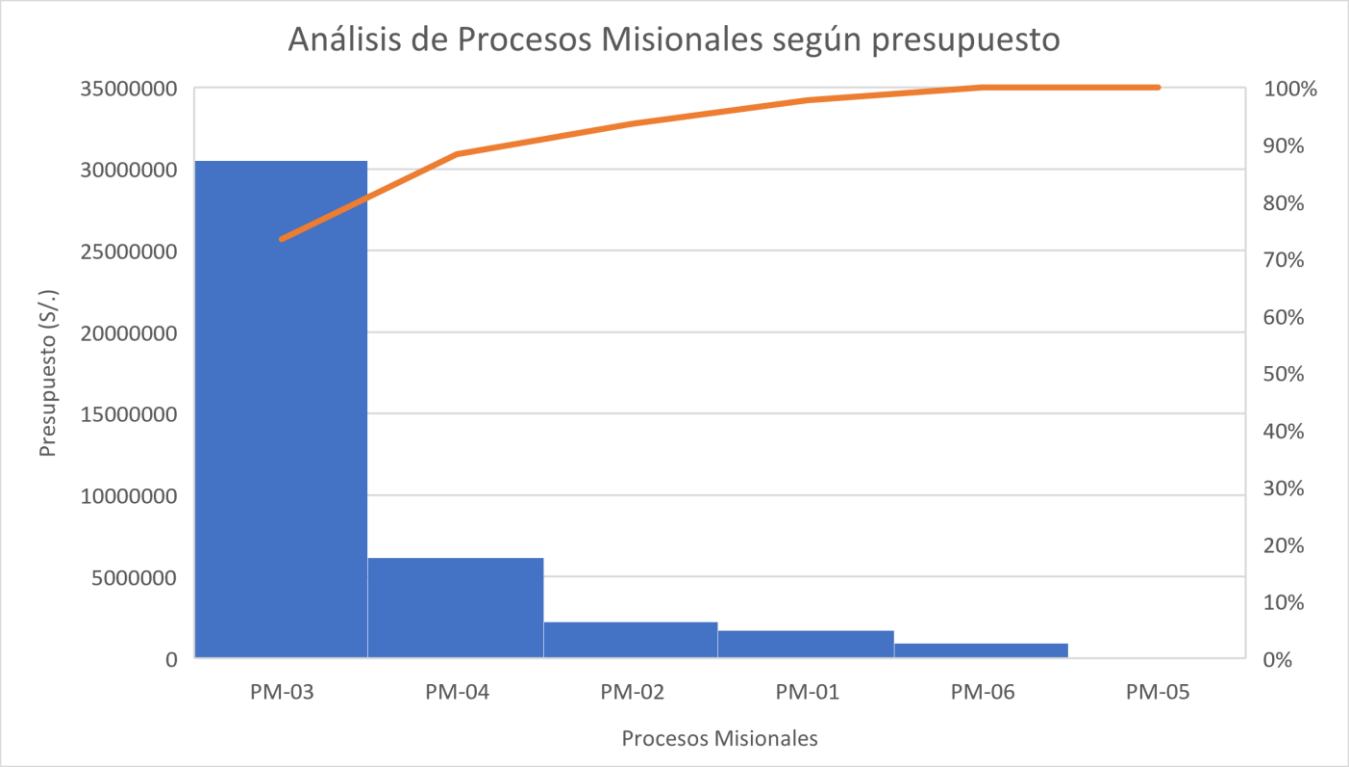
Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

Figura N°05: Diagrama de Pareto Procesos Misionales según Producto Priorizado



Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

Figura N°06: Diagrama de Pareto Procesos Misionales según Presupuesto



Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres a partir del Informe N°061-2024-SANIPES/OPPM

Como se puede observar, a partir del análisis según los criterios planteados, se determinaron las actividades críticas, los cuales son:

- PM-01 Gestión de investigación en inocuidad y sanidad
- PM-03 Gestión de fiscalización
- PM-04 Gestión de habilitaciones, registros y certificaciones sanitarias

ANEXO N°02: PROTOCOLO DE ACTUACIÓN Y/O RESPUESTA ANTE LA OCURRENCIA DE EVENTOS QUE AFECTEN LA GESTIÓN DOCUMENTAL

I. OBJETIVO

Establecer procedimientos de respuesta ante la ocurrencia de eventos que afecten la gestión documental a nivel central en el Organismo Nacional de Sanidad Pesquera - SANIPES.

II. ALCANCE

Las disposiciones contenidas en el presente procedimiento son de obligatorio cumplimiento, por todos los servidores civiles que prestan servicios en la entidad, independientemente del régimen laboral y/o contractual

III. BASE LEGAL

- Ley N°25323, Ley del Sistema Nacional de Archivos y su reglamento, aprobado mediante Decreto Supremo N°008-92-JUS.
- Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres.
- Decreto Supremo N°038-2021-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050, de carácter multisectorial.
- Decreto Supremo N°048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres.
- Decreto Supremo N°115-2022-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022 – 2030.
- 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.
- Resolución Ministerial N°039-2024-SANIPES/PE, Resolución Presidencia Ejecutiva que aprueba la conformación del Grupo de Comando para la gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera - SANIPES.
- Resolución de Gerencia General N°081-2023-SANIPES/GG, que crea la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión de Riesgo de Desastres, dependiente de la Gerencia General del Organismo Nacional de Sanidad Pesquera - SANIPES.
- Resolución de Gerencia General N°026-2021-SANIPES-GG, que aprueba la Gestión de Documentos Normativos y Orientadores en el Organismo Nacional de Sanidad Pesquera – SANIPES.
- Resolución Jefatural N°159-97-AGN/J, que aprueba el Plan de prevención y recuperación de siniestros por inundación en archivos.
- Resolución Jefatural N°292-2008-AGN/J, que aprueba la Prevención de siniestros por incendio en archivos.

IV. RESPONSABILIDADES

4.1. De las Funciones de la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres tiene las siguientes funciones:

- ✓ Formular el Plan de continuidad operativa del SANIPES, tomando en cuenta las actividades críticas de las Direcciones/Oficinas.

- ✓ Elaborar y desarrollar los instrumentos técnicos que el SANIPES pueda utilizar para la planificación, organización, ejecución y seguimiento de las acciones de estimación, prevención y reducción de riesgos.

4.2. El/la jefe/a de la Unidad de Atención al Ciudadano y Gestión Documental (UACGD), es responsable de:

- ✓ Proponer los instrumentos de Gestión preventivos y de acción ante cualquier hecho fortuito que se presente en las instalaciones de la sede central del Organismo Nacional de

Sanidad Pesquera – SANIPES.

- ✓ Asegurar que el personal de la Unidad actué frente cualquier hecho, ocurrencia, evento que pueda afectar a los procesos de la gestión documental (integridad de los documentos) y conservados en sus diferentes soportes tanto en el área de tramitación como en los diferentes niveles de Archivo.

4.3. El/la jefe/a de la Oficina de Tecnologías de la Información tendrá que garantizar:

- ✓ Asegurar la disponibilidad de los documentos electrónicos que se albergan en los sistemas de tramitación documental institucional y garantizar su cadena de custodia así como la gestión de archivos en todos los niveles.

4.4. El/la jefe/a de la Oficina de Administración, es responsable de:

- ✓ Dotar de materiales indispensables, para la respuesta oportuna ante algún suceso u ocurrencia que se pueda presentar y que afecte a la Gestión documental en todos sus niveles en el Organismo Nacional de Sanidad Pesquera (SANIPES).

V. DEFINICIONES

5.1. **Archivo:** Conjunto organizado de documentos archivísticos producidos por una persona natural o jurídica, entidad pública o privada en el ejercicio de sus funciones, respetando su procedencia y orden original, que son utilizados a modo de consulta por los servidores o la ciudadanía en general, independiente del soporte, espacio o lugar en que se resguarden. También puede ser entendido del soporte, espacio o lugar en que se resguarden también puede ser entendido por su dimensión institucional, como una unidad de organización o funcional que administra documentos archivísticos y brinda servicios de acceso.

5.2. **Archivo Central:** Es el ambiente donde se custodia los documentos archivísticos que han sido transferidos por los Archivos de Gestión una vez concluidos el trámite y cumplido el periodo de retención establecidos, conservando los documentos archivísticos producidos por la entidad pública, como parte de la fase semiactiva e inactiva del ciclo vital del documento archivístico.

5.3. **Cadena de custodia o preservación:** Sistema de controles que se extiende sobre todo el ciclo de vital de los documentos archivísticos que se custodian y preservan en la entidad para asegurar su registro, identidad, autenticidad, fiabilidad, integridad, disponibilidad y usabilidad a lo largo del tiempo.

5.4. **Disponibilidad:** Cualidad o característica de un documento archivístico para ser localizado, recuperado, legible, consultado, presentado o interpretado. El documento archivístico debe señalar la actividad o actuación donde se generó; proporcionar la información necesaria para la compresión de las actuaciones que motivaron su creación y utilización; identificar el contexto marco de las actividades y las funciones de la entidad y mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actuaciones.

5.5. **Documento archivístico:** Documento producido (recibido o emitido) en el ejercicio de una función, procedimiento, actividad, tarea o acción por persona natural, institución pública o privada, contiene información de cualquier fecha, forma soporte físico y cualquier otro que se genere como resultado del avance tecnológico. Entiéndase también como documento de archivo.

5.6. **Documento electrónico:** Unidad básica estructurada de información, es susceptible de ser clasificada, transmitida, procesada o conservada utilizando medios electrónicos, sistemas de información o similares. Contiene información de cualquier naturaleza, es registrado en un soporte electrónico o digital, en formato abierto y de aceptación general, a fin de facilitar su recuperación y conservación en el largo plazo. Asimismo, tiene asociado datos que permiten su individualización, identificación, gestión y puesta al servicio del ciudadano. Entiéndase también como documento archivístico.

5.7. **Documento archivístico digital:** Documento electrónico que contiene información en soporte o medio digital y es conservado de manera segura como evidencia y/o activo de información, respetando su integridad documental. Es producido por una persona natural, persona jurídica

o una entidad pública, en el ejercicio de sus actividades, proceso, funciones y/o competencias.

- ✓ Documento digitalizado: Representación digital, obtenida a partir de un documento registrado en un medio o soporte físico, mediante un proceso de digitalización. Se puede considerar como una forma de producción de documentos electrónicos.

- ✓ Documento nativo digital: Documentos producidos originalmente en medios electrónicos y que permanecen en estos durante su ciclo vital.

5.8. **Expediente:** Conjunto organizado e integrado de documentos producidos que son testimonio y prueba de una o varias acciones sujetas a un procedimiento administrativo agregado de tal forma que pueda ser recuperado para una acción o como evidencia.

5.9. **Expediente electrónico:** Conjunto organizado de documentos archivísticos digitales que respetando su integridad documental están vinculados lógicamente y forman parte de un procedimiento administrativo o servicio prestado en exclusividad en una determinada entidad de la administración pública, conforme a lo establecido en el artículo 31 TUO de la ley 27444. Asimismo, todas las actuaciones del procedimiento se registran y conservan íntegramente y en orden sucesivo en el expediente electrónico.

5.10. **Fiabilidad:** Característica o cualidad de un documento archivístico cuando su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades, manteniendo sus atributos de contexto y procedencia.

5.11. **Trámite documentario o mesa de partes:** Es el área encargada de la recepción, registro y distribución de la documentación ingresada al SANIPES, producto del inicio de un procedimiento TUPA.

VI. DISPOSICIONES GENERALES

TIPOS DE EVENTOS:

Incendio: La ocurrencia de un incendio en la Sede Central del SANIPES, podría ocasionar daños a los mobiliarios, equipos y documentos que serían incinerados, afectaría el equipamiento informático perdiendo su operatividad paralizando los procesos informáticos que la entidad realiza a través de los aplicativos entre ellos al sistema documentario, con los que se atienden los distintos servicios que se brindan a los usuarios internos y externos.

Sismo: Lima se encuentra localizada en un área altamente sísmica, ello debido a su proximidad continental con el Cinturón de Fuego del Pacífico, lo que genera que se encuentre expuesto a sismos de gran intensidad, con una recurrencia constante a nivel nacional, asimismo, existe un silencio sísmico que se viene prolongando desde el último terremoto de 1746 ocurrido en Lima, el mismo que provocó un tsunami; es así que, estudios científicos realizados proyectan la ocurrencia de un evento sísmico de gran magnitud con intensidad de 8.8 MM en la escala de Mercalli, seguido de un Tsunami, lo que ocasionará la afectación de la infraestructura de las instalaciones del PRODUCE, generando la interrupción de las actividades, los equipos, así como la interrupción del sistema de gestión documentaria y posible pérdida de los archivos.

Inundación: En caso de inundaciones las causas más comunes son generadas por fallas en las conexiones de agua potable y alcantarillado, al encontrarnos en instalaciones arrendadas el servicio de mantenimiento realiza las coordinaciones respectivas para no afectar a la documentación que se encuentre susceptible a ser humedecerse y que se encuentre próximo a estos ambientes.

Sabotaje: La ocurrencia de un sabotaje en la sede central del SANIPES y en la Sede Ventanilla del Archivo Central, podría generar daños, averías y la obstrucción del correcto funcionamiento del sistema documentario y a los documentos almacenados en ambas sedes. Este sabotaje es producto de la agitación violenta de carácter social o político, realizado por parte de colectivos sociales fuera de control, con el fin de alterar el orden y la normalidad de

las actividades realizadas en la entidad, tomando el espacio público e instalaciones para la atención de sus demandas.

VII. DISPOSICIONES ESPECÍFICAS

7.1. Mesa de partes / Atención, orientación al ciudadano.

El presente protocolo se debe aplicar en la recepción de documentos en la mesa de partes de la sede central del SANIPES, ante los eventos de incendio, sismo, inundación y/o sabotaje, los cuales implicarían 02 situaciones:

- ✓ De carecer de energía eléctrica en los módulos de trabajo,
- ✓ De contar con energía eléctrica y sin sistema de tramite documentario

7.1.1. De carecer de energía eléctrica en los módulos de trabajo.

a) Recepción de documentos:

- ✓ A través de la mesa de partes en forma presencial, se usará sello de recepción y será derivado físicamente a la dependencia, con el correspondiente cargo.
- ✓ Se le genera un registro de 9 dígitos + el año + iniciales del/a asistente de mesa partes, el cual se anotará a puño y letra a continuación del sello de recepción del documento original, así como en la copia que conservará el administrado

- ✓ El código a generar se inicia con el 00000001-año-Iniciales del/a asistente de mesa de partes que recibe la documentación. La recepción de dichos documentos se regulariza una vez se restablezca la energía eléctrica, así como el funcionamiento del Sistema de trámite documentario, manteniendo su orden de ingreso.

- ✓ La mesa de partes que regulariza el documento en el Sistema de tramite documentario, coloca obligatoriamente dentro del campo “asunto” el código manual generado al momento de recibir el documento en mesa de partes física.

- ✓ Cada asistente de mesa partes elabora el Excel Anexo 01: Formato de Recepción de Documentos, que es alimentado con cada registro que genere, con la data que se precisa a continuación:

    - o Número de registro, en orden consecutivo, evitando la repetición.
    - o Fecha y hora de recepción.
    - o Nombre o razón social del administrado.
    - o DNI / RUC (dependiendo si es persona natural o jurídica).
    - o Dirección en la que se le hará llegar las comunicaciones que recaigan en su trámite, en tanto no se restablezca la energía eléctrica.
    - o Correo electrónico, para cuando se restablezca.
    - o Número de teléfono, celular y fijo si tuviese.
    - o El asunto de su solicitud claramente definido (al final del asunto se debe colocar el número de Registro manual generado para ese documento).
    - o Número de folios.
    - o Observaciones de ser necesarias.

- ✓ Una vez que retorne la energía eléctrica; así como, el funcionamiento del Sistema de trámite documentario y a fin de gestionar electrónicamente, la digitalización y grabación de los documentos y expedientes ingresados que se encuentren en trámite, se debe realizar el proceso de regularización de los documentos en el Sistema de trámite documentario a partir de los formatos generados por cada operador y seguidamente regular su gestión o flujo documentario por el área responsable de su atención. Para tal fin, se establecerá un cronograma.

b) Derivación de la documentación a las dependencias

- ✓ El reparto de la documentación a las dependencias para su atención se llevará a cabo en dos cortes horarios: a las 10:30 horas (de lo ingresado en el transcurso de la mañana hasta esa hora) y un segundo corte a las 14:30 horas, lo que ingrese posteriormente se despachará al

día siguiente hábil. Se recibirá bajo cargo manual según listado.

c) Emisión de documentos por las dependencias

- ✓ Cada dependencia, generará el registro de los documentos que emite, de forma manual el cual estará conformado por 8 dígitos + año + SANIPES + siglas de la Sede. Se inicia del 00000001 cada tipo documental. En dicho registro se deberá especificar: fecha y hora de emisión, nomenclatura del documento, asunto del documento, y a quién deriva el documento

- ✓ Una vez que se restablezca la energía eléctrica y los sistemas que se requieren para la gestión documental, las Dependencias procederán a digitalizar los documentos y expedientes que se encuentren en trámite en sus oficinas o direcciones para proseguir el trámite electrónicamente, incorporándolo al Sistema de trámite documentario mediante proveído

7.1.2. De contar con energía eléctrica y sin Sistema de tramite documentario

a) Recepción de documentos

- ✓ Se recibe a través del correo electrónico tramitesdoc@sanipes.gob.pe y se deriva por el mismo medio a la dependencia competente para su atención, para tal efecto cada dependencia debe contar con un correo genérico con las siglas que las identifican, al cual se remitirá la documentación que ingrese a la entidad para su atención.

- ✓ Los/as asistentes de mesa de partes, convierten los documentos que registran a la extensión PDF, para asegurar su integridad. Se considera recibido de manera inmediata por las sedes, todo correo que derive documentos, enviado por los/as asistentes de mesa de partes.

- ✓ A continuación, las/os asistentes de mesa de partes, le generan un registro de 8 dígitos + el año + iniciales de operador, el cual se comunica al administrado respondiendo el correo electrónico mediante el que fue remitido el documento al SANIPES y luego lo deriva a la unidad orgánica competente.

- ✓ El código a generar se inicia con el 00000001-año-Iniciales, del/la asistente de mesa partes que recibe la documentación.

- ✓ La recepción de dichos documentos es regularizada una vez se restablezca el funcionamiento del Sistema de tramite documentario, manteniendo su orden de ingreso. Asimismo, adiciona en el campo “asunto” (sin modificar el asunto original del correo) el código de 08 dígitos + el año + iniciales del /la asistente de mesa partes, que recibe el correo electrónico.

- ✓ Cada asistente de mesa de partes, elabora un registro en Excel Anexo 02: Formato de recepción virtual de documentos, que es alimentado con cada registro que genera, con la data que se precisa a continuación:

    - Número de registro, en orden consecutivo, evitando la repetición.
    - Fecha y hora de recepción.
    - Nombre o razón social de administrado.
    - DNI / RUC (dependiendo si es persona natural o jurídica).
    - Dirección en la que se le hará llegar las comunicaciones que recaigan en su trámite.
    - Correo electrónico, para cuando se restablezca el funcionamiento del Sistema de trámite documentario.
    - Número de teléfono, celular y fijo si tuviese.
    - El asunto claramente definido, (al final del asunto se debe colocar el número de Registro manual generado para ese documento).
    - Número de folios.
    - Observaciones de ser necesarias

- ✓ Una vez que se reestablezca el funcionamiento del Sistema de trámite documentario a fin de gestionar electrónicamente la digitalización y grabación de los documentos y expedientes ingresados que se encuentren en trámite, se debe realizar el proceso de regularización de los documentos en el Sistema de tramite documentario a partir de los formatos generados por

cada asistente de mesa partes y seguidamente regular su gestión o flujo documentario por el área responsable de su atención. Para tal fin, se establecerá un cronograma.

b) Emisión de documentos

- ✓ Las dependencias generarán documentos electrónicos en extensión PDF y en caso se pueda hacer uso de los certificados, con la firma digital correspondiente.
- ✓ Cada dependencia procederá a atender la solicitud, produciendo sus documentos con los registros manuales en tanto no se regularice el funcionamiento del Sistema de trámite documentario.
- ✓ Se mantendrá el mismo criterio de codificación. Tipo documental (memorando, informe, carta, oficio, resolución, cédula de notificación) + número de 8 dígitos + año + SANIPES/ sede que lo produce y una vez emitido se convertirá a PDF, de ser posible firmar digitalmente se efectúa.
- ✓ Cada Dependencia lleva un registro manual de los tipos documentales que genere, con numeración correlativa, descripción del asunto, fecha y Dependencia a la que fue dirigida.
- ✓ Una vez se restablezca el funcionamiento del Sistema de trámite documentario se comenzará a generar los tipos documentales desde el número siguiente al último registro manual efectuado por cada tipo documental. Esta funcionalidad es habilitada por la Oficina de Tecnologías de la información a fin de regularizar los números de registro emitidos manualmente.
- ✓ El/la asistente de mesa de partes que regulariza en el Sistema de trámite documentario, el documento o expediente recibido y derivado por correo electrónico, incluye obligatoriamente dentro del campo “asunto” el código generado manualmente.
- ✓ El/la jefe/a encargado/a designará un responsable que llevará un control estricto del registro de los documentos recibidos en las contingencias.

7.2. Correspondencia y notificaciones

El presente Protocolo se debe aplicar en la recepción de correspondencia emitida por las sedes del SANIPES, ante los eventos de Incendio, Sismo, Inundación y/o Sabotaje.

De no contar con los equipos informáticos disponibles en la Sede Central del SANIPES para el desarrollo de las actividades, las/os asistentes de mesa partes se dividirán en dos grupos rotativos, el primer grupo asistirá en la modalidad de trabajo presencial y será responsable de todas las atenciones de la correspondencia en físico; así como, recepción, verificación, derivación, registro de datos de notificación, digitalización de cargos (de ser el caso) y devolución de cargos “físicos” mediante el Excel Anexo 03: Formato reporte de cargos devueltos de las unidades de organización.

El segundo grupo estará a cargo de la verificación, aceptación, derivación por los canales virtuales asignados de notificación, registro de datos de notificación y la devolución de cargos digitales y/o acuse de recibo mediante correo electrónico institucional, el cual será remitido al personal responsable de cada sede que corresponda, para continuidad de los procesos.

Al finalizar el día de la atención, las/os asistentes de mesa partes que se encuentren en la modalidad de trabajo remoto remitirían al jefe/a de la Unidad de Atención al Ciudadano y Gestión Documental un correo con el resumen y detalle de las atenciones del día.

7.2.1. Documentos emitidos por las dependencias del SANIPES.

a) Tratamiento en físico

- ✓ Procedimiento para la recepción de correspondencia:
  - o La recepción de la correspondencia externa emitida para su notificación en “físico” tales como: Oficios, Cartas, Múltiples y Cédulas de Notificación Personal, se efectuará en el horario publicado por la Unidad de Atención al Ciudadano y Gestión Documental y en el ambiente que el equipo de seguridad y salud en el trabajo deberá destinar para tal fin.
  - o Los documentos deben ser entregados en sobre cerrado, rotulados con el número de

documento, destinatario y domicilio completo y/o de corresponder referencias del domicilio, con el "cargo" del documento engrapado en el sobre.
- El/la asistente de mesa partes, verificara el rótulo del sobre y documento que indique "CARGO" y anotarán a manuscrito por orden de llegada los datos del documento en el formato establecido, Excel Anexo 04: Formato recepción y despacho de documentos diarios por tipo de servicio.

✓ Procedimiento para el despacho de correspondencia con el servicio de mensajería contratada:
- Al terminar el horario de recepción de la correspondencia, el/la asistente de mesa partes entregarán a la empresa de mensajería los documentos físicos con la relación de documentos, los cuales deberán de estar seleccionados de acuerdo al ámbito e importancia; "URGENTE, LOCAL, NACIONAL e INTERNACIONAL".
- La relación de documentos conforme al formato establecido en Excel Anexo 04: Formato recepción y despacho de documentos diarios por tipo de servicio debe ser entregada por duplicado.
- La empresa de mensajería verificará la cantidad de documentos y firmará el Excel Anexo 04: Formato recepción y despacho de documentos diarios por tipo de servicio por duplicado entregando una copia del formato, además de la Guía de Recojo en señal de conformidad.

✓ Procedimiento para el retorno de cargos
- La empresa de mensajería entregará a diario el listado de cargos diligenciados y/o notificados con los datos de recepción descritos en el formato Excel Anexo 05: Formato retorno de cargos y documentos atendidos por el servicio de mensajería de forma impresa y vía digital al correo electrónico del coordinador (a) de correspondencia del SANIPES en formato Excel.
- El/la asistente de mesa partes verificará y contrastará la relación de documentos y datos de notificación con los cargos físicos, de estar conforme se firmará el formato de devolución de Cargos en señal de conformidad por duplicado.

✓ Procedimiento para la devolución de cargos a las sedes del SANIPES
- El/la asistente de mesa partes clasificará los Cargos por Dependencias y elaborará el Excel Anexo 03: Formato reporte de cargos devueltos de las unidades de organización.
- Las Dependencias podrán recoger sus cargos en los horarios y en las instalaciones destinadas, las mismas que serán entregadas previa verificación y en señal de conformidad, el responsable asignado de cada Dependencia colocará su firma, nombres, apellidos, fecha y hora de recepción en el Excel Anexo 03: Formato reporte de cargos devueltos de las unidades organización por duplicado, una copia será entregada para el archivo y/o custodia de la Unidad de Atención al Ciudadano y Gestión Documental y la segunda copia será para la unidad de organización que corresponda.

- Una vez se restablezcan los servicios; así como, el funcionamiento del Sistema de tramite documentario a fin de gestionar electrónicamente, la documentación recepcionada, se debe realizar el proceso de regularización de los documentos en el Sistema a partir de los formatos generados por cada operador y seguidamente regular su gestión o flujo documentario por el área responsable de su atención. Para tal fin, se establecerá un cronograma.

b) Tratamiento en virtual

En caso los sistemas informáticos se encuentren operativos contamos con los siguientes canales virtuales de notificación, previa indicación y asistencia por parte de la Oficina de Tecnologías de la Información:

✓ Notificación por mesa de partes virtual – MVP: Se refiere a la Plataforma de Interoperabilidad del Estado - PIDE. La Plataforma Nacional de Interoperabilidad es una infraestructura tecnológica administrada por la Secretaría de Gobierno Digital que permite la Cooperación entre instituciones de la administración pública a través de internet y admite el envío y recepción de Oficios o Cartas.

En este proceso la Unidad de Atención al Ciudadano y Gestión Documental valida la información la cual debe contener los anexos y referencias citadas en el documento principal, de existir alguna observación se comunicará vía correo electrónico al personal responsable de cada sede para su subsanación o reenvío.

- ✓ Notificación "por correo electrónico": Para la Correspondencia externa tales como: Oficios, Oficios Múltiples, Cartas, Cartas Múltiples, Cédulas de Notificación Personal y Notificación de Imputación de Cargo, generado y/o emitidos por las unidades de organización del SANIPES para su notificación.

  Esta modalidad debe ser seleccionada cuando las unidades de organización envían la correspondencia externa para su notificación de forma directa a un correo electrónico autorizado por el administrado u entidad, a través de un link o a una página web, que funciona como mesa de partes, también cuando el administrado lo recoge en la misma oficina o cuando un colaborador de la misma oficina lo entrega en el domicilio del administrado.

  Si se realiza la notificación usando esta modalidad "por correo electrónico" es responsabilidad del personal administrativo de la unidad de organización realizar esta tarea; registrar los datos de la notificación y subir la imagen del cargo, constancia de entrega o acuse de recibido en al Sistema de trámite documentario.

7.3. Archivos de gestión y Archivo Central

Procedimientos a seguir en caso de eventos fortuitos vinculados a desastres de inundación, incendio, sismo y situaciones de orden público o sabotaje.

7.3.1. Procedimiento ante una inundación:

a) Acciones a tomar durante una inundación:
   - ✓ Cortar inmediatamente el fluido eléctrico. (Debe designarse a un titular y un suplente).
   - ✓ Desconectar todo tipo de aparato eléctrico. (Debe designarse a un titular y un suplente).
   - ✓ Cerrar la llave general del agua.
   - ✓ Activar o dar la alarma al superior jerárquico, personal presente, al personal de seguridad interna para que apoye en la comunicación inmediata a Servicios Generales y a la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión de Riesgo de Desastres sobre el siniestro.
   - ✓ Cubrir los documentos con plástico si la inundación proviniera del techo.
   - ✓ Evacuar cuidadosamente los documentos afectados, priorizando la documentación más valiosa a ambientes adecuados con áreas ventiladas donde no reciban la luz solar directamente.
   - ✓ Expulsar el agua empozada mediante el uso de baldes, recogedores, escobas, mangueras, esponjas, etc.
   - ✓ Si hubiera documentación sumergida es preferible no extraerla sin antes haber expulsado la totalidad del agua ya que el documento húmedo se vuelve muy frágil y corre el riesgo de destrozarse.
   - ✓ Colocar mediante extensiones aéreas de fluido eléctrico, ventiladores y deshumedecedores en las zonas afectadas. De no contar con deshumedecedores proponer su adquisición ante la Oficina de Administración.
   - ✓ En caso de intervención de personal externo al archivo para apoyar en las acciones a tomar durante y después de la inundación; el responsable Archivo Central deberá mantenerlos en constante orientación.
   - ✓ De ser necesario, comunicarse con las autoridades de Defensa Civil y Compañía de Bomberos.

b) Acciones a tomar después de una inundación:

   - ✓ En caso de que el agua haya ingresado a los repositorios se deberá verificar el nivel alcanzado. Si el agua alcanzo las baldas de las estanterías, deberá evacuarse las cajas afectadas.
   - ✓ Adecuar ambientes para el traslado seguro de la documentación recuperable, para proceder a su recuperación.
   - ✓ Sacar la documentación de las cajas archiveras y aplicar de manera inmediata medidas de recuperación.

- ✓ En caso de que el volumen documental afectado sea poco y pueda ser recuperado de manera inmediata, será necesario extender cordeles y colgar los documentos con ganchos plásticos en lugar ventilado, para su secado o extenderlos sobre mesas o anaqueles, para luego ser sometidos a ventilación natural o artificial. Nunca exponerlos al calor ni a la incidencia directa de rayos solares.
- ✓ Colocar papel secante entre las hojas de los documentos para evitar que se peguen entre sí. Alternativamente al papel secante puede usarse papeles blancos o cartulinas porosas absorbentes.
- ✓ No almacenar en cajas la documentación antes que esté totalmente seca.
- ✓ Evitar la activación del fluido eléctrico mientras haya humedad en el local.
- ✓ Verificar el contenido de los documentos con los instrumentos archivísticos existentes como inventarios, guías, catálogos, cuadernos de cargo, entre otros, para identificar pérdidas.
- ✓ Se deberá inventariar los documentos deteriorados, a fin de conocer la magnitud del daño para establecer un cuadro de prioridades de acción a través de la valoración de las series documentales afectadas.
- ✓ El local deberá ser limpiado y fumigado para evitar la proliferación de agentes contaminantes.
- ✓ En caso de identificar el extravío de documentos, estos deberán ser descritos mediante informe a la Unidad de Atención al Ciudadano y Gestión Documental.
- ✓ El/la jefe/a de la Unidad de Atención al Ciudadano y Gestión Documental es quien gestiona hace de conocimiento al Comité Evaluador de Documentos, quien mediante Acta de comité remite a la unidad de organización correspondiente para determinar las responsabilidades.
- ✓ Mientras dure la recuperación de los documentos deteriorados, las solicitudes de servicio archivístico podrán ser atendidas con los documentos que estén identificados, ubicados y en buen estado de conservación. Para ello deberá contarse con los recursos mínimos siguientes:
    - Personal capacitado en el proceso de servicio archivístico,
    - Un lugar seguro, ventilado y seco donde trabajar,
    - Energía eléctrica, de no ser factible iluminación con medios idóneos,
    - Un computador con los inventarios documentales correspondientes, de no contar con energía eléctrica, en forma manual,
    - Conexión a internet.

- ✓ Informar mensualmente a la Unidad de Atención al Ciudadano y Gestión Documental sobre el avance de los trabajos de recuperación, tanto de los documentos existentes como de las instalaciones

7.3.2. Procedimiento ante un incendio

a) Acciones a tomar ante un incendio

- ✓ Activar o dar la alarma.
- ✓ Utilizar los extintores, inmediatamente al inicio del fuego.
- ✓ Evacuar de inmediato el local, sin correr.
- ✓ El personal designado deberá cortar la energía eléctrica
- ✓ Llamar a la brigada contra incendios y a los Bomberos según sea el caso. Los teléfonos de emergencia se encuentran indicados en todas las puertas de acceso en todos los pisos de la sede Ventanilla.
- ✓ El personal de vigilancia deberá constatar, con el apoyo del listado de ingreso, que todos hayan evacuado el edificio.
- ✓ Informar a la Unidad de Atención al Ciudadano y Gestión Documental, a Servicios Generales y a la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión de Riesgo de Desastres sobre el siniestro.
- ✓ Evacuar los documentos pertenecientes a las series documentales vitales, que son los más importantes dentro de los documentos de valor permanente.

b) Acciones a tomar después de un incendio

- ✓ Informar a la Unidad de Atención al Ciudadano y Gestión Documental, de lo acontecido.
- ✓ Luego de apagado el fuego, verificar el área afectada.
- ✓ Adecuar ambientes para el traslado seguro de la documentación recuperable, para proceder a su recuperación, que comprende la revisión y tratamiento conforme a los procedimientos archivísticos.
- ✓ Proceder a la recuperación del material siniestrado el cual debe ser tratado solo por personal especializado.
- ✓ Verificar el contenido de los documentos con los instrumentos archivísticos existentes como

inventarios, guías, catálogos, entre otros, para identificar pérdidas.

- ✓ Se deberá inventariar los documentos deteriorados, a fin de conocer la magnitud del daño para establecer un cuadro de prioridades de acción a través de la valoración de las series documentales afectadas.
- ✓ El local deberá ser habilitado, limpiado y fumigado.
- ✓ En caso de identificar el extravío de documentos, estos deberán ser descritos mediante informe a la Unidad de Atención al Ciudadano y Gestión Documental.
- ✓ Presentar la denuncia correspondiente ante las autoridades competentes.
- ✓ Mientras dure la recuperación de los documentos deteriorados, las solicitudes de servicio archivístico podrán ser atendidas con los documentos que estén identificados, ubicados y en buen estado de conservación. Para ello se deberá contar con los siguientes recursos:
  - o Personal capacitado en el proceso de servicio archivístico,
  - o Un lugar seguro, ventilado y seco donde trabajar,
  - o Energía eléctrica. De no ser factible iluminación con medios idóneos,
  - o Un computador con los inventarios documentales correspondientes,
  - o Conexión a internet.

- ✓ Informar mensualmente a la Unidad de Atención al Ciudadano y Gestión Documental sobre el avance de los trabajos de recuperación, tanto de los documentos existentes como de las instalaciones

7.3.3. Procedimiento ante un sismo

a) Acciones a realizar un sismo:

- ✓ Evacuar de inmediato el local, sin correr, con las manos colocadas sobre la cabeza, y dirigirse a la zona segura definida.
- ✓ El personal designado deberá cortar la energía eléctrica.
- ✓ Al culminar el sismo, se deberá contar y verificar al personal con el listado de ingreso de personal de Vigilancia.
- ✓ Esperar la orden de la sede Central del SANIPES y de Unidad Funcional de Seguridad y Defensa Nacional y de Gestión de Riesgo de Desastres sobre las siguientes acciones a seguir.

b) Acciones a tomar luego de un sismo:

- ✓ Informar a la Unidad de Atención al Ciudadano y Gestión Documental, de lo acontecido.
- ✓ Esperar una decisión técnica y especializada, según la intensidad del sismo y el rigor de los daños causados, a efectos de iniciar el levantamiento de la documentación y mobiliario, la eliminación de polvo, y el descarte de posibles desprendimientos. Adecuar ambientes para el traslado seguro de la documentación recuperable, para proceder a su recuperación.
- ✓ Verificar el contenido de los documentos con los instrumentos archivísticos existentes como inventarios, guías, catálogos, cuadernos de cargo, entre otros, para identificar pérdidas.
- ✓ Se deberá inventariar los documentos deteriorados, a fin de conocer la magnitud del daño para establecer un cuadro de prioridades de acción a través de la valoración de las series documentales afectadas.
- ✓ Aplicar un proceso de recuperación, limpieza, y reordenamiento de la documentación que conforma las series documentales vitales que son los más importantes dentro de los documentos de valor permanente, con brochas y aspiradoras, para ubicarlas en cajas archivadoras. Al finalizar estas, se proseguirá con el resto de las series documentales conforme a su valoración.
- ✓ El local deberá ser evaluado, reparado, limpiado y fumigado.
- ✓ En caso de identificar el extravío de documentos, estos deberán ser descritos mediante informe a la Unidad de Atención al Ciudadano y Gestión Documental.
- ✓ Convocar a sesión de Comité Evaluador de Documentos de existir perdida documental.
- ✓ Mientras dure la recuperación de los documentos deteriorados, las solicitudes de servicio archivístico podrán ser atendidas con los documentos que estén identificados, ubicados y en buen estado de conservación. Para ello se deberá contar con los siguientes recursos:
  - ▪ Personal capacitado en el proceso de servicio archivístico,
  - ▪ Un lugar seguro, ventilado y seco donde trabajar,
  - ▪ Energía eléctrica; De no ser factible iluminación con medios idóneos,
  - ▪ Un computador con los inventarios documentales correspondientes,
  - ▪ Conexión a internet.

- ✓ Informar mensualmente a la Unidad de Atención al Ciudadano y Gestión Documental sobre el avance de los trabajos de recuperación, tanto de los documentos existentes como de las instalaciones.

7.3.4. Procedimiento ante situaciones de orden público o sabotaje.

a) Acciones a tomar durante una situación de orden público o sabotaje
   - ✓ Resguardar la vida y salud de las personas.
   - ✓ En caso de ser posible, documentar la situación con fotografías o audiovisuales.
   - ✓ Informar a las autoridades competentes sobre la situación, e informar a la Unidad de Atención al Ciudadano y Gestión Documental.

b) Acciones a tomar después de una situación de orden público o sabotaje.
   - ✓ Informar a la Unidad de Atención al Ciudadano y Gestión Documental de lo acontecido.
   - ✓ Realizar un diagnóstico para evaluar el grado de pérdida de documentación.
   - ✓ Registrar gráficamente el estado de los espacios destinados a la custodia de los documentos.
   - ✓ Verificar el contenido de los documentos con los instrumentos archivísticos existentes como inventarios, guías, catálogos, cuadernos de cargo, entre otros, para identificar pérdidas.
   - ✓ Se deberá inventariar los documentos deteriorados, a fin de conocer la magnitud del daño para establecer un cuadro de prioridades de acción a través de la valoración de las series documentales afectadas.
   - ✓ Aplicar el plan de prevención de siniestros para la recuperación, limpieza, y reordenamiento de la documentación siniestrada, teniendo prioridad las series documentales vitales que son los más importantes dentro de los documentos de valor permanente, prosiguiendo con el resto de las series documentales conforme a su valoración.
   - ✓ En caso de sufrir daños, el local deberá ser evaluado, reparado, limpiado y fumigado.
   - ✓ En caso de identificar el extravío de documentos, estos deberán ser descritos mediante informe a su autoridad superior, con copia a Unidad de Atención al Ciudadano y Gestión Documental.
   - ✓ Informar mediante sesión al Comité Evaluador de Documentos en caso de identificar el extravío de documentos.
   - ✓ Mientras dure la recuperación de los documentos deteriorados, las solicitudes de servicio archivístico podrán ser atendidas con los documentos que estén identificados, ubicados y en buen estado de conservación. Para ello se deberá contar con los siguientes recursos:
     - o Personal capacitado en el proceso de servicio archivístico,
     - o Un lugar seguro, ventilado y seco donde trabajar,
     - o Energía eléctrica; De no ser factible iluminación con medios idóneos,
     - o Un computador con los inventarios documentales correspondientes,
     - o Conexión a internet.

   - ✓ Informar mensualmente a la Unidad de Atención al Ciudadano y Gestión Documental sobre el avance de los trabajos de recuperación, tanto de los documentos existentes como de las instalaciones.

7.4. Proceso de Escaneado dentro del Archivo Central

7.4.1. Caso de incendio

a) Procedimiento para la recepción y preparación de documentos
   - ✓ Trasladar toda la documentación a un ambiente que se encuentre fuera del incidente para registrar y organizar la documentación.
   - ✓ Realizar un inventario de toda la documentación afectada y los documentos que se encuentran en buen estado.
   - ✓ Separar la documentación afectada por el siniestro, recuperar toda la información necesaria e informar a la Unidad de Atención al Ciudadano y Gestión Documental el estado de la documentación y las pérdidas de información.

b) Procedimiento para el escaneo de documentos
   - ✓ Ante un evento de incendio en la Sede Central del SANIPES, La Unidad de Atención al Ciudadano cuenta con equipos y escáneres en la Sede del Archivo Central, puesto que, representa un plan de contingencia para continuar con la digitalización de documentos provenientes de la mesa de partes y el archivo central, hasta que se dé la autorización de volver al área correspondiente.

c) Procedimiento entrega de documentos a las unidades de organización
   - ✓ La derivación de los documentos presentados por la mesa de partes, se hará de manera digital a través de los correos electrónicos institucionales u otro sistema que habilite la Oficina de Tecnologías de la Información.
   - ✓ El reparto de la documentación física a las dependencias para su atención se llevará a cabo en dos cortes horarios: a las 10:30 horas (de lo ingresado en el transcurso de la mañana hasta esa hora) y un segundo corte a las 14:30 horas, lo que ingrese posteriormente se despachará al día siguiente hábil. Se recibirá bajo cargo manual según listado (este proceso se realizará previa coordinación con las unidades de organización competentes).

7.4.2. Caso falla eléctrica

a) Procedimiento para la recepción y preparación de documentos
   - ✓ El/la asistente de mesa partes o en Archivo Central verificará la relación de documentos ingresados y los guardará de manera ordenada según el numero correlativo.
   - ✓ Se clasificará y se dará atención a la documentación ingresada, según la hora de ingreso del documento y la urgencia de lo solicitado.

b) Procedimiento para el escaneo de documentos.
   - ✓ En la mesa partes sólo se emplearán los equipos si se llega a contar con equipos eléctricos para su funcionamiento.
   - ✓ Hasta el retorno de la energía eléctrica, los documentos físicos serán trasladados a la sede del Archivo Central para continuar con el escaneo de documentos y evitar retraso en la reproducción de las imágenes.
   - ✓ Al reincorporarse la energía eléctrica, la documentación digitalizada será almacenada en los equipos de la Sede del archivo central, los cuales serán trasladados a la Unidad de Atención al Ciudadano y Gestión documental a través de discos duros para que se carguen en el Sistema de trámite documentario.

c) Procedimiento para la entrega de documentos a las unidades de organización

   - ✓ Se realizarán las coordinaciones con las unidades de organización competentes para el préstamo de los documentos físicos de alta prioridad, con el objetivo que puedan trabajar con ello hasta que se restablezca la energía eléctrica y, por consiguiente, retorne la documentación al área para su escaneo.
   - ✓ La entrega de los documentos físicos, se hará a través de un formato de préstamo de documentos Excel Anexo 06: Formato de préstamo de documentos, donde se registrará el número de registro, la cantidad de folios, dependencia receptora, razón social, hora de préstamo, firma del Responsable del Archivo Central que entrega y firma del personal de la unidad de organización que recepciona, asimismo durante el retorno de la documentación se firmará la devolución.

VIII. DISPOSICIONES COMPLEMENTARIAS

Única: El presente protocolo entra en vigencia a partir de la aprobación del Plan de Continuidad Operativa de SANIPES a cargo de la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión de Riesgo de Desastres.

IX. ANEXOS

Anexo 01: Formato de recepción de documentos
Anexo 02: Formato de recepción virtual de documentos
Anexo 03: Formato reporte de cargos devueltos a las unidades de organización de SANIPES.
Anexo 04: Formato recepción y despacho de documentos diarios por tipo de servicio.
Anexo 05: Formato de retorno de cargos y documentos atendidos por el servicio de mensajería
Anexo 06: Formato de préstamo de documentos.

Anexo 01: Formato de recepción de documentos

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 01: FORMATO DE RECEPCIÓN DE DOCUMENTOS

N°	N° REGISTRO	FECHA	HORA	NOMBRE O RAZON SOCIAL	DNI / RUC	DOMICILIO	CORREO ELECTRONICO	NUMERO TELEFONO	ASUNTO	# FOLIOS	OBSERVACIONES

Anexo 02: Formato de recepción virtual de documentos

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 02: FORMATO DE RECEPCIÓN VIRTUAL DE DOCUMENTOS

N°	N° REGISTRO	FECHA	HORA	NOMBRE O RAZON SOCIAL	DNI / RUC	DOMICILIO	CORREO ELECTRONICO	NUMERO TELEFONO	ASUNTO	# FOLIOS	OBSERVACIONES

Anexo 03: Formato reporte de cargos devueltos a las unidades de organización de SANIPES

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 03: FORMATO REPORTE DE CARGOS DEVUELTOS DE LAS UNIDADES DE ORGANIZACIÓN

N°	CODIGO	N° DOCUMENTO	REMITENTE	RAZON SOCIAL	UNIDAD DE ORGANIZACIÓN	FECHA ENTRG. COURRIER	FECHA DEVOL. COURRIER	ESCANEADO	NOMBRE RECEPTOR	FECHA	HORA	OBSERVACIONES

Anexo 04: Formato recepción y despacho de documentos diarios por tipo de servicio.

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 04: FORMATO RECEPCIÓN Y DESPACHO DE DOCUMENTOS DIARIOS POR TIPO DE SERVICIO

N°	CODIGO	EXP.	DOC.	FECHA EMISIÓN	# DOCUMENTO	REMITENTE	RAZÓN SOCIAL	SEDE	TIPO DE SERVICIO	FECHA ENT. COURRIER	CLASE DOCUMENTO	# GUIA

Anexo 05: Formato de retorno de cargos y documentos atendidos por el servicio de mensajería

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 05: FORMATO RETORNO DE CARGOS Y DOCUMENTOS ATENDIDOS POR EL SERVICIO DE MENSAJERIA

N°	CODIGO	EXP.	DOC.	FECHA EMISIÓN	# DOCUMENTO	REMITENTE	RAZÓN SOCIAL	SEDE	TIPO DE SERVICIO	FECHA ENT. COURRIER	PERSONA QUE RECIBE	# GUIA	OBSERVACIONES

Anexo 06: Formato de préstamo de documentos.

SANIPES
Organismo Nacional de Sanidad Pesquera

ANEXO 06: FORMATO DE PRÉSTAMO DE DOCUMENTOS

UNIDAD DE ORGANIZACIÓN: ______________________________

N°	# DOCUMENTO	FECHA REGISTRO	FECHA RECEPCIÓN	TIPO DOCUMENTO	USUARIO DE ENTREGA	REMITENTE	FOLIOS	ESTADO DOCUMENTO	OBSERVACIONES

TOTAL DE DOCUMENTOS ENTREGADOS

ENTREGADO POR ______________________________ FECHA RECEPCIÓN ____________

RECIBIDO POR ______________________________ FECHA RECIBIDO ____________

DEVUELTO POR ______________________________ FECHA DEVOLUCIÓN ____________

OBSERVACIONES ______________________________

ANEXO N°03: PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES DEL SANIPES

1. FINALIDAD

   Garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la Organización Nacional de Sanidad Pesquera (SANIPES), a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

2. OBJETIVOS

   2.1 Objetivo General

   Establecer los principios básicos y el marco necesario para garantizar la operatividad de los servicios y/o procesos de tecnologías de la información y comunicaciones de mayor urgencia del SANIPES, ante la eventual presencia de siniestros que los pueda paralizar parcial o totalmente y garantizar que se continúen prestando de una manera razonable.

   2.2 Objetivos Específicos

   - Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.
   - Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
   - Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.
   - Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

3. ALCANCE

   El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Unidad Funcional de Tecnologías de la Información y Comunicación (UFTIC), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

4. BASE LEGAL

   - Ley Nº29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
   - Decreto Supremo N°018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
   - Decreto Supremo N°115-2022-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2022-2030.
   - Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
   - Resolución Ministerial N° 004-2016-PCM - Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.
   - Resolución Ministerial N°320-2021-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.

5. MARCO TEORICO

5.1 Plan de Contingencia Informático

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- Antes, como un plan de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

5.2 Incidente

Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en SANIPES.

5.3 Método de análisis de riesgos

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

En el Anexo 1, se detalla la metodología utilizada en el presente Plan.

5.4 Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

5.5 Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

5.6 Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

5.7 Plan de Pruebas

Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

6. METODOLOGIA

El desarrollo del presente Plan seguirá la siguiente metodología basada en siete (7) fases:

- Fase 1: Planificación
- Fase 2: Determinación de vulnerabilidades y escenarios de contingencia
- Fase 3: Estrategias

- Fase 4: Elaboración del Plan de Contingencia Informático
- Fase 5: Definición y Ejecución del Plan de Pruebas
- Fase 6: Implementación del Plan de Contingencia
- Fase 7: Monitoreo

A continuación, se detalla cada fase:

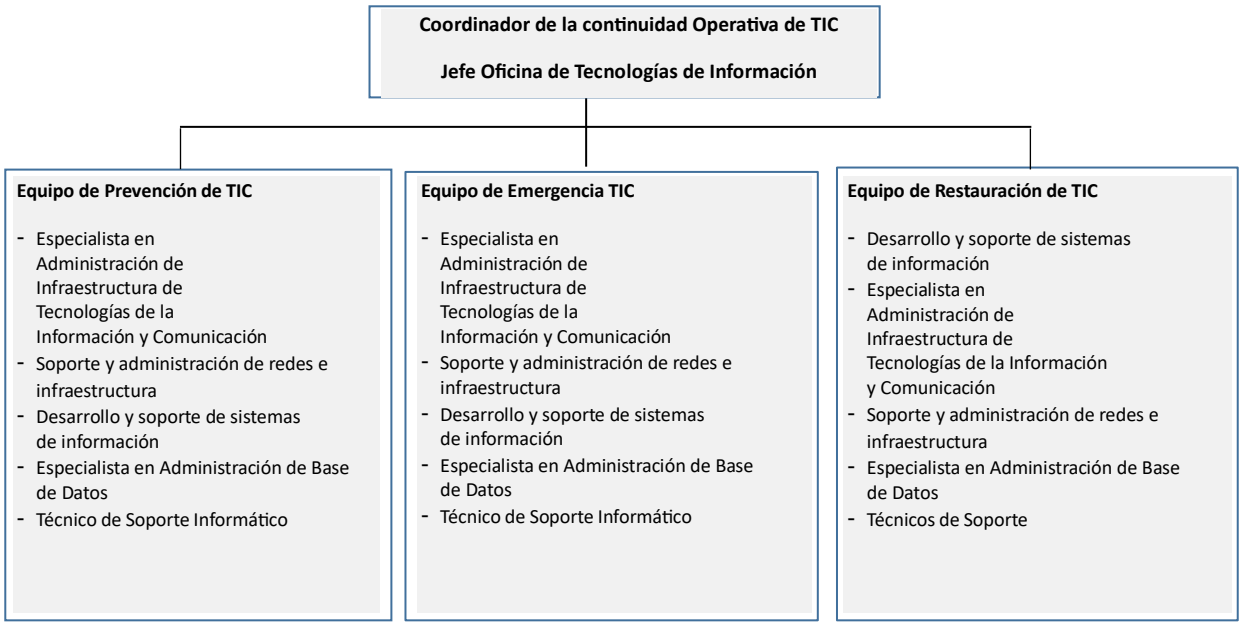
6.1 Fase 1: Planificación

6.1.1. Organización

La Oficina de Tecnologías de la Información (OTI) depende directamente de la Gerencia General (GG), y tiene dentro de sus funciones administrar la integridad, confiabilidad, y seguridad en el acceso de la base de datos institucional, así como establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos; además de diseñar, construir, implantar, mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos del SANIPES, así como asegurar la disponibilidad ybrindar soporte a los mismos.

Para el funcionamiento del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicación, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal de la UFTIC:

Figura N°1 – Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicación (TIC)



El Jefe de la Oficina de Tecnologías de la Información debe nombrar un miembro titular y un alterno, por cada integrante de los tres (3) equipos mencionados previamente, detallados en la Figura N°1. Para tal efecto,se debe contar con la relación del personal de la OTI que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

Asimismo, los responsables de cada Equipo previamente señalados deben estar atento y alertas para las comunicaciones pertinentes. De igual manera, los correos electrónicos registrados deben estar alojados en plataforma nube, que garantice la disponibilidad de este servicio.
La relación del personal de la OTI que forma parte del Plan de contingencia debe ser actualizada de manera permanente y socializada al siguiente personal:

- Personal de la OTI.
- Personal de la Alta Dirección.
- Personal de Servicios Generales (Personal de vigilancia).

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes.

6.1.2. Roles, funciones y responsabilidades dentro del Plan

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

a. Coordinador de Continuidad de TIC

Está representado por jefe de la OTI y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.
- Guiar y supervisar a los equipos operativos de contingencia informática, en el desarrollo de sus actividades.
- Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.
- Notificar y mantener informados, a la Alta Dirección acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicación, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización y en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicación, en el menor tiempo posible.

El responsable del Equipo de Prevención de TIC es el/la Especialista en Administración de Infraestructura de Tecnologías de la Información y Comunicación.

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

Especialista en Administración de Infraestructura de Tecnologías de la Información y Comunicación

- Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de desastres.

- Mantener actualizado el inventario hardware y software utilizado en elCentro de Datos de la entidad.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos, considerando el tiempo de vida útil y garantía de estos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación.

Soporte y administración de redes e infraestructura
- Monitorear el funcionamiento de la Central Telefónica
- Verificar que la central telefónica cuenta con las garantías requeridas.
- Mantener actualizada la lista de anexos y teléfonos.
- Actualizar el software que utiliza la central telefónica.

Desarrollo y soporte de sistemas de información
- Coordinar acciones de mantenimiento de sistemas de informaciónexistentes asegurando el cumplimiento del ciclo de vida de software
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- Coordinar y verificar que se realicen las copias de respaldo de las fuentes delos aplicativos informáticos existentes en un ambiente adecuado.
- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los logs de los aplicativos informáticos afectados durante la emergencia

Especialista en Administración de Base de Datos
- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Administración de Infraestructura de Tecnologías de la Información.

c. Equipo de Emergencia de TIC

Este equipo es el encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información de SANIPES, procurando salvaguardar su pérdida o deterioro.

A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Especialista en Administración de Infraestructura de Tecnologías de la Información y Comunicación
- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los equipos informáticos y

componentes instalados en el Centro de Datos de SANIPES.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos del SANIPES, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.
- Apoyar en las labores de verificación y validación de operación de los servicios de TIC.

Soporte y administración de redes e infraestructura
- Ejecutar las acciones de emergencia en los equipos celulares y central telefónica instalada en el Centro de Datos del SANIPES.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Desarrollo y soporte de sistemas de información
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.
- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los logs de los aplicativos informáticos afectados durante la emergencia

Especialista en Administración de Base de Datos
- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

Técnico de Soporte Informático
- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios de SANIPES.

d. Equipo de Restauración de TIC

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos de SANIPES.

Especialista en Administración de Infraestructura de Tecnologías de la Información y Comunicación
- Es el responsable del equipo de Restauración de TIC
- Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos de SANIPES.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos de SANIPES.
- Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.
- Elaborar *un informe técnico*, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.
- Supervisar la restauración de los servicios de TI.

- Validar la información documentada de los procedimientos de restauración utilizados.

Soporte y administración de redes e infraestructura

- Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el Centro de Datos de SANIPES, así como a los equipos móviles.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Elaborar *un informe técnico*, que incluya las acciones de recuperación de los equipos móviles y la central telefónica ubicada del Centro de Datos.

Desarrollo y soporte de sistemas de información

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información.
- Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.
- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones de SANIPES.
- En caso se quiera desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información de SANIPES.

Especialista en Administración de Base de Datos

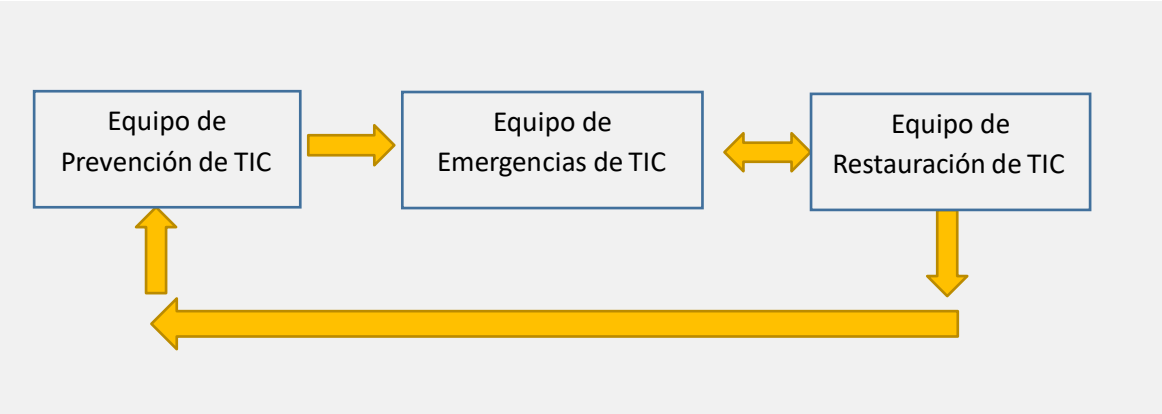
- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso searequerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información de SANIPES luego de efectuado el proceso de recuperación.

Técnico de Soporte

- Verificar el funcionamiento de los equipos personales de SANIPES afectadas, distribuyendo el trabajo entre el personal de soporte.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del personal de SANIPES, luego de efectuado el proceso de recuperación.

Cabe precisar que los equipos podrían ejecutar sus actividades paralelamente, de acuerdo al siguiente orden de operación:

Figura N°2 – Flujo del orden de operación de los equipos de TI



6.2 Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

En esta fase se procederá a la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

6.2.1. Procesos y recursos críticos

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Tabla N°1 – Procesos y recursos críticos de TI

Proceso crítico	Aplicaciones y/o recursos críticos	Tiempo de Recuperación (RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	12 h
	Equipos de protección eléctrica del centro de datos (UPS)	12 h
	Sistema de aire acondicionado del Centro de Datos	12 h
	Infraestructura del Centro de Datos	12 h
	Cableado de red de datos	12 h
	Enlaces de fibra óptica para Internet	12 h
	Sistema de almacenamiento (storage)	12 h
	Medios de respaldo (cintas de backup)	12 h
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	12h
	Servidores de red en general.	12h
	Central Telefónica	12h
Gestión de sistemas de información y bases de datos	Sistemas de información y portales core	12 h
	Sistemas de información administrativos	12 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	12 h
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	12 h
Operación y mantenimiento de TICS	Personal crítico responsable de los procesos de TIC.	4 h

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.

6.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios

TIC de SANIPES, considerando la ubicación geográfica, el contexto actual del centro de datos, así como la percepción del juicio experto.

Tabla N°2 – Amenazas a los servicios de TI

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en el Centro de Datos.	
03	Incendio en el Centro de Datos.	
04	Falla en telecomunicaciones.	Tecnológicos
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en el Centro de Datos y gabinetesde comunicación.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
09	Pandemia y/o Epidemia	Ambiental

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos. A continuación, se detalla el resultado obtenido:

Tabla N°3 – Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad estimada
01	Terremoto.	2	4	Moderado
02	Inundación y aniego en el Centro de Datos.	2	2	Menor
03	Incendio en el Centro de Datos.	1	3	Menor
04	Falla en telecomunicaciones.	3	4	Moderado
05	Delitos informáticos.	2	4	Moderado
06	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	3	3	Moderado
07	Falla del hardware y software.	3	3	Moderado
08	Ausencia o no disponibilidad del personal crítico de TI.	2	3	Menor
09	Pandemia y/o Epidemia	1	2	Menor

6.2.3. Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer que tan protegidos estánlos recursos de TI de SANIPES frente a cada amenaza.

- Acuerdos de niveles de servicio con proveedor de línea de internet de SANIPES.
- Cámaras de vigilancia en el interior del Centro de Datos.
- Mantenimiento de UPS, el cual está a cargo de la OTI.
- Mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Redundancia en los enlaces de internet (fibra óptica), pero con el mismo proveedor.
- Respaldo de servidores críticos.
- Solución antivirus instalada en los servidores de red y computadoras.

6.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico de SANIPES, se consideraron los controles existentes que mitigan la afectación de la amenaza

descritos en el punto 6.2.2 y de acuerdo a la aplicación de la metodología de riesgos descrita en el Anexo 1, se obtuvo el siguiente resultado:

Tabla N°4 – Resultado de la evaluación de riesgos de los servicios de TI

N°	**Recursos Críticos / Amenazas (Eventos)**	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Delitos informáticos	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.									
2	Equipos de protección eléctrica del centro de datos (UPS).									
3	Aire acondicionado de precisión del Centro de Datos.									
4	Infraestructura del Centro de Datos.									
5	Cableado de red de datos.									
6	Enlaces de fibra óptica para Internet.									
7	Sistema de almacenamiento (storage).									
8	Servidores de red									
9	Medios de respaldo (cintas de backup)									
10	Sistemas de información y portales web									
11	Base de datos utilizados por los sistemas y aplicativos.									
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)									
13	Personal crítico responsable de los procesos de TIC.									

6.2.5. Escenarios de riesgo

- Destrucción e indisponibilidad del centro de datos por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Tabla N° 5 – Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad del centro de Datos	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro datos, como también los componentes del mismo.	Extremo
Falla en el funcionamiento de los sistemas de información y portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.	Este escenario consiste en el corte o interrupción de las comunicaciones en el centro de datos, así como los servicios publicados en internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionaría caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Alto

6.3 Fase 3: Estrategias del Plan de Contingencia

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

6.3.1. Estrategias de prevención de tecnologías de la información

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

b) Sitios Alternos para el Centro de Datos
   El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; el sitio alternativo es el Centro de Datos del Ministerio de la Producción.

c) Evaluación y gestión de proveedores
   - Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
   - Mantener listas detalladas de necesidades de equipos y sus especificaciones

técnicas.

- Si es necesario, adquirir o habilitar hardware y software, así como transportarlos al sitio alterno de ser el caso; las estrategias básicas para disponer de equipo de reemplazo serán:

  - Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
  - Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa. (*)
  - Equipo compatible existente: Equipo existente en sitios alternativos.

  (*) Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación comience más rápidamente.

d) Entrenamiento y personal de reemplazo
   - Todo el personal de la OTI, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
   - Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de OTI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como del administrador de la infraestructura TI.
   - Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica
   - Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
   - Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro adquirir equipos de contingencia.

f) Activación de trabajo remoto
   - Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios TICs.
   - Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
   - En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la sede de SANIPES, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Administración.
   - Activación del desvío de las llamadas telefónicas a los usuarios asignados encargados de la atención de la central telefónica.
   - Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios TICs, a cargo de la OTI en el Centro de Datos.

6.3.2. Estrategia frente a emergencias en tecnologías de la información

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

emergencia o desastre. A continuación, se citan las acciones que se realizarán durante y después de una contingencia:

Acciones durante la contingencia

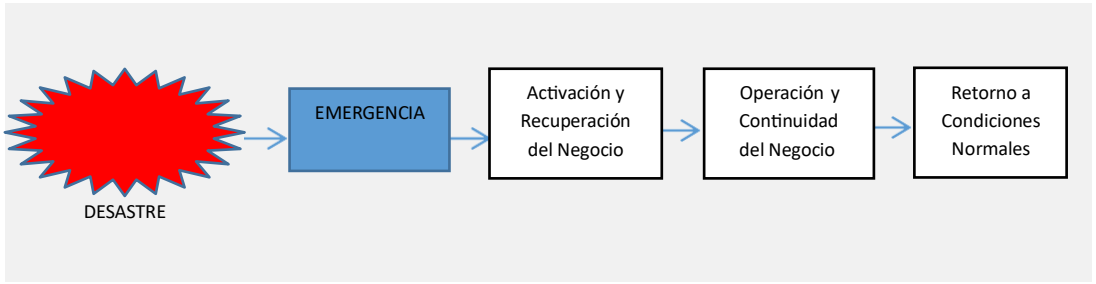
- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
- Informar a la Alta Dirección sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación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

6.3.3. Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos de SANIPES para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cualse definen las pautas que permitan al personal de la OTI garantizar la continuidad de las operaciones en la entidad.

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

Figura N° 3 – Ciclo de la estrategia de recuperación de TI



La priorización de la restauración de los servicios de tecnologías de información de SANIPES se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

Tabla N° 6 – Prioridad de atención durante la restauración de TIC

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema Integrado de Gestión Administrativa (SIGA), Portal Web institucional, servidores de bases de datos, entre otros.

-

2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Primavera, etc.

En el Aneo 2 y Anexo 3 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

Acciones después de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

6.4 Fase 4: Elaboración del Plan de Contingencia y Recuperación de Servicios de TIC

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente.

El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información yComunicación comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N°7 – Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Terremoto /Sismo	Extremo	FPC - 01
2	Delito informático (ataque)	Extremo	FPC - 02
3	Falla de hardware y software	Extremo	FPC - 03
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Alto	FPC - 04

En el Anexo 4 se presenta el desarrollo de cada formato.

6.5 Fase 5: Definición y Ejecución del Plan de Pruebas

El plan de pruebas está enfocado principalmente en simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos de la UFTIC, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente

esquema:

- Metodología (descripción de la prueba a efectuarse)
- Alcances (áreas afectadas / personal involucrado)
- Resultados

Las pruebas relacionadas a este plan se deberán ejecutar semestralmente, en los meses de junio y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el Anexo N°5.

6.6 Fase 6: Implementación del Plan de Contingencia

La implementación del presente plan se realizará a partir del segundo mes de su aprobación.

Para tal efecto, el/la Oficial de Seguridad de la Información, realiza las siguientes funciones:

- Supervisar las actividades de copias de respaldo y restauración.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).
- Participar en las pruebas y simulacros de desastres.

6.7 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. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

- Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.
- Revisión continua de las aplicaciones, sistemas de información y portales web.
- Revisión continua del sistema de copias de respaldo (backups).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos.

ANEXOS

- Anexo 1 Metodología aplicada a la gestión de riesgos
- Anexo 2 Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC
- Anexo 3 Listado de equipos del Centro de Datos y Gabinetes de Comunicación clasificados por prioridad de atención para la recuperación de TIC
- Anexo 4 Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones por evento de riesgo
- Anexo 5 Formato de Control y certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones

ANEXO 1

METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. **Cálculo de la Probabilidad de Ocurrencia de la Amenaza**. Para realizar este cálculo, se toman en cuenta dos variables: “Ocurrencia” y “Percepción”.

   Se considera “ocurrencia” a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado al SANIPES directamente. Se consideró la siguiente tabla de valores para el cálculo:

N°	Ocurrencia	Descripción
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy Frecuente	Se presentó más de una vez al mes en el último año

   La “Percepción” está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

#	Percepción	Descripción
1	Muy Difícil	• <= 1% probabilidad, o • El acontecimiento requiere de circunstancias excepcionales, o • La probabilidad es nula, incluso en un futuro a largo plazo
2	Difícil	• >1% ó <=10% de probabilidad, o • Puede ocurrir, pero no será anticipada
3	Mediana	• >10% ó <=50% de probabilidad, o • Puede ocurrir en el mediano plazo
4	Posible	• >50% ó <=75% de probabilidad, o • Podría ocurrir anualmente
5	Muy Posible	• >75% ó 100% de probabilidad, o • El impacto está ocurriendo ahora, o • Podría ocurrir dentro de unos meses

   Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. **Identificación de las amenazas que se tomarán en cuenta para la evaluación**. De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

Nivel de Probabilidad Estimada	Interpretación
Extrema	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	Probabilidad de ocurrencia intermedia (Eval. de prioridad baja)
Menor	Probabilidad de ocurrencia muy baja (Eval. sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. **Cálculo de la Probabilidad de Afectación del Recurso.** Se utiliza la siguiente tabla de valores para el cálculo:

#	Probabilidad	Descripción
1	Improbable	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados
2	Baja	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas.
3	Moderada	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
4	Alta	Algunos controles se prueban esporádicamente, debido a que no cuentan conun programa definido o de existir no se cumple con el mismo.
5	Muy Alta	Bajo nivel de controles o los controles existentes no son efectivos o eficientes.

4. **Cálculo del Impacto del Recurso**. Se utiliza la siguiente tabla de valores para el cálculo:

#	Impacto	Descripción
1	No significativo	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada.
2	Menor	Afecta hasta en 6 horas las operaciones de la sede evaluada.
3	Moderado	Afecta hasta en 24 horas las operaciones de la sede evaluada.
4	Mayor	Afecta hasta en 48 horas las operaciones de la sede evaluada.
5	Catastrófico	Afecta por más de una semana las operaciones de la sede evaluada.

5. **Cálculo del Nivel de Riesgo**. Se calcula considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Afectación		**Impacto**				
		No Significativo (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Muy Alta	(5)	Alto	Alto	Extremo	Extremo	Extremo
Alta	(4)	Moderado	Alto	Alto	Extremo	Extremo
Moderada	(3)	**Bajo**	Moderado	Alto	Extremo	Extremo
Baja	(2)	**Bajo**	**Bajo**	Moderado	Alto	Extremo
Improbable	(1)	**Bajo**	**Bajo**	Moderado	Alto	Alto

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Nivel de Riesgo	Interpretación
Extremo	Riesgo no deseable, se requiere acción correctiva inmediata
Alto	Riesgo no deseable que requiere de una acción correctiva, pero se permite alguna discreción de la gerencia sobre los plazos y compromisos
Moderado	Riesgo aceptable con revisión de la dirección
Bajo	Riesgo aceptable sin revisión

ANEXO 2

LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema /Aplicativo	Breve descripción	Área Usuaria	Motor BD	Tipo	Prioridad
1	SIAF-MEF	Sistema Integrado de Administración Financiera	OA UA UCFT URH OPPM	SQL	Desktop	1
2	Servicios Web - PIDE	Integrar los servicios web de la Plataforma de Interoperabilidad del Estado (PIDE), de la ONGEI para consulta de información por parte del personal de SANIPES	OTI	No usa base de datos	Web	1
3	Portal Web Institucional	Página informativa de las actividades que viene realizando SANIPES.	GERENCIA GENERAL		Web	1
4	INTRANET	Control de asistencia: Verificación de asistencia, Gestión de Papeletas	UNIDAD RECURSOS HUMANOS	SQL	Web	1
		Gestión de usuario: Gestión de usuario de la Intranet	OFICINA TECNOLOGIA INFORMACION	SQL	Web	1
		Mesa de ayuda	OFICINA TECNOLOGIA INFORMACION	SQL	Web	1
		Página web: Publicación de Protocolos, Registros sanitarios.	GERENCIA GENERAL OFICINA TECNOLOGIA INFORMACION	SQL	Web	1
		Consultas PIDE: Consulta de RENIEC, SUNAT, SUNARP, etc.	OFICINA TECNOLOGIA INFORMACION	No aplica	Web	1
		Usuarios VUCE: Gestión de usuarios de comprobantes de VUCE	OFICINA TECNOLOGIA INFORMACION	SQL	Web	1
		Fiscalización Posterior Abastecimiento: Entre un porcentaje aleatorio del Listado de Órdenes de Compra y Servicio a Fiscalizar	UNIDAD ABASTECIMIENTO	SQL	Web	2
		PAS Videos: Publicación de videos para el proceso de Sanciones de Bizagi	DIRECCION SANCIONES	No aplica	Web	2
		Directorio Telefónico	UNIDAD RECURSOS HUMANOS	SQL	Web	2

		Seguimiento de actividades	UNIDAD RECURSOS HUMANOS	SQL	Web	1
N°	**Sistema / Aplicativo**	**Breve descripción**	**Área Usuaria**	**Motor de BD**	**Tipo**	**Prioridad**
5	SIGAWEB	Sistema Integrado de Gestión Administrativa - web	TODO SANIPES	SQL	Web	2
6	SIGESDOC (Sistema de Gestión Documental)	Sistema de Gestión Documental: Ingreso de Trámites regulares y TUPA 1	ATENCION AL CIUDADANO	SQL	Web	1
		Módulo de Habilitaciones: Consulta de Expedientes Antiguos, Emisión de Vigencia de Protocolos	SUB DIRECCION HABILITACIONES	SQL	Web	1
		Módulo de Tesorería: Generación de Comprobantes, Serie 01	TESORERIA	SQL	Web	1
7	SIGESDOC REPORT	Servicio de Reportes del SIGESDOC	ATENCION AL CIUDADANO	SQL	Web	1
8	SISP (Sistema Integrado de Sanidad Pesquera)	Módulo de Certificaciones: Seguimiento a Expedientes de Certificaciones que ingresan por VUCE y Mesa de Partes	DIRECCION HABILITACIONES Y CERTIFIC.	SQL	Web	1
9	Integrador	Servicio de Interoperabilidad VUCE – SANIPES: Recepción de Trámites TUPA 25, 30, 31, 34, 35, 35, 36, 37, 38, 39, 40	DIRECCION HABILITACIONES Y CERTIFIC.	SQL	Web	1
10	Trazamobi	Sistema de Trazabilidad de Moluscos Bivalvos: Solicitud del DER, Emisión del DER	DIRECCION FISCALIZACION SANITARIA	SQL	Web y Móvil	1
11	VUSA (Ventanilla Única del Sanipes)	Módulo de Registro de Trámites Regulares	ATENCION AL CIUDADANO	SQL	Web	2
		Módulo de Registro de Trámites de Habilitaciones	SUB DIRECCION HABILITACIONES	SQL	Web	2
12	Tesorería VUCE	Generación de Comprobantes enviados por la VUCE	TESORERIA	SQL	Web	1
13	Medidas Sanitarias	Registro de Medidas Sanitarias de Fiscalización	DIRECCION FISCALIZACION SANITARIA	SQL	Web	2
14	Bizagi	Módulo de Habilitaciones (Registro de todos los TUPAS de Habilitaciones)	SUB DIRECCION HABILITACIONES	SQL	Web	1
		Módulo de Certificaciones (TUPA 30)	SUB DIRECCION CERTIFICACIONES	SQL	Web	1

15	Aula Virtual	Plataforma E-Learning de Autoaprendizaje “Gestión Sanitaria en el Cultivo de Trucha Arcoíris”	DIRECCION SANIDAD E INOCUIDAD	SQL	Web	1
16	Reserva de Salas	Registro y Seguimiento a la Reserva de Salas del SANIPES	PRESIDENCIA	MySQL	Web	2

ANEXO 3

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de Equipo	Rol	Descripción	Prioridad
1	Servidor tipo cuchilla (Dell)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Convergente	2
2	Servidor tipo cuchilla (Dell)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Convergente	2
3	Servidor tipo cuchilla (DELL)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Convergente	2
4	Servidor rackeable (SuperMicro)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Hiperconvergente	2
5	Servidor rackeable (SuperMicro)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Hiperconvergente	2
6	Servidor rackeable (SuperMicro)	Virtualización de servidores	Host para virtualizar servidores que se usan para desarrollo y calidad de los sistemas. Sistema Hiperconvergente	2
7	Servidor rackeable (Lenovo)	Virtualización de servidores	Host para virtualizar servidores que se usan para producción de los sistemas. Sistema Hiperconvergente	1
8	Servidor rackeable (Lenovo)	Virtualización de servidores	Host para virtualizar servidores que se usan para producción de los sistemas. Sistema Hiperconvergente	1
9	Servidor rackeable (Lenovo)	Central telefónica	Servidor donde se encuentra implementado el software de telefonía y la conexión de la telefonía fija con los anexos de la entidad	1
10	Servidor rackeable (Dell)	Servidor de Backup	Se encuentra implementado el software de backup, para los backups de información (carpetas) y servidores	1
11	Servidor rackeable (Dell)	Virtualización de servidores	Host para virtualizar servidores en la DMZ	1
12	Librería Rackeable (IBM)	Backup a cintas	Se usar para trasladar el backup de la información hacia cintas tape backup	1
13	Storage (Dell)	Almacenamiento para servidores	Discos SAN, que se usan para la información de servidores virtuales (desarrollo y calidad), en la Solución de servidores tipo cuchilla (Dell)	2
14	Storage (Promise)	Almacenamiento para servidores	Discos SAN, que se usan para la información de servidores virtuales (desarrollo y calidad), en la Solución de servidores tipo cuchilla (Dell)	2
15	Storage (IBM)	Almacenamiento para servidores	Discos SAN, que se usan para la información de servidores virtuales (producción), en la Solución de servidores rackeable (Lenovo)	1

N°	Tipo de Equipo	Rol	Descripción	Prioridad
16	Switch SAN (Brocade)	Conexión a 8Gbps de servidores	Se usa para la comunicación de 8Gbps entre los servidores blade con los Storage	2
17	Switch SAN (IBM)	Conexión a 16Gbps de servidores	Se usa para la comunicación de 8Gbps entre los servidores de producción con el switch core	1
18	Switch Core (Arista)	Switch principal para la conexión e interconexión de redes	Equipos principales, que administra las redes de la entidad	1
19	Switch de distibución (Cisco)	Switch para servidores	Equipo usado para la conexión de los servidores con el switch Core	1
20	Firewal perimetral (Forinet)	Seguridad para la red externa	Equipo de seguridad, para todo lo que entra desde el internet, son 02 equipos que trabajan en HA. También permite la conexión cifrada (VPN)	2
21	Firewall de aplicaciones (Barracuda)	Seguridad para los sistemas de la entidad	Equipo de seguridad para las aplicaciones críticas de la entidad	1
22	UPS (Newave)	Equipo de energía ininterrumpida	Se usa para la autonomía de energía eléctrica de los equipos informáticos en el data center de la entidad	1
23	Aire acondicionado (Gforce)	Equipo de climatización	Se usa para climatizar el ambiente (data center) donde se encuentra los equipos informáticos	1

ANEXO 4

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

SANIPES	Evento: Terremoto /Sismo	FPC – 01

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina deenergía, que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por SANIPES, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- Oficinas y/o Centro de Datos Principal

Recursos Humanos

- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de SANIPES, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central donde se encuentra el Centro de Datos.

d) Personal Encargado

La Alta Dirección de SANIPES, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones de SANIPES, el mismo que debe ser de conocimiento de todo el personal.
- Realización de simulacros de evacuación con la participación de todo el personal.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC

- Evaluar el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración deinformación base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro

de Datos.

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de laentidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de laentidad.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos Relacionados antes del evento
- Tener la lista actualizada de los servidores por Direcciones y/u Oficinas.
- Mantenimiento del orden y limpieza de los ambientes de la sede central y Centro de Datos.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia informáticaEl/La Coordinador/a de Continuidad de TIC.

d) Personal Encargado
Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia
- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal de SANIPES que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento detrozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientesde trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personalde mantenimiento de SANIPES, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Coordinador/a de la UFTIC deberá coordinar con el/la Jefe/a de la OGA.

f) Duración
Los procesos de evacuación del personal de SANIPES deberán ser calmados y demorar 5 minutoscomo máximo.
La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y losdaños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI de SANIPES.

b) Descripción de actividades

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:

- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Realizar el encendido de las máquinas virtuales en el sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Comando de Continuidad Operativa.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
  - Confirmar los puntos de recuperación de datos de las aplicaciones.
  - Verificar que las funcionalidades de comunicación están funcionando correctamente.
  - Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
  - Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.
- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TIC, presentará un informe a la Alta Dirección, explicando qué parte de las actividades u operaciones de tecnologías dela información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica a la Alta Dirección

e) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TIC, luego del cual se determinará las acciones a tomar.

SANIPES	Evento: Delito Informático	FPC - 02
1. PLAN DE PREVENCIÓN		
a) Descripción del evento		

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por SANIPES, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Sistemas de información, aplicativos y portales de SANIPES

b) Objetivo
Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalarlas aplicaciones dañadas.

c) Entorno
Este evento puede darse en cualquiera de los servidores y estaciones ubicadas en la sede principal de SANIPES.

d) Personal Encargado
El Equipo de Prevención de TIC es el responsable del correcto funcionamiento de los servidores,estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

e) Condiciones de Prevención de Riesgo
- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadasen las estaciones de trabajo.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos enlos correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para sureemplazo provisional hasta su desinfección y habilitación.
- Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que nolo requieran.
- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al personal de OTI, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de lainformación procesada y almacenada en el Centro de Datos.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de laentidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases dedatos.
- Documentar y validar los manuales de restauración de los sistemas de información en producción.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos relacionados antes del evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estacionesde trabajo.

c) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC y el/la Oficial de Seguridad de la Información puedenactivar la contingencia.

g) Personal Encargado

Equipo de Emergencia de TIC.

d) Descripción de las actividades después de activar la contingencia
- Desconectar o retirar de la red de datos de SANIPES, el servidor o la estación infectada o vulnerada.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

e) Duración

La duración del evento no deberá ser mayor DOS HORAS en caso se confirme la presencia de un virus en estaciones de trabajo y de CUATRO HORAS en servidores de red. Esperar la indicacióndel personal de soporte técnico para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El equipo de restauración de TIC, luego de restaurar el correcto funcionamiento del servidor,estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o Director del área para reanudar las labores de trabajo con elequipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a él/la Coordinador/a de UFTIC de SANIPES el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, consus respectivas librerías y niveles de seguridad.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema deinformación.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible(Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red de SANIPES.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de informaciónafectado.
- Comunicar el restablecimiento del servicio

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivasdel caso enviando una alerta vía correo al personal de SANIPES.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentesde seguridad de la información.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gobierno Digital.

El personal Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso,presentará un informe a el/la Coordinador/a de UFTIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC de SANIPES, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red,en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

SANIPES	Evento: Falla de hardware y software	FPC – 03

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Storage

Software

- Aplicativos usados por SANIPES y de servicio al ciudadano

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de las imágenes de los servidores o máquinas virtuales en producción.

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a lasoperaciones de SANIPES.

d) Personal Encargado

Equipo de Prevención de TIC.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamientode los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de laentidad, así como de las imágenes de los servidores.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención,revisión del sistema y mantenimiento general.
- Disponer de servidores de bases de datos de contingencia, con la instalación del motor debase de datos.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de

información.

- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centrode Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de laentidad.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datospara su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internosde forma anual.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
   - Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
   - Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b) Procesos Relacionados antes del eventoDisponibilidad de las copias de respaldo.
   Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia
   El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
   - Realizar la revisión del servidor averiado, buscando un recurso de reemplazo
   - verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevoservidor virtual configurado de acuerdo a lo requerido.
   - Solicitar las cintas de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.

e) Duración
   El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
   El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores, y el/la Coordinador/a de Continuidad de TIC informará a los Directores y/o Jefes para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades
   El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores.

   Se debe realizar como mínimo las siguientes actividades:
   - Instalación y puesta a punto de un cómputo compatible y hardware necesarios para lainstalación del sistema de información con las características mínimas exigidas.
   - Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
   - Instalación y configuración del sistema de información y el motor de la base de datos, consus respectivas librerías y niveles de seguridad.
   - Proceder a la restauración de las copias de respaldo, de la información de los servidores

afectados.

- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios de SANIPES informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará el incidente en el Sistema de Gestión de Tickets utilizado por Soporte Técnico de la OTI, precisando las acciones realizadas.

El/La Especialista en Redes y Comunicaciones, presentará un informe a el/la Coordinador/a de OTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC, se desactivará el presente Plan.

e) Proceso de Actualización

En base al informe presentado por el/la Especialista en Redes y Comunicaciones, quien identifica las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el/la Especialista en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

SANIPES	Evento: Falla del suministroeléctrico en el Centro de Datos y gabinetes de comunicación.	FPC - 04

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos o sede principal de laentidad.

Este evento incluye los siguientes elementos mínimos identificados por SANIPES, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS
- Aire acondicionado

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Este evento puede darse en cualquiera de las instalaciones de SANIPES, considerando la Sede Central, que es la que contiene el Centro de Datos, los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

El/La Coordinador/a de la Unidad Funcional de Abastecimiento de la OGA y el/la Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones de SANIPES se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos considerados como críticos.
- Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 02 horas como mínimo.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 02 horas.
- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del Centro de Datos de SANIPES (puertas, contactos magnéticos, etc.)

- Verificación del cableado eléctrico de la sede Principal de SANIPES, una vez por año.
- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

f) Acciones del Equipo de Prevención de TIC
- Revisar periódicamente y de forma conjunta con el área de Servicios Generales las instalaciones eléctricas del Centro de Datos de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos de SANIPES.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

Corte de suministro de energía eléctrica en los ambientes de SANIPES.

b) Procesos Relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia

El/La Jefe/a de OGA y/o Coordinador de Continuidad de TIC pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- Informar a el/la Gerente General / Presidencia Ejecutiva del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas de SANIPES y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía en el Centro de Datos sea mayor a dos (02) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

e) Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energíaeléctrica.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de Restauración de TIC, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información.

Se debe realizar como mínimo las siguientes actividades:

- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguiente detalle:
  - Equipos de Comunicaciones (router, switches core, switches de acceso)
  - Equipos de almacenamiento (storage)
  - Servidores físicos por orden de prioridad
  - Servidores virtuales por orden de prioridad
- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

El/La Especialista en Redes y Comunicaciones presentará un informe a él/la Coordinador/a de la UFTIC, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Este informe deberá ser elevado a la Alta Dirección de SANIPES.

d) Desactivación del Plan de Contingencia

El/La Coordinador de Continuidad de TIC desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

ANEXO 5

FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA N° |

Escenario de Prueba: (Descripción del escenario a probar/certificar)

Área Responsable: (Área responsable del escenario de prueba a probar/certificar)

INFORMACION DEL PROCESO

Metodología: (Detallar lo que se va a hacer en la prueba)

Alcance: (Definir hasta donde va a abarcar)

Condiciones de Ejecución

Equipo: Nombre Servidor/PC de prueba **Aplicación/Software:**

Ubicación: Lugar de prueba **Fecha de Backup:** / /

RESULTADO DE LA PRUEBA

Resultado: **Satisfactorio:** **Satisfactorio con Observaciones:** **Deficiente:**

Observaciones: (En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados)

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: (Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

ACTUALIZACION PARTICIPANTES

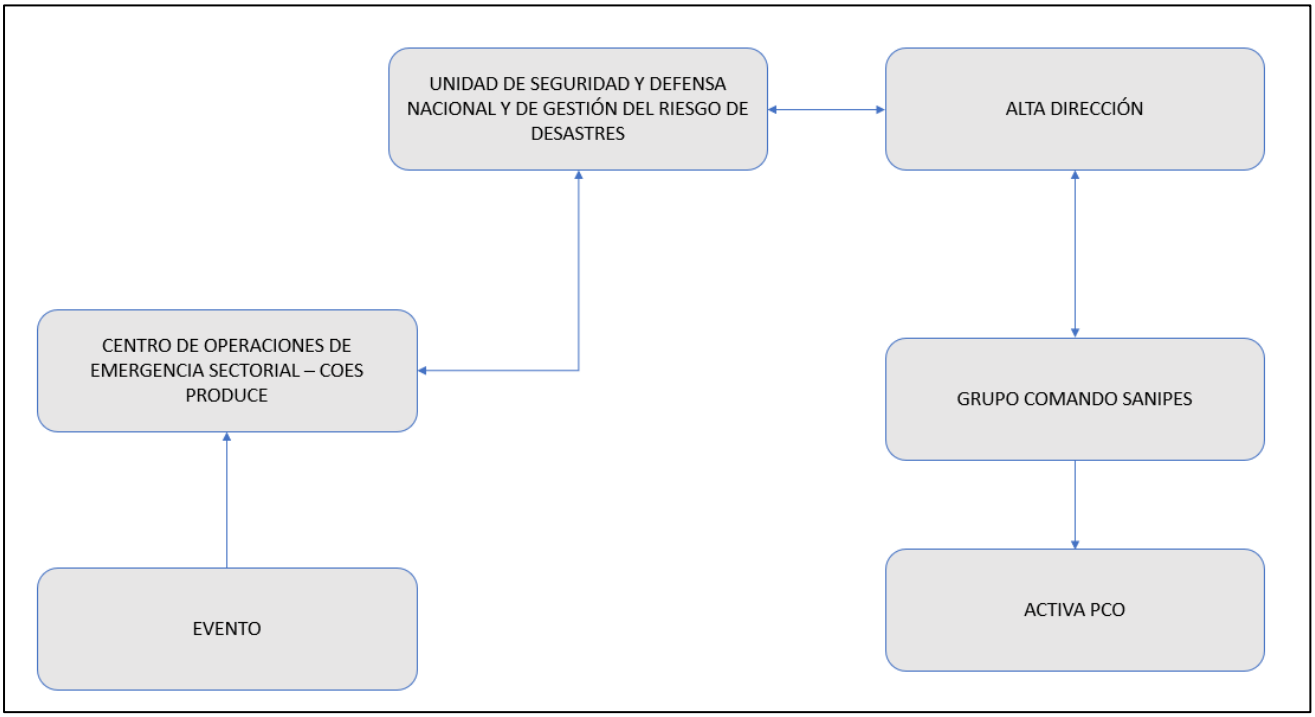
Participante	Cargo	Firma

ANEXO N°04: PROCEDIMIENTO PARA LA CONVOCATORIA DEL PERSONAL INVOLUCRADO EN LA EJECUCIÓN DE ACTIVIDADES CRÍTICAS

Ejecución de la convocatoria y actividades a desarrollar

1. Una vez producido el evento de gran magnitud, la alta dirección del SANIPES convoca de manera inmediata al Grupo Comando, reuniéndose en el local determinado como sede Alterna del SANIPES.
2. En caso de activar el PCO, el Presidente del Grupo Comando, coordina, en sesión de Grupo de Comando, con el representante de la Oficina de Administración la movilización del personal titular que realizará trabajo presencial en la Sede Alterna.
3. Para realizar las comunicaciones se crea el sistema que garantiza la interacción remota para responder a la activación del Plan de Continuidad Operativa, en ese sentido, las comunicaciones se ejecutarán mediante telefonía móvil, mensajería instantánea, mensajería por correo electrónico, mensajería de voz y datos. La Unidad de Recursos Humanos y la Unidad de Imagen institucional, se encargan de los comunicados oficiales a ser emitidos al personal o a los medios de comunicación de ser el caso. De esta manera, se tomaría concomimiento de forma oportuna de los peligros y emergencias, del alcance de daño, características e implicancias, promoviendo las disposiciones para su atención inmediata a través de las coordinaciones pertinentes para la movilización del recurso humano, la logística permitiendo dar continuidad a las operaciones de la institución.
4. Dar inicio a las actividades críticas, de apoyo y de recuperación determinadas por las unidades orgánicas del SANIPES.
5. Reportar las novedades de personal y material al inicio de las actividades críticas de las unidades orgánicas a la Alta Dirección, así como de las actividades de recuperación.
6. De acuerdo a las informaciones y reportes recibidos por parte de los integrantes del Grupo de Comando, determinar la desactivación de la Sede Alterna del SANIPES, de corresponder.

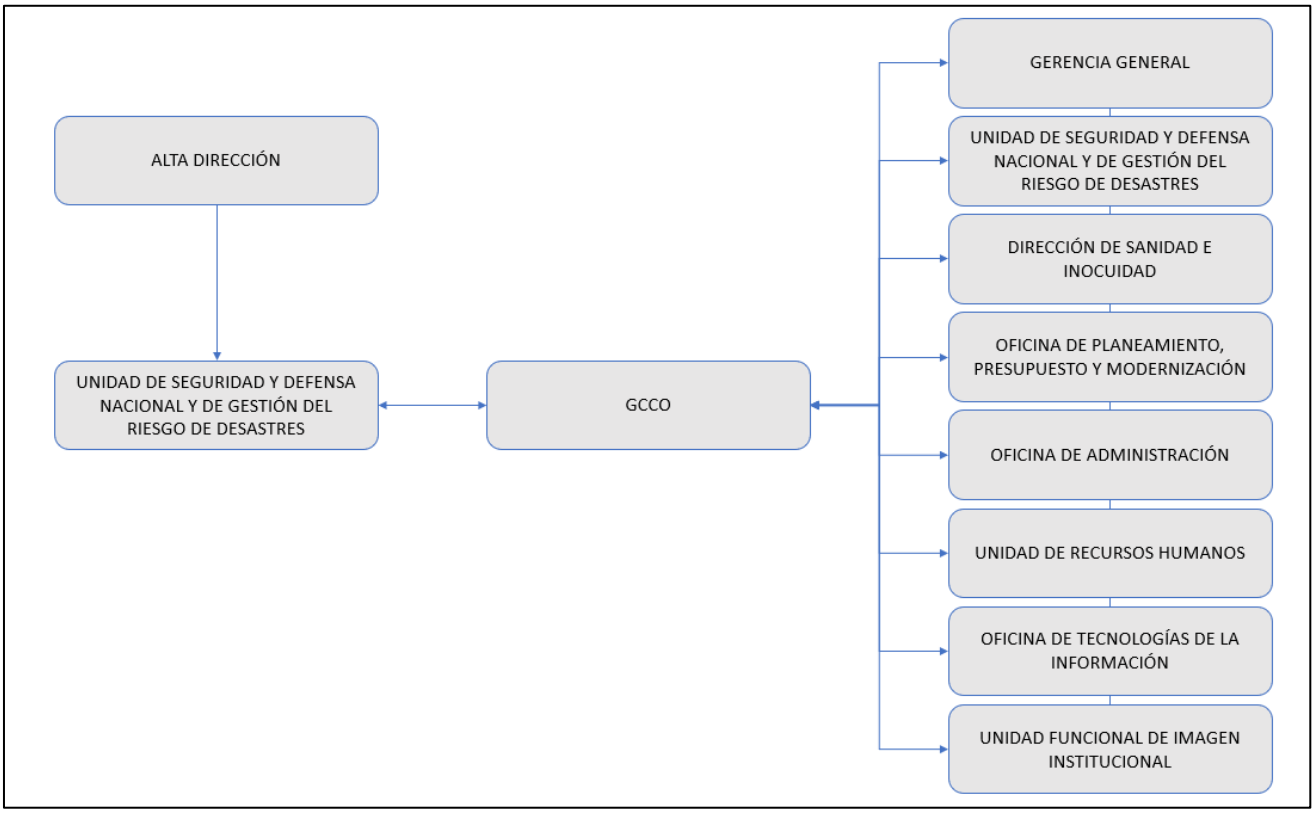
Figura N°07: Organización para Coordinación Externa



Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

Figura N°08: Coordinación Interna

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres



ANEXO N°05: DIRECTORIO DE GRUPO COMANDO

Tabla N°22: Directorio del Grupo Comando para la Gestión de la Continuidad Operativa del Organismo Nacional de Sanidad Pesquera – SANIPES

Integrantes	Unidad de organización	Nombres y apellidos	Cargo	Correo
Titular de la unidad orgánica responsable de la Gestión de la Continuidad Operativa del SANIPES	Gerencia General	Julio Américo Falconi Canepa	Gerente General	julio.falconi@sanipes.gob.pe
Representante de Gerencia General - Unidad Funcional de Seguridad y Defensa Nacional y Gestión del Riesgo de Desastres	Unidad Funcional de Seguridad y Defensa Nacional y Gestión del Riesgo de Desastres	Johnny Edgard Calderón Higginson	Especialista en Seguridad y Defensa Nacional y Gestión del Riesgo de Desastres	1565-grd-gg@sanipes.gob.pe
Representante de la Unidad de Planeamiento, y Modernización	Unidad de Planeamiento, y Modernización	Pierina Isabel Valdiviezo Flores	Especialista en Planeamiento Estratégico	pierina.valdiviezo@sanipes.gob.pe
Representante de la Dirección de Sanidad e Inocuidad	Dirección de Sanidad e Inocuidad	Muriel María Gomez Sanchez Orezzoli	Directora	muriel.gomez@sanipes.gob.pe
Representante de la Unidad de Recursos Humanos	Unidad de Recursos Humanos	Paola Nathali Soto Pejerrey	Especialista en Seguridad y Salud en el Trabajo	paola.soto@sanipes.gob.pe
Representante de la Oficina de Administración	Unidad de Abastecimiento	Juan Carlos Rojas Chávez	Encargado de Servicios Generales	carlos.rojas@sanipes.gob.pe
Representante de la Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Melitón Ricardo Otoya Verástegui	Jefe	meliton.otoya@sanipes.gob.pe
Representante de la Unidad Funcional de Imagen Institucional o la que haga sus veces	Unidad Funcional de Imagen Institucional	Alfredo Lizandro Loayza Leonardo	Analista en Comunicación Audiovisual	alfredo.loayza@sanipes.gob.pe

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

ANEXO N°06: ORGANIZACIÓN PARA EL DESARROLLO DE ACTIVIDADES CRÍTICAS

Tabla N°23: Organización de Actividades Críticas

Código	Actividad Crítica	Objetivo	Unidad Orgánica responsable	Dueño del Proceso	Tareas/Procedimientos
PM-01	Gestión de investigación en inocuidad y sanidad	Establecer los procedimientos correspondientes a la investigación en inocuidad y sanidad	Dirección de Sanidad e Inocuidad	Director de Sanidad e Inocuidad	PM-01.01 Formulación de proyectos de investigación PM-01.02 Ejecución de proyectos de investigación y difusión de resultados PM-01.03 Gestión de la inocuidad pesquera y acuícola PM-01.04 Gestión de la sanidad de los recursos hidrobiológicos PM-01.05 Emisión de Opinión Técnica en materia de sanidad e/o inocuidad
PM-03	Gestión de fiscalización	Verificar el cumplimento de las obligaciones, prohibiciones o limitaciones exigibles a los operadores de las actividades pesqueras y acuícolas en el ámbito nacional establecidas en la normativa sanitaria y en base al plan anual de controles oficiales y fiscalizaciones sanitarias a nivel nacional, asimismo ejecutar las actividades para la atención de las solicitudes de fiscalización no programadas; además de autorizar y fiscalizar a las entidades de inspección y/o ensayo que brindan servicios complementarios y vinculados con el sector pesca y acuicultura, a los operadores y comercializadores.	Dirección de Fiscalización Sanitaria	Director de Fiscalización Sanitaria	PM-03.01 Ejecución de fiscalización regular PM-03.02 Ejecución de fiscalización especial PM-03.03 Gestión de fiscalización a las entidades de inspección y/o ensayo
PM-04	Gestión de habilitaciones, registros y certificaciones sanitarias	Realizar la gestión correspondiente para la emisión documentos de habilitaciones, autorizaciones, registros sanitarios y certificados sanitarios.	Dirección de Habilitaciones y Certificaciones	Director de Habilitaciones y Certificaciones	PM-04.01. Gestión de habilitaciones y registros PM-04.02. Gestión de certificaciones

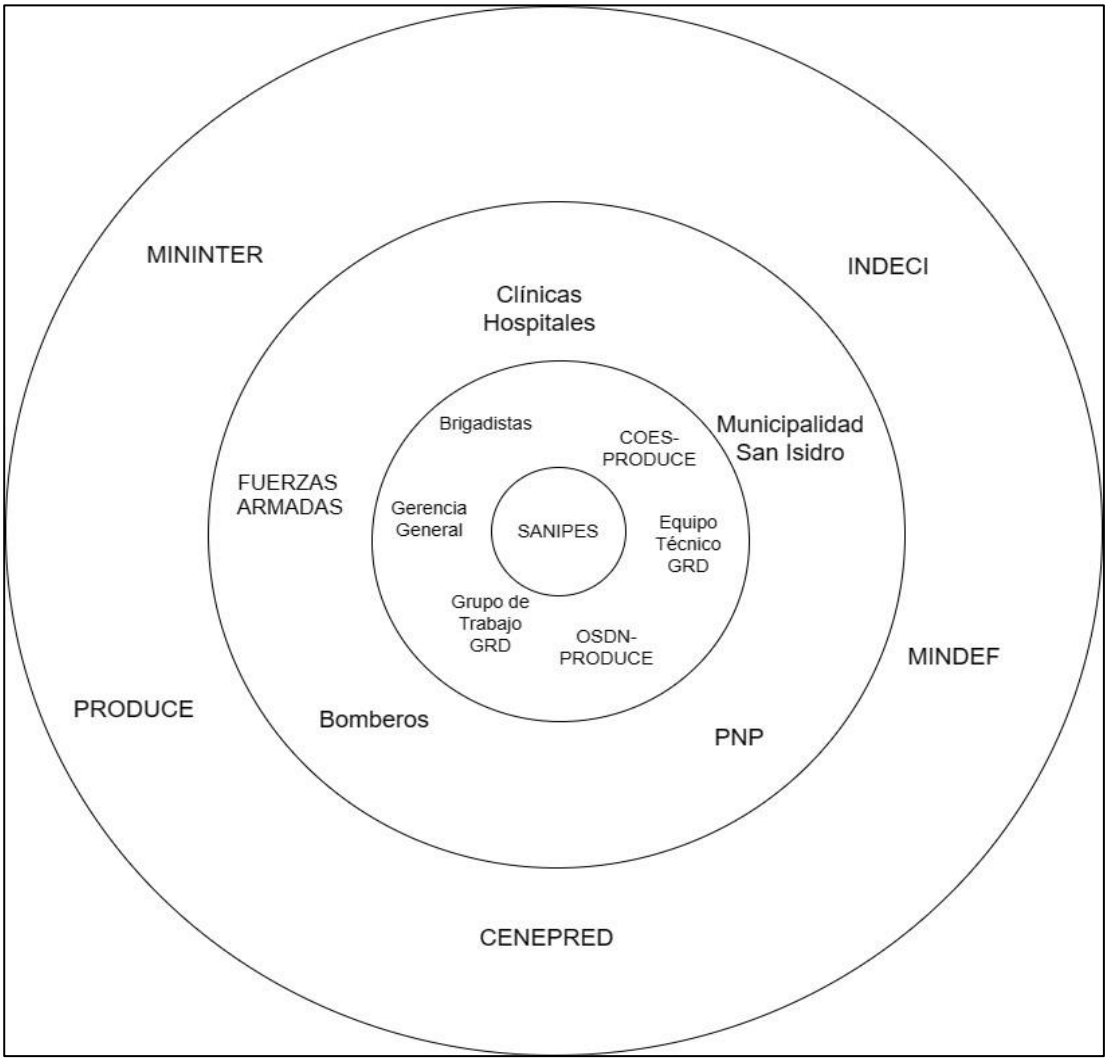
Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

ANEXO N°07: SISTEMA DE COMUNICACIONES DE EMERGENCIA

El Sistema de Comunicación de Emergencia se activa ante la ocurrencia de eventos de gran magnitud: sismos, incendios, inundaciones, ataques informáticos, entre otros que ponen en riesgo la integridad de los servidores, así como la infraestructura SANIPES.

En ese sentido, se busca mantener la comunicación entre el Grupo Comando y personal clave y de apoyo a fin de determinar el nivel de afectación en el SANIPES a fin de activar el Plan de Continuidad Operativa. A continuación, se muestra el mapa de actores de SANIPES en caso de un desastre y/o emergencia:

Figura N°09: Mapa de Actores SANIPES



Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres

Medios de Comunicación:

- Canales de comunicación
- Radios Tetra
- Telefonía celular (mensajes de texto)
- Correos electrónicos
- Aplicativos de mensajería instantánea
- Medios de comunicación social (radio, redes sociales, televisión)

ANEXO N°08: CRONOGRAMA DE IMPLEMENTACIÓN DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA

Tabla N°24: Cronograma de Implementación de la Gestión de Continuidad Operativa

Actividades	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre
Fortalecimiento de capacidades de los servidores y funcionarios del Grupo de Comando en la Gestión de la Continuidad Operativa.	X						X				X	
Realizar el seguimiento a las acciones de implementación.				X								X

Fuente: Elaborado por la Unidad Funcional de Seguridad y Defensa Nacional y de Gestión del Riesgo de Desastres