PROGRAMA NACIONAL "A COMER PESCADO"

PLAN DE CONTINUIDAD OPERATIVA

2025 – 2027

CONTENIDO

I INFORMACIÓN GENERAL

El Programa Nacional "A Comer Pescado" (en lo sucesivo, PNACP) es un programa adscrito al Ministerio de la Producción, creado mediante Decreto Supremo N° 007-2012-PRODUCE, con una vigencia de cinco (05) años, la misma que fue ampliada mediante Decreto Supremo N° 016-2017-PRODUCE y Decreto Supremo N° 018-2022-PRODUCE, encontrándose vigente hasta el 31 de diciembre de 2027.

El PNACP depende del Despacho Viceministerial de Pesca y Acuicultura del Ministerio de la Producción y es financiado con el Presupuesto Institucional del Pliego 038: Ministerio de la Producción. La ejecución de los recursos asignados al PNACP se realiza a través de la Unidad Ejecutora 003: Fomento al Consumo Humano Directo - A Comer Pescado.

Mediante Resolución Ministerial N° 292-2020-PRODUCE, se aprueba el Manual de Operaciones del PNACP, modificado mediante Resolución Ministerial N° 127-2025-PRODUCE, en cuyo contenido se establece:

"**Artículo 1.- Objetivo General**

El Programa Nacional "A Comer Pescado", en adelante el PNACP, tiene como objetivo general fomentar, consolidar y expandir los mercados internos para el consumo final de productos derivados de los recursos hidrobiológicos de los ámbitos marítimo y continental del país.

Artículo 2.- Objetivos específicos

Los objetivos específicos del PNACP son los siguientes:

- **i.** Contribuir al desarrollo de hábitos de consumo de la población que coadyuven a la inclusión permanente de una mayor proporción de recursos derivados de la actividad pesquera nacional en la canasta familiar, fomentando la disponibilidad y acceso a los productos y brindando información, como herramienta de promoción, sobre los excelentes atributos alimenticios de los mismos.
- **ii.** Fomentar la mejora económica de las actividades de la pesca artesanal y la acuicultura de menor escala, articulando dichas actividades con el impulso a la demanda, y fomentando la iniciativa para la asociatividad privada buscando el desarrollo de nuevas variedades de productos de alta calidad.
- **iii.** Fomentar la apertura de líneas de negocio, incluyendo la consolidación de cadenas de distribución, en el sector pesquero nacional general, con orientación al consumo humano directo, con la finalidad de asegurar la disponibilidad en tiempo y forma de los productos con potencial éxito comercial en los mercados de consumo final."

Asimismo, el PNACP tiene por finalidad contribuir al incremento del consumo de productos hidrobiológicos en todo el país, con especial énfasis en las zonas de menor consumo articulando la demanda con la oferta de productos para el consumo humano directo.

La sede central del PNACP; se encuentra ubicada en la Calle Antequera 671 Urb. Jardín - San Isidro – Lima – Perú; en local alquilado, con un área de 300 m2, un perímetro de 152.75 metros, 02 niveles y 1 azotea. La edificación tiene una antigüedad de 50 a 55 años, donde funciona la Coordinación Ejecutiva y todas las unidades orgánicas.

El PNACP cuenta con las siguientes Unidades:

Unidad de Dirección

- Coordinación Ejecutiva

Unidades de Asesoramiento

- Unidad de Asesoría Legal
- Unidad de Planeamiento, Presupuesto y Modernización

Unidades de Apoyo

- Unidad de Administración y Finanzas
- Sub Unidad de Recursos Humanos
- Sub Unidad de Abastecimiento
- Sub Unidad de Contabilidad
- Sub Unidad de Tesorería
- Sub Unidad de Servicios Generales

Unidades de Línea

- Unidad de Sensibilización
- Unidad de Promoción
- Unidad de Articulación
- Unidad de Gestión Regional

Respecto de la unidad vehicular asignada al PNACP, se cuenta para uso institucional, con una cochera ubicada en Calle Elías Aguirre 214, Bellavista Callao.

Para el Archivo Central del PNACP se cuenta con un depósito ubicado en Av. Paseo de la República 3591, San Isidro – Lima, que garantiza el servicio y acceso controlado a los documentos archivísticos bajo su custodia.

En suma, para la operatividad del PNACP, ésta cuenta, a nivel de todas las regiones del país, con veintiséis (26) depósitos, los mismos que facilitan el resguardo de los materiales para las actividades de plataformas comerciales (Mi Pescadería, Conservas Peruanas en tu Mesa y Pesca con Valor), materiales para asistencia técnica y articulación comercial para la promoción de la implementación de sistemas de almacenamiento de productos hidrobiológicos provenientes de la pesca y acuicultura, materiales para actividades de sensibilización para el fomento del consumo de productos hidrobiológicos; que comprenden el desarrollo de las funciones de las cuatro (04) Unidades de Línea, con la finalidad de dar cumplimiento a nuestros objetivos institucionales a nivel nacional.

A Continuación, en el cuadro 01; se detalla el Listado de Locales del PNACP a nivel nacional:

Cuadro N° 01: Listado de Locales del PNACP a nivel Nacional

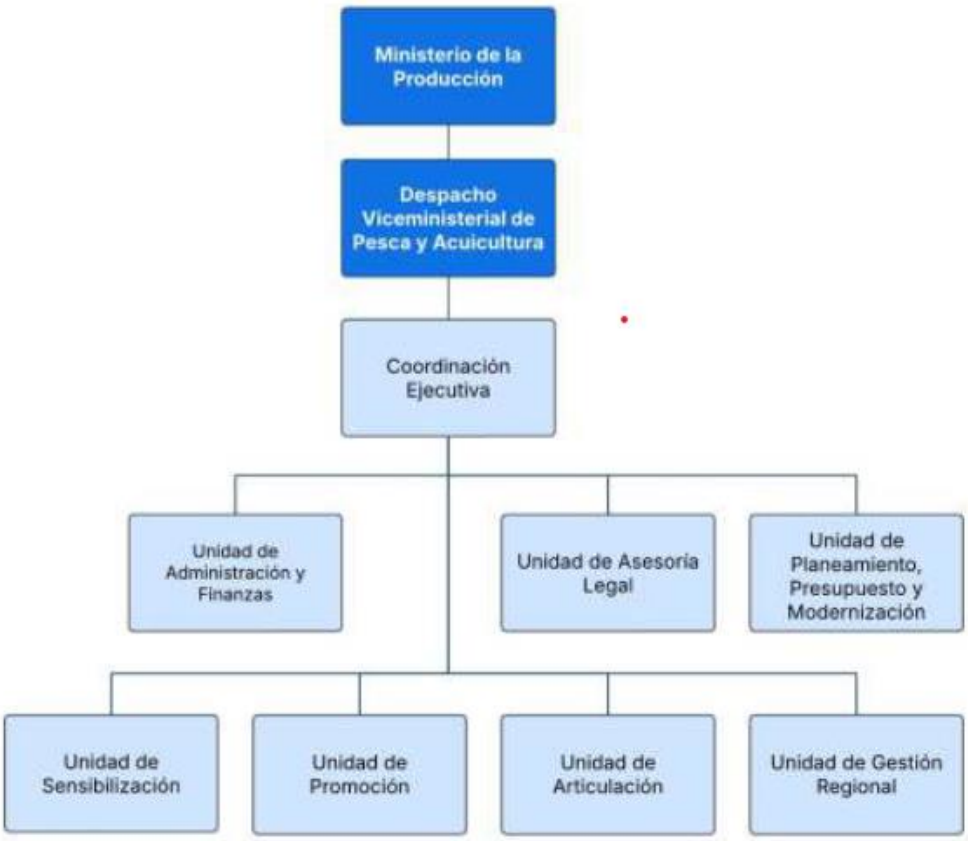
N°	USO	REGIÓN	DIRECCION
1	SEDE CENTRAL SAN ISIDRO	LIMA	Calle Antequera 671 Urb. Jardín, San Isidro, Lima, Lima
2	COCHERA	CALLAO	Calle Elías Aguirre 214 Bellavista Callao
3	DEPÓSITO	LIMA METROPOLITANA	Av. Paseo de la República 3591 San Isidro - Lima
4	DEPÓSITO	LIMA	Av. Francisca Vidal N°701 C 1er Piso Distrito de Huacho, Provincia de Huaura Dpto. Lima
5	DEPÓSITO	HUANCAVELICA	Malecón Santa Rosa N°160 - Provincia y departamento de Huancavelica
6	DEPÓSITO	APURIMAC	Av. Pachacútec N°200-202 pasaje S/N Mz. A Lt. 8 1er nivel Asociación 7 de agosto - Abancay
7	DEPÓSITO	ICA	Mza D-13 A2 Urb. Santa Elena - Ica.
8	DEPÓSITO	MADRE DE DIOS	Jr. Sinchi Roca - Lote 11 S/N Tambopata - Madre de Dios
9	DEPÓSITO	AREQUIPA	Av. Independencia N°2053 distrito del Cercado de Arequipa, Arequipa
10	DEPÓSITO	PASCO	Jr. Manuel Ubalde N°406 - Urb. San Juan Cerro de Pasco
11	DEPÓSITO	MOQUEGUA	Villa Moquegua Mz. 05, Lote 11 Distrito de San Antonio Provincia Mariscal
12	DEPÓSITO	TUMBES	Jr. Huáscar N°110-Tumbes
13	DEPÓSITO	CAJAMARCA	Jr. Tarapacá N°414 Distrito, provincia y departamento de Cajamarca
14	DEPÓSITO	AMAZONAS	Jr. Hermosura N°708 Distrito y provincia de Chachapoyas - Amazonas
15	DEPÓSITO	TACNA	Asociación de Vivienda Cabo Teodoro R. Pisco Mz H lote 14, 1er Piso - Tacna
16	DEPÓSITO	UCAYALI	Jr. Raymondi N°250 C - Ucayali
17	DEPÓSITO	AYACUCHO	Jr. Los laureles N°202 - Ayacucho
18	DEPÓSITO	LA LIBERTAD	Calle Borgoño N°195 Int. 101 Barrio Molino - Trujillo
19	DEPÓSITO	CUSCO	Urb. Kennedy "A" A-28 - Cusco
20	DEPÓSITO	JUNÍN	Jr. Lomas N°116 Distrito provincia de Huancayo Departamento de Junín
21	DEPÓSITO	HUÁNUCO	Av. Universitaria n° 246 Mz 03 - Lote 01 Urb. T.R.M Pilcomarca - Huanuco
22	DEPÓSITO	PIURA	AA. HH. Lo ficus Mz H2 Lote 4 - 2da Etapa
23	DEPÓSITO	PUNO	Ilave N° 760 Distrito de Puno Prov. de Puno y Distrito de Puno
24	DEPÓSITO	SAN MARTÍN	Jirón Jorge Chávez número 726-728 de la Ciudad de Tarapoto, provincia de San Martín, departamento de San Martín
25	DEPÓSITO	ANCASH	Av. Centenario s/n, Barrio Monterrey, distrito de Independencia, provincia de Huaraz y departamento de Ancash
26	DEPÓSITO	LORETO	Calle Pablo Rosell N°759 AAHH Daniel Alcides Carrión Mz. D Lote17 segunda etapa
27	DEPÓSITO	LAMBAYEQUE	Calle Alfonso Ugarte N° 546, distrito y provincia de Chiclayo
28	DEPÓSITO	LIMA	Calle Antequera 606 Ofic. 201 Segundo Piso Urb. Jardín, San Isidro, Lima, Lima

Las funciones asignadas al PNACP se encuentran establecidas en el Manual de Operaciones del Programa, aprobado con la Resolución Ministerial N° 00292-2020-PRODUCE, modificado por la Resolución Ministerial N° 000127-2025-PRODUCE, el cual contiene la estructura funcional, las funciones de cada unidad, el inventario de procesos y el organigrama del PNACP; en concordancia con la normativa vigente y los lineamientos de política en materia de Pesca y Acuicultura aprobados por el Ministerio de la Producción.

ORGANIGRAMA INSTITUCIONAL

El PNACP cuenta con la siguiente estructura:

Gráfico N°01: Organigrama del PNACP



Fuente: Resolución Ministerial N° 292-2020-PRODUCE y modificada mediante Resolución Ministerial N°127-2025-PRODUCE

El Plan de Continuidad Operativa (PCO) es concebido en el marco y conformidad de los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno", aprobado mediante Resolución Ministerial N°320-2021-PCM, cuya finalidad es fortalecer la implementación de la gestión de la continuidad operativa en las entidades públicas de los tres niveles de gobierno, ante la ocurrencia de desastres o cualquier evento que interrumpa prolongadamente sus operaciones.

Al respecto, la implementación de la continuidad operativa requiere de un alto grado de participación y compromiso del personal y del órgano de dirección, que permita lograr un resultado eficiente y eficaz en la capacidad de respuesta del PNACP, previniendo anticipadamente y disminuyendo el factor sorpresa de las emergencias.

En este contexto, mediante Resolución de Coordinación Ejecutiva Nº00001-2025-PNACP del 03 de enero del 2025, se aprobó la conformación del Grupo de Comando del Programa Nacional "A

Comer Pescado", encargado de la elaboración del Plan de Continuidad Operativa de la entidad y de la toma de decisiones respecto a la implementación de dicho plan; además de cumplir con las funciones establecidas en el sub numeral 6.1.3 de 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", aprobados con Resolución Ministerial N° 320-2021-PCM.

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. Es 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) **Personal Crítico:** Es la relación del personal prioritario mínimo indispensable, para asegurar la continuidad operativa de la entidad.

f) **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.

g) **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.

h) **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.

Siglas y acrónimos:

CE	:	Coordinación Ejecutiva
COE	:	Centro de Operaciones de Emergencia
GCO	:	Gestión de Continuidad Operativa
GCCO	:	Grupo de Comando de Continuidad Operativa
GRD	:	Gestión del Riesgo de Desastres
CSST	:	Comité de Seguridad y Salud en el Trabajo
GTGRD	:	Grupo de Trabajo para la Gestión del Riesgo de Desastres
INDECI	:	Instituto Nacional de Defensa Civil
OCIIN	:	Oficina de Comunicaciones e Imagen Institucional
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
SINAGERD	:	Sistema Nacional de Gestión del Riesgo de Desastres
SUB-UABAS	:	Sub Unidad de Abastecimiento
SUB-URH	:	Sub Unidad de Recursos Humanos
SUB-UC	:	Sub Unidad de Contabilidad
SUB-UT	:	Sub Unidad de Tesorería
SUB-USSGG	:	Sub Unidad de Servicios Generales
OSDN	:	Oficina de Seguridad y Defensa Nacional
UAF	:	Unidad de Administración y Finanzas
UA	:	Unidad de Articulación
US	:	Unidad de Sensibilización
UP	:	Unidad de Promoción
UGR	:	Unidad de Gestión Regional
UPPM	:	Unidad de Planeamiento, Presupuesto y Modernización
UAL	:	Unidad de Asesoría Legal
TI	:	Tecnologías de la Información

II BASE LEGAL

2.1. Decreto Legislativo N° 1587 que modifica la Ley N°29664, Ley del Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD

2.2. Decreto Supremo N°060-2024-PCM, Decreto que modifica el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) aprobado por Decreto Supremo N° 048-2011-PCM.

2.3. Decreto Supremo N° 007-2012-PRODUCE, que crea el PNACP, cuya vigencia fue ampliada mediante los Decretos Supremos Nos. 016-2017-PRODUCE y 018-2022-PRODUCE.

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

2.5. Decreto Supremo N°038-2021-PCM, Política Nacional de Gestión del Riesgo de Desastres al 2050.

2.6. Decreto Supremo N° 002-2017-PRODUCE, Reglamento de Organización y Funciones del Ministerio de la Producción.

2.7. Resolución Ministerial N° 320-2021-PCM, Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno.

2.8. Resolución Ministerial N°292-2020-PRODUCE, que aprueba el Manual de Operaciones del PNACP, modificado mediante Resolución Ministerial N°127-2025-PRODUCE.

2.9. Resolución Ministerial N° 028-2015-PCM, que aprueba los lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.

2.10. Resolución Secretarial N°039-2020-PRODUCE, que aprueba el Manual de Procedimientos del PNACP.

2.11. Resolución de Coordinación Ejecutiva Nº00001-2025-PNACP, que aprueba la conformación del Grupo de Comando del Programa Nacional “A Comer Pescado” y designa al Jefe del Unidad de Planeamiento, Presupuesto y Modernización como Presidente de la Gestión de la Continuidad Operativa del PNACP.

III OBJETIVOS

3.1 OBJETIVO GENERAL

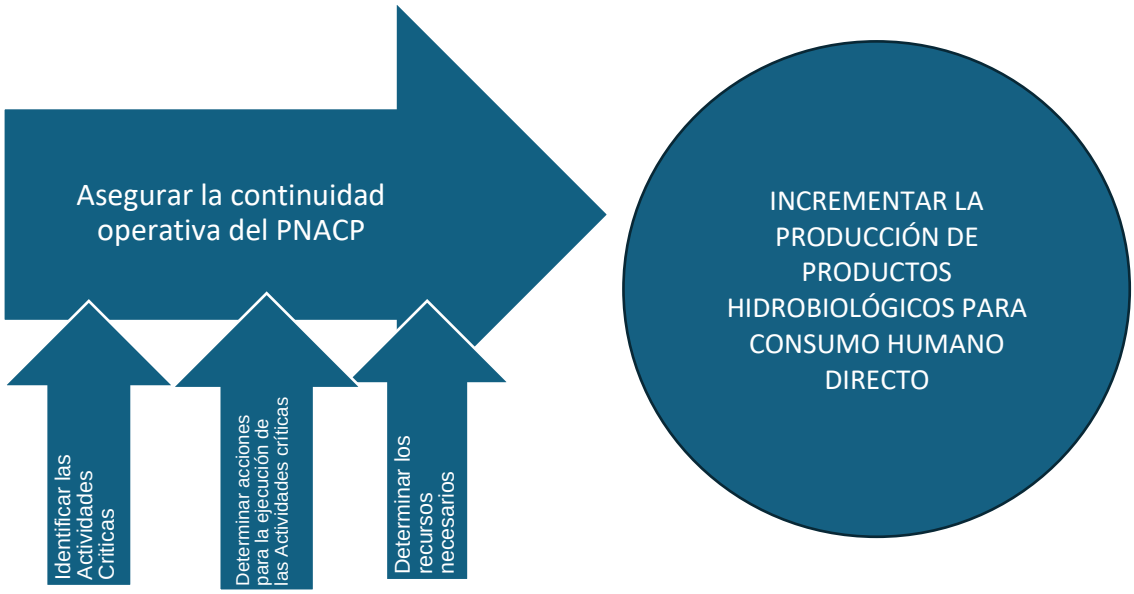
Fortalecer la capacidad de respuesta del PNACP ante eventos adversos o desastres, y asegurar la continuidad de las operaciones de la entidad mediante la ejecución de las actividades críticas identificadas, ante eventos que afecten significativamente u ocasionen la paralización prolongada de las operaciones de la entidad, garantizando que el PNACP ejecute las actividades críticas asociadas al cumplimiento de sus objetivos institucionales.

3.2 OBJETIVOS ESPECÍFICOS

Los objetivos específicos para la implementación del presente plan son los siguientes:

1. Identificar las actividades críticas del PNACP.
2. Determinar los recursos necesarios (humanos, materiales, equipos, financieros, informáticos), para ejecutar las actividades críticas.
3. Ejecutar las acciones y procedimientos necesarios para implementar la Gestión de la Continuidad Operativa del PNACP y la ejecución de las actividades críticas.

Gráfico N° 02: Acciones en el Marco del Objetivo del PNACP



Fuente: Resolución Ministerial N°292-2020-PRODUCE

IV IDENTIFICACIÓN DE RIESGOS Y RECURSOS

El Riesgo (R) es una función del Peligro (P) y la Vulnerabilidad (V), y se expresa como la probabilidad de que ocurra una pérdida en un determinado elemento, como resultado de la ocurrencia de un peligro[1].

Asimismo, se define el peligro como la probabilidad de que un fenómeno, potencialmente dañino, se presente en un lugar específico, con una cierta intensidad y en un período de tiempo y frecuencia definidos[2]. El peligro, según su origen, puede ser de dos clases: los generados por fenómenos de origen natural, y los inducidos por la acción humana.

Al identificar un riesgo, se determina los posibles eventos que con su materialización puedan impactar sobre los objetivos, estrategias, planes, proyectos y servicios; que, como misión, tiene el PNACP.

En ese sentido, basados en la información técnico-científica de un evento disruptivo en Lima Metropolitana, la provincia Constitucional del Callao y Regiones, el PNACP pone especial atención y concentra sus principales actividades y gestión institucional en dicho ámbito geográfico.

Por lo indicado en los párrafos anteriores, se siguieron los pasos para la 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".

4.1 MATRIZ DE RIESGOS

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".

La Matriz de Riesgos se realiza tomando en cuenta la intersección del peligro y la vulnerabilidad, tal como indica el cuadro siguiente:

[1] Anexo 2 de "Los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las entidades públicas de los tres niveles de gobierno", aprobado por Resolución Ministerial N° 320-2021-PCM del 30.12.2021

[2] Manual para la Evaluación de Riesgos originados por Fenómenos Naturales Versión 2.0 CENEPRED.

Cuadro N° 02: Matriz de Evaluación de Riesgos

PELIGRO MUY ALTO	Riesgo alto	Riesgo alto	Riesgo muy alto	Riesgo muy alto
PELIGRO ALTO	Riego medio	Riesgo alto	Riesgo alto	Riesgo muy alto
PELIGRO MEDIO	Riego medio	Riego medio	Riesgo alto	Riesgo alto
PELIGRO BAJO	Riesgo bajo	Riego medio	Riego medio	Riego medio
P V	VULNERABILIDAD BAJA	VULNERABILIDAD MEDIA	VULNERABILIDAD ALTA	VULNERABILIDAD MUY ALTA

Nota: (P) Peligro y (V) Vulnerabilidad.
Fuente: Resolución Ministerial N°320-2021-PCM

4.1.1 DESCRIPCIÓN DE PRINCIPALES PELIGROS IDENTIFICADOS:

Se han considerado los eventos adversos que pudieran generar amenazas e interrupción de los servicios, afectar la infraestructura, recursos y vida humana, y que tengan alta probabilidad de ocurrir en las localidades donde se encuentran ubicados la Sede Central del PNACP, la cochera, y los veintiséis (26) depósitos a nivel nacional, que incluye el depósito de Archivo Central.

A continuación, en el cuadro N° 03 se presenta la relación entre el tipo de amenaza que afectaría la operatividad del PNACP y su relación con los objetivos específicos.

Cuadro N° 03: Tipos de Amenazas que afectarían al PNACP

AMENAZAS	CLASIFICACION	OBJETIVOS RELACIONADOS	DESCRIPCION
SISMO DE GRAN MAGNITUD	NATURAL	Este tipo de evento compromete los OBJ: 1 ,2 Y 3	Liberación de energía interna de la tierra mediante la ruptura de las capas de corteza y que se manifiesta como movimientos ondulatorios que pueden llegar a alcanzar magnitudes variadas
INCENDIO	INDUCIDOS POR ACCION HUMANA	Este tipo de evento compromete los OBJ: 2 Y 3	Un incendio puede afectar la resistencia de las estructuras y la exposición directa al fuego de los colaboradores, pudiendo causar graves problemas por inhalación, intoxicación y sofocación por gases tóxicos
HELADAS Y FRIAJE	NATURAL	Este tipo de evento compromete los OBJ: 1 ,2 Y 3	Lluvias intensas sobrepasan el nivel del caudal del cauce de un río, el volumen máximo de agua del río es superado que tiende a desbordarse
MOVIMIENTOS EN MASA	NATURAL	Este tipo de evento compromete los OBJ: 1,2 Y 3	Movilización lenta o rápida de masa (huaycos), 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
EPIDEMIA O PANDEMIA	INDUCIDOS POR ACCION HUMANA	Este tipo de evento compromete los OBJ: 1 ,2 Y 3	La experiencia vivida en el Perú como la epidemia del cólera, la pandemia de la gripe A (H1N1); el Dengue, así como la Fiebre de Chikungunya y Zika, y sobre todo la pandemia por COVID-19 entre otras. Indica que hay un potencial epidémico ya existente de una alta probabilidad de brotes de Virus, que originarían una alta amenaza
HELADAS Y FRIAJE	NATURAL	Este tipo de evento compromete el OBJ: 3	Mediante la georreferenciación de las infraestructuras estas pueden verse afectadas por los escenarios en cuanto el descenso de temperatura en distintas regiones HELADAS (Sierra) FRIAJE (Selva)
ALTERACIONES EN EL ORDEN PUBLICO	INDUCIDOS POR ACCION HUMANA	Este tipo de evento compromete los OBJ: 1 ,2 Y 3	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

Elaboración: Grupo de Comando del PNACP

4.1.1.1 Sismo de gran magnitud

Los sismos son fenómenos que representan la liberación de energía interna de la tierra mediante la ruptura de las capas de corteza y que se manifiesta como movimientos ondulatorios que pueden llegar a alcanzar magnitudes variadas. A todos estos movimientos, el clasificador de peligros de la Evaluación de Daños, lo denomina SISMOS.

El Perú está ubicado al borde del encuentro de dos placas tectónicas: la placa sudamericana que choca y se monta sobre la placa de Nazca, (subducción), lo cual causa la mayor parte de los macrosismos en la costa occidental de América.

Lima es la zona del país donde se ha acumulado la mayor cantidad de energía sísmica, esto se sustenta en la investigación científica, la misma que ha puesto en evidencia tres áreas con importante acumulación de energía sísmica, las cuales se ubican frente a las costas. La más importante de estas zonas, en términos de tamaño y magnitud estimada, se ubica frente a la costa central del Perú (Lima, Ancash e Ica).

De acuerdo con el Instituto Geofísico del Perú, en el caso de Lima se pronostica un movimiento telúrico de magnitud 8.8 Mw. Un sismo de esta magnitud dejaría inmerso en un caos al departamento de Lima y la provincia constitucional del Callao.

Ante este escenario, las sedes institucionales en Lima y Callao pueden presentar daños severos que comprometerían la estabilidad de sus estructuras, ya que la edificación podría quedar debilitada y colapsar, quedando rezagada o interrumpida la prestación de servicios que brinda la entidad.

Dicho esto, el Perú está definido como escenario principal de afectación ante 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 PNACP que, por presentar la edificación una antigüedad de 50 a 55 años, podría verse seriamente afectada con complicaciones visibles y otras de análisis necesario que pudiesen llevar a determinar su inhabitabilidad para continuar con las operaciones propias de la entidad[3].

4.1.1.2 Incendio Urbano

El acontecimiento de un incendio puede afectar la resistencia de las estructuras y la exposición directa al fuego de los colaboradores, pudiendo causar graves problemas por inhalación, intoxicación y sofocación por gases tóxicos que se produce al momento del desastre.

Existe una probabilidad de ocurrencia de un incendio en los locales institucionales durante horas laborables, debido al aumento de los espacios dedicados a las Unidades Administrativas y Técnicas del PNACP, la instalación de equipos eléctricos, electrónicos y la alta concentración de material inflamable en algunos puntos dentro de la sede central y depósitos regionales.

Si bien los dispositivos contra incendios (detectores de humo y temperatura, extintores portátiles y rociadores automáticos de agua) ayudan en detectar y extinguir el fuego de fuentes eléctricas, químicas, orgánicas o de otras fuentes; éstos pueden que no sean suficientes, lo que limitaría la capacidad de respuesta.

Estar preparados para combatir un incendio, se vuelve un tema importante, sobre todo, con el objetivo de garantizar la seguridad de las personas y, en un segundo plano, resguardar la inversión en equipos, con el fin de reducir los tiempos requeridos para reiniciar las actividades. Un incendio puede suceder fuera del horario de trabajo o en días no laborables, teniendo graves consecuencias como la inhabilitación del ambiente físico, el colapso de los sistemas de comunicación y gestión de la información institucional, lo que requeriría la activación del Plan de Continuidad Operativa, con la diferencia que en este caso la afectación es solo en la infraestructura de la sede institucional.

Asimismo, un incendio originado en alguno de los depósitos del PNACP comprometería las acciones programadas en esa región y eliminaría el material resguardado para las actividades de plataformas comerciales (Pesca con Valor, Mi Pescadería y Conservas Peruanas en tu Mesa); materiales para asistencia técnica y articulación comercial para la promoción de la implementación de sistemas de almacenamiento de productos hidrobiológicos provenientes de la pesca y acuicultura; materiales para actividades de sensibilización para el fomento del consumo de productos hidrobiológicos; así como para los eventos protocolares del PNACP.

4.1.1.3 Lluvias Intensas e Inundación

[3] En cuanto al análisis en relación con la Identificación y Elaboración de Escenarios de Riesgo de Infraestructuras del Sector Producción frente a un sismo de gran magnitud, La Oficina de Seguridad y Defensa Nacional del Ministerio de la Producción remite el INFORME Nº 000000102-2024-PRODUCE/OSDN-dcruces, en el cual incluye el análisis para las Infraestructuras del PNACP a nivel regional.

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, por lo 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 a las infraestructuras, entre ellas los depósitos que se encuentran a nivel de las regiones.

Asimismo, frente a inundaciones se ven afectados los canales de acceso de distribución de recursos hidrobiológicos, pudiendo afectar la disponibilidad de éstos en los mercados.

4.1.1.4 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 podría comprometer a las infraestructuras de algunos depósitos ubicados en las regiones, así como la seguridad y bienestar del personal de la zona o si éstos estuviesen ejecutando alguna actividad o intervención del PNACP, por lo que es necesario la activación del PCO.

También, frente a este suceso se pueden ver afectados los canales de acceso de distribución de recursos hidrobiológicos, pudiendo afectar la disponibilidad de los mismos en los mercados, y las acciones relacionadas a las actividades programadas en cuanto a talleres de difusión, campañas, plataformas comerciales, entre otros.

4.1.1.5 Epidemia o Pandemia

Para el caso de una emergencia de epidemia o pandemia declarada por la autoridad máxima del Estado, como ya se vivió en el año 2020, se seguirán los protocolos declarados por el Gobierno y establecidos por el PNACP.

Con motivo de frenar la propagación del virus, está ya establecido que se vean paralizadas 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 a la Sede Central, y convocando solo la asistencia de la Alta Dirección y los Jefes de las Unidades que están a cargo de la toma de decisiones e involucrados directamente en procesos para la operatividad del PNACP.

Frente a esta amenaza se tiene la experiencia de las 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 PNACP en el ámbito de su competencia.

Sin embargo, se requeriría la activación del Plan de Continuidad Operativa, en cuanto a las actividades relacionadas a la captación de demanda del recurso hidrobiológico como lo son los talleres de difusión, campañas, plataformas comerciales, entre otras; en cuanto a la disposición, acceso y distribución de la oferta.

4.1.1.6 Heladas y Friaje

Las heladas y el friaje son fenómenos atmosféricos que ocurren en el Perú y afectan la salud, la economía y la agricultura. Las Heladas se producen cuando la temperatura del aire baja a 0°C o menos, son más frecuentes en los departamentos de Puno, Arequipa y Tacna (sierra) y van de abril a septiembre, con mayor intensidad en junio y julio.

El Friaje se produce cuando aire frío de la Antártida ingresa al Perú por la selva sur, se caracteriza por lluvias, tormentas eléctricas y viento; afectaría a los departamentos de Madre de Dios, Ucayali, Huánuco, San Martín y Loreto (selva), provoca un aumento de infecciones respiratorias, como gripe, resfriado, bronquitis, amigdalitis y faringitis; lo que representa un riesgo de mortalidad infantil y de la población adulta mayor.

Ante este escenario, cabe indicar que ambas amenazas representan un riesgo directo en la población, así como la seguridad y bienestar del personal de la zona o si éstos estuviesen ejecutando alguna actividad o intervención del Programa, afectando seriamente el objetivo del PNACP.

Asimismo, frente a esta amenaza, la infraestructura expuesta del PNACP es evaluada ante acontecimientos de heladas y friajes, por lo que se realizan diferentes análisis para cada una de las eventualidades, consecuentes del descenso de temperatura en la sierra y selva[4].

4.1.1.7 Alteraciones en el Orden Público

En concordancia con el Plan de Continuidad Operativa del Ministerio de la Producción, se consideran 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 los objetivos en cuanto a la demanda y oferta del recurso hidrobiológico, ya que el PNACP no se encuentra exento de huelgas, concentraciones públicas (por parte de diversos grupos humanos, tales como gremios, grupos políticos, grupos terroristas, vandalismo, delitos, entre otros), que instiguen la agitación y generen acciones violentas, que vulneren la seguridad de las instalaciones y del personal, tanto en la Sede Central del PNACP como cuando se esté llevando a cabo alguna intervención a nivel regional; así también se ve afectado la salud e integridad de las personas y se generan daños materiales frente a hurto, sabotaje de sistema eléctrico, interrupción de las comunicaciones y de los servicios informáticos.

4.1.2 DESCRIPCIÓN DE LA INFRAESTRUCTURA

[4] En cuanto al análisis en relación con la Identificación y Elaboración de Escenarios de Riesgo de Infraestructuras del Sector Producción expuestas a Helada y Friaje, La Oficina de Seguridad y Defensa Nacional del Ministerio de la Producción remite el Informe Nº 00000090-2024-PRODUCE/OSDN-dcruces, en el cual incluye el análisis para las Infraestructuras del PNACP a nivel nacional.

Como se indicaba en el capítulo I. Información General, el PNACP cuenta, a nivel nacional, con una (01) sede central, una (01) cochera y veintiséis (26) depósitos; los cuales facilitan el resguardo de los materiales para las actividades de plataformas comerciales (Pesca con Valor, Mi Pescadería y Conservas Peruanas en tu Mesa); materiales para asistencia técnica y articulación comercial para la promoción de la implementación de sistemas de almacenamiento de productos hidrobiológicos provenientes de la pesca y acuicultura; materiales para actividades de sensibilización para el fomento del consumo de productos hidrobiológicos; así como para los eventos protocolares del Programa a nivel regional.

En ese sentido, el detalle de cada uno de los locales antes mencionados se presenta en el siguiente cuadro:

Visado por TORREBLANCA GARCIA Miluska Erika FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/04/30 10:24:15-0500

Visado por MILLONES SORIANO Luis Andres FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/04/30 15:24:53-0500

Visado por PUENTE DE LA VEGA CHUMBE Felix Fabian FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/04/30 15:27:40-0500

Cuadro N° 04: Descripción de la infraestructura del PNACP

N°	Tipo de Local	Condición del Inmueble	Tipo de Bien	Uso Específico	Departamento	Provincia	Distrito	Dirección	Urbanización - Sector	Mz - Lote	Área (m2)	Tipo de Documento Registral	Número de Partida Registral
1	COCHERA	ALQUILADO	Edificio completo / otras edificaci	Cochera	Callao	Callao	Bellavista	Elías Aguirre 214			642.00	Partida Registral	70093243 - 70093244
2	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Huancavelica	Huancavelica	Huancavelica	Malecón Santa Rosa N°160	-	-	80.00	Partida Registral	11030342
3	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Apurímac	Abancay	Abancay	Av. Pachacútec N°200-202 pasaje S/N	Asociación Villa Republicana 7 de agosto	Mz A Lote 8- Primer Pis	80.00	Partida Registral	2003396
4	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Ica	Ica	Ica	Urbanizacion Santa Elena D-13 A2			72.00	Partida Registral	11059264
5	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Madre de dios	Tambopata	Tambopata	Jr. Sinchi Roca	-	Lote 11 S/N	72.00	Partida Registral	57006005
6	SEDE CENTRAL	ALQUILADO	Edificio completo / otras edificaci	Sede Central	Lima	Lima	Sain isidro	Calle Antequera N° 671			543.93	Partida Registral	12435913
7	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Pasco	Pasco	Yanacancha	Jr. Manuel Ubalde N° 406	San Juan		120.00	Partida Registral	P 13008390
8	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Moquegua	Mariscal Nieto	Moquegua	Villa Moquegua	CP San Antonio	Mz 05 Lote 11	120.00	Partida Registral	P 08009260
9	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Tumbes	Tumbes	Tumbes	Jr. Huascar N°110	-	-	140.00	Partida Registral	2004717
10	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Cajamarca	Cajamarca	Cajamarca	Jr. Tarapaca N°414			120.00	Partida Registral	2121291
11	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Amazonas	Amazonas	Chachapoyas	Jr. Hermosura N° 708			80.00	Partida Registral	11022113
12	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Tacna	Tacna	Tacna	Asociacion de Vivienda Cabo Teodoro R. Pisco, 1er Piso	-	Mz H lote 14	100.00		-
13	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Ucayali	Coronel Portillo	Calleria	Jr. Raymondi N° 250-C			65.59	Partida Registral	627
14	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Ayacucho	Huamanga	Ayacucho	Jr. Los laureles N° 202			82.00	Partida Registral	11092456
15	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	La libertad	Trujillo	Trujilo	Calle Borgoño 195 Barrio Int. 101	El Molino		82.50	Partida Registral	11017020
16	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Cusco	Cusco	Wanchaq	Urb. Jhon f Kennedy Zona A , Pasaje Onix		MZ A Lote 28	140.00	Partida Registral	2002169
17	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Junín	Huancayo	El Tambo	Jr. Las Lomas N° 116			152.00	Partida Registral	11147987
18	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Huánuco	Huanuco	Huanuco	Av. Universitaria N° 246	Urb. T.R.M Pilcomarca	Lote 01	72.00	Partida Registral	2006700
19	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Piura	Piura	Piura	AA.HH. Los Ficus		Mz H2 Lote 4 - Segunda Etapa	80.00	Partida Registral	P15043539
20	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Puno	Puno	Puno	llave N° 760			55.00	Partida Registral	11089259
21	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Lima	Huaura	Huacho	Av. Francisca Vidal N° 701 C 1er Piso			45.00	Partida Registral	50002784
22	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	San Martín	San Martin	Tarapoto	Jirón Jorge Chávez N° 726-728			96.00	Partida Registral	5005443
23	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Ancash	Huaraz	Independencia	Av. Centenario S/N	Barrio Monterrey		100.00	Partida Registral	2003136
24	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Loreto	Maynas	Loreto	Calle Pablo Rosell N° 759	AAHH Daneil Alcides Carrión	Mz D, Lote17 Segunda etapa	177.64	Partida Registral	P12016587
25	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Lambayeque	Chiclayo	Chiclayo	Calle Alfonso Ugarte N° 546			40.00	Partida Registral	P10123882
26	ARCHIVO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Lima	Lima	San Isidro	Av. Paseo de la República 3591			6.70	Partida Registral	13009416
27	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Deposito	Arequipa	Arequipa	Cercado de Arequipa	Av. Independencia N°2053			100.00	Partida Registral	11563236
28	DEPÓSITO	ALQUILADO	Edificio completo / otras edificaci	Sede central	Lima	Lima	Sain isidro	Calle Antequera N° 606			120.00	Partida Registral	49030870

Fuente: Sub Unidad de Abastecimiento del PNACP

4.1.3 DETERMINACIÓN DEL RIESGO

Para la determinación del riesgo, el PNACP 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 del Objetivo Estratégico Institucional de la institución, cuyo local se encuentra dentro del ámbito a nivel nacional:

Cuadro N° 05: Listado de sedes y depósitos a nivel nacional del PNACP

PELIGROS DE ORIGEN NATURAL Y/O PELIGROS POR ACCIÓN HUMANA	LISTADO DE LOCALES DEL PNACP A NIVEL NACIONAL																											
	LIMA	CALLAO	LIMA	LIMA PROVINCIA	HUANCAVELICA	APURIMAC	ICA	MADRE DE DIOS	AREQUIPA	PASCO	MOQUEGUA	TUMBES	CAJAMARCA	AMAZONAS	TACNA	UCAYALI	AYACUCHO	LA LIBERTAD	CUSCO	JUNÍN	HUANUCO	PIURA	PUNO	SAN MARTÍN	ANCASH	LORETO	LAMBAYEQUE
	SEDE CENTRAL LIMA SAN	COCHERA	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO	DEPÓSITO
SISMO DE GRAN MAGNITUD																												
INCENDIO																												
LLUVIAS INTENSAS - INUNDACION																												
MOVIMIENTOS EN MASA																												
EPIDEMIA O PANDEMIA																												
HELADAS Y FRIAJE																												
ALTERACIONES EN EL ORDEN PUBLICO																												

Elaboración: Grupo de Comando del PNACP

Al respecto, cabe resaltar que, a pesar de no encontrarse con un alto impacto en todas las regiones de intervención del Programa, se ha considerado como un riesgo a los fenómenos naturales de heladas y friajes, y lluvias intensas, debido a que, en caso se concrete uno de estos riesgos en las zonas de impacto medio, alto y muy alto, se ocasionaría la interrupción de los servicios del Programa en forma total o parcial.

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 los objetivos e intervenciones del PNACP, estableciendo el período máximo tolerable de interrupción.

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 el siguiente cuadro 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:

Cuadro N° 06: Matriz de Impacto

PELIGRO / ESTIMACION DEL NIVEL DE IMPACTO	SISMO DE GRAN MAGNITUD	INCENDIO	EPIDEMIA O PANDEMIA	HELADAS FRIAJE	ALTERACIONES EN EL ORDEN PUBLICO	PERIODO TOLERABLE MAXIMO DE INTERRUPCION
ARTICULACIÓN COMERCIAL DE PRODUCTOS HIDROBIOLÓGICOS	Riesgo Medio	Riesgo Bajo	Riesgo Medio	Riesgo Bajo	Riesgo Muy Alto	1 DIA
TALLERES DE SENSIBILIZACIÓN EN EDUCACIÓN ALIMENTARIA	Riesgo Alto	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Riesgo Muy Alto	1 DIA
PROMOCIÓN DE PRODUCTOS HIDROBIOLÓGICOS	Riesgo Medio	Riesgo Alto	Riesgo Medio	Riesgo Medio	Riesgo Muy Alto	1 DIA

Fuente: Grupo de Comando del PNACP

De acuerdo con el cuadro N° 06, el nivel de impacto que tendría cada uno de los servicios del PNACP frente a los peligros identificados, muestra la acción que requiere seguirse frente a una evacuación y el periodo máximo de interrupción que este peligro genere.

En la misma línea de mostrar el nivel de impacto a mayor detalle, a nivel de cada una de las estructuras, el nivel de riesgo para el PNACP se grafica en el cuadro N° 05, en la página anterior.

4.3 IDENTIFICACIÓN DE RECURSOS

Conociendo los peligros y los niveles de impacto que ocasionaría algún evento disruptivo, es necesario precisar que el PNACP debe contar con recursos prioritarios para la respuesta ante cualquier 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 (carpas). En tal sentido, se identificaron los recursos humanos potenciales y recursos materiales indispensables del PNACP.

4.3.1 Identificación de los recursos humanos del PNACP

Para determinar la relación nominal del personal crítico (mínimo indispensable), se considera asegurar la continuidad operativa del PNACP ante un evento adverso. Para ello, es necesario comprender que no está referido a todo el personal de las unidades orgánicas, sino el personal mínimo que se necesita en esas condiciones. En ese sentido, el alcance del personal priorizado en el PNACP[5] se ha identificado en base a la necesidad de cada unidad de organización, entendiéndose que ha de desarrollar la priorización de las actividades a fin de mantener la continuidad operativa de la entidad. En lo posible debe considerarse doble asignación de funciones, si así se requiriese.

[5] Mediante el Informe Técnico Nº 00000014-2025-PNACP/UAF-SUB-URH se brinda información respecto a la identificación de los recursos humanos para la ejecución de las actividades críticas en la Entidad.

Cuadro N° 07: Identificación de Recursos Humanos

PERSONAL PRIORITARIO	UNIDAD ORGANICA	CANTIDAD DE PERSONAS SEDE CENTRAL	CANTIDAD DE PERSONAS REGIONALES	TOTAL PERSONAL CLAVE
UNIDAD DE DIRECCION	COORDINACION EJECUTIVA	2		2
UNIDADES DE ASESORAMIENTO Y APOYO	UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	2		2
	UNIDAD DE ASESORIA LEGAL	2		2
	UNIDAD DE ADMINISTRACION Y FINANZAS	11		11
	UNIDAD DE ADMINISTRACION Y FINANZAS	2		2
	SUB UNIDAD DE RECURSOS HUMANOS	2		2
	SUB UNIDAD DE ABASTECIMIENTO	4		4
	SUB UNIDAD DE CONTABILIDAD	1		1
	SUB UNIDAD DE SERVICIOS GENERALES	1		1
	SUB UNIDAD DE TESORERÍA	1		1
UNIDADES TÉCNICAS	UNIDAD DE SENSIBILIZACIÓN	3	10	13
	UNIDAD DE PROMOCIÓN	2	25	27
	UNIDAD DE ARTICULACIÓN	3	15	18
	UNIDAD DE GESTIÓN REGIONAL	2	10	12
TOTAL		**27**	**60**	**87**

Fuente: Sub Unidad de Recursos Humanos del PNACP

4.3.2 Identificación de los recursos materiales del PNACP

Luego de conocer el personal crítico (mínimo indispensable), se debe asegurar contar con los recursos materiales para la continuidad operativa del PNACP ante un evento adverso. En ese sentido, el alcance del material priorizado en el PNACP[6] se ha identificado en base a la necesidad de cada unidad orgánica.

Respecto a lo anterior, del parque informático existente se ha priorizado para las actividades críticas en el PNACP, según se detalla en el siguiente cuadro.

[6] Mediante el Informe Técnico Nº 00000006-2025-CCANALES se brinda información respecto a la identificación de los recursos materiales en la Entidad.

Cuadro N° 08: Equipos asignados por Unidades del PNACP

UNIDAD ORGANICA	CPU	MONITOR	UPS
COORDINACION EJECUTIVA	2	2	2
UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	2	2	2
UNIDAD DE ASESORIA LEGAL	2	2	2
UNIDAD DE ADMINISTRACION Y FINANZAS	11	11	11
UNIDAD DE ADMINISTRACION Y FINANZAS	2	2	2
SUB UNIDAD DE RECURSOS HUMANOS	2	2	2
SUB UNIDAD DE ABASTECIMIENTO	4	4	4
SUB UNIDAD DE CONTABILIDAD	1	1	1
SUB UNIDAD DE SERVICIOS GENERALES	1	1	1
SUB UNIDAD DE TESORERÍA	1	1	1
UNIDAD DE SENSIBILIZACIÓN	3	3	3
UNIDAD DE PROMOCIÓN	2	2	2
UNIDAD DE ARTICULACIÓN	3	3	3
UNIDAD DE GESTIÓN REGIONAL	2	2	2
TOTAL	27	27	27

Fuente: Unidad de Administración y Finanzas

Cuadro N° 09: Servidores Informáticos del PNACP

N°	Oficina	CPU
1	Servidor NAS	2
2	Servidor HP	2
3	Servidor DELL	3
4	Switch Capa 3	7
5	UPS + Banco de bateria (3kva)	7
Total		**21**

Fuente: Sub-Unidad de Abastecimiento del PNACP

Cabe precisar que el Sistema de Trámite Documentario - SITRADOC se encuentra alojado en los servidores del Ministerio de Producción, donde el PNACP es un usuario más. Ante un evento adverso, la operatividad del trámite documentario para el PNACP debe ser garantizada de acuerdo con el Plan de Recuperación de los Servicios Informáticos del Ministerio de la Producción, aprobado mediante Resolución Ministerial N° 00307-2022-PRODUCE.

Asimismo, ante cualquier amenaza interna o externa que comprometa y/o afecte los diferentes sistemas de información de los que el PNACP es usuario, que comprende todos los elementos orientados al tratamiento y administración de datos e información, organizados para su uso posterior, que han sido generados para cubrir una necesidad u objetivo del PNACP, incluyendo hardware, software, así como cualquier elemento interno o externo relacionado a los mismos, será de aplicación lo dispuesto en el Anexo 2: Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información de la Sala de Servidores , y supletoriamente lo mencionado en el Plan de Recuperación de los Servicios Informáticos del Ministerio de la Producción.

V ACCIONES PARA LA CONTINUIDAD OPERATIVA

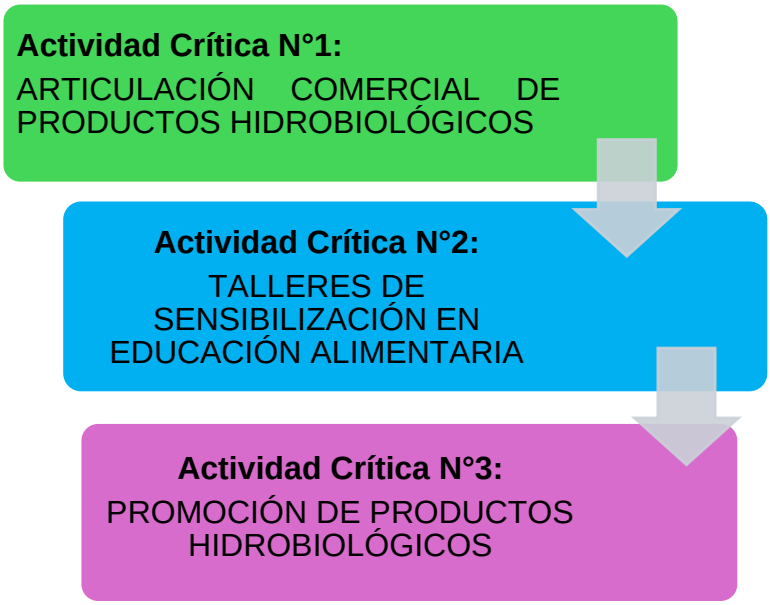
El PNACP, en cuanto a las acciones a seguir para asegurar la continuidad operativa, determina las actividades críticas que son aquellas actividades y tareas que se desarrollan en la entidad, en sus diferentes unidades orgánicas que hayan sido identificadas como actividades críticas indispensables y que no deberían paralizar las acciones normales del Programa, y se analizan con el propósito de asistir al cumplimiento de la misión institucional.

5.1 DETERMINACIÓN DE LAS ACTIVIDADES CRÍTICAS DEL PNACP

Las diferentes unidades orgánicas del Programa determinaron las actividades críticas que consideraron son indispensables en el marco de la gestión de continuidad operativa.

El Grupo de Comando, conforme a las disposiciones específicas establecidas en 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", aprobados por Resolución Ministerial N° 320-2021-PCM del 30.12.2021, ha priorizado tres (03) actividades críticas, las cuales se indican a continuación:

Gráfico N° 03: Actividades Críticas



En la gestión de la continuidad operativa, las actividades críticas son aquellas que no deben detenerse ante alguna ocurrencia de un desastre o cualquier evento que interrumpa prolongadamente sus operaciones; 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 el siguiente cuadro se detalla las actividades con mayor prioridad, las cuales se considerarán como actividades críticas para el presente Plan de Continuidad Operativa (PCO); a continuación, se muestra la relación de las Actividades Críticas, Unidad responsable y los procedimientos asociados identificados:

Cuadro N° 10: Actividades Críticas y Procedimientos Asociados

PROCESO	ACTIVIDAD CRÍTICAS	TAREAS / ACCIONES	UNIDAD RESPONSABLE (*)
Agentes de la pesca y acuicultura con apertura a nuevos mercados y consolidación de mercados existentes	Articulación comercial de productos hidrobiológicos	Pedido y venta concretada de productos hidrobiológicos	Unidad de Articulación
		Registro de colocaciones	
		Registro de Planes de Negocio	
		Registro de Estudios de Mercado	
Organización y ejecución de espacios e iniciativas para fomentar la comercialización y consumos de productos hidrobiológicos	Talleres de sensibilización en educación alimentaria	Coordinación con la comunidad educativa	Unidad de Sensibilización
		Programación de talleres de sensibilización	
		Ejecución y seguimiento de los talleres de sensibilización	
		Reporte de los talleres de sensibilización	
Ciudadanos con mayor acceso y disponibilidad de productos hidrobiológicos ofertados por Agentes de la Pesca y Acuicultura	Promoción de productos hidrobiológicos	Contacto con el GORE o GOL	Unidad de Promoción
		Coordinación de la feria de promoción	
		Programación de la feria de promoción	
		Difusión de la feria	
		Ejecución de la feria de promoción	
		Registro de información de la feria	

(*) Corresponde a Unidades de Línea del PNACP con actividades críticas.
Elaboración: Grupo de Comando del PNACP.

5.2 ASEGURAMIENTO DEL ACERVO DOCUMENTARIO

Frente a las amenazas potenciales, es necesario adoptar e implementar una serie de medidas de emergencia que nos permitan proteger y custodiar la documentación que poseen los archivos del PNACP. Por ello, es necesario realizar periódicamente copias de seguridad de las principales series documentales que por su valor e importancia requieren conservarse.

En el Manual de Operaciones se establece que la Sub-Unidad de Abastecimiento es la que conduce, organiza y ejecuta la gestión documentaria y archivo.

Considerando la gestión documental del PNACP, se realizará y aplicará un conjunto de procedimientos con el objetivo de organizar, dirigir, almacenar y controlar los documentos en soporte físico y electrónico. Por estas razones, para el aseguramiento del acervo documentario se deberá de realizar las siguientes actividades:

- Cada unidad orgánica es responsable de su acervo documentario en soporte físico. Para el caso de documentos electrónicos se deberá de coordinar con la Sub Unidad de Abastecimiento la custodia y almacenamiento de sus documentos generados electrónicamente (copias de seguridad de sus documentos generados por el Sistema de Trámite Documentario – (SITRADOC).

- La Sub Unidad de Abastecimiento cuenta con un Plan Anual de Trabajo Archivístico (PATA) que se actualiza cada año. Este plan contempla actividades de digitalización de documentos sin valor legal (valor informativo), como medida de contingencia ante cualquier eventualidad, y con el objetivo de garantizar la integridad y disponibilidad de dichos documentos.

En previsión de casos de desastre, o de algún ataque informático, en el que se vieran afectados los equipos de la entidad, la data, el motor de la base de datos, entre otros; el PNACP ha previsto contar con un servicio de respaldo en la nube (Cloud) o la ubicación de algún equipo de backup en, al menos, otra región del país. En estos momentos se realizan backups a los correos, base de datos y a los servidores virtuales en un equipo NAS y un equipo File Server. Se deberá prever las acciones necesarias, con la debida anticipación, para contar con suficiente capacidad de almacenamiento antes de estar bordeando el total de dicha capacidad.

Corresponde al encargado de la gestión documentaria y archivo coordinar las inspecciones y operaciones de mantenimiento del Archivo Central (repositorios) que alberga la documentación en soporte físico, para prever incendios y demás accidentes o incidentes que coloquen en riesgo la información que contienen los mencionados documentos, así como goteos e incremento de la humedad en los documentos, lo que generará un alto desarrollo de ácaros y hongos que deteriorarán la documentación.

5.3 ASEGURAMIENTO DE LA BASE DE DATOS MEDIANTE LA EJECUCIÓN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS.

Teniendo en cuenta que el desarrollo y ejecución de las actividades críticas identificadas para el Plan de Continuidad Operativa del PNACP, dependen de la disponibilidad inmediata de los aplicativos informáticos requeridos para estas funciones críticas, se debe asegurar la Base de Datos del PNACP.

De ser necesaria la recuperación de la Base de Datos, los servicios de tecnología de la información deben ser realizados por personal técnico y profesional para mantener y restablecer de forma inmediata las acciones administrativas para las operaciones del PNACP. En ese sentido, se listan las herramientas informáticas a considerar para su mantenimiento correctivo y restablecimiento.

- Sistema Integrado de Administración Financiera (SIAF)

- Sistema Integrado de Gestión Administrativa (SIGA)
- Sistema de Trámite Documentario (SITRADOC)
- Sistema de Información PNACP.

5.4 ROLES Y RESPONSABILIDADES PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

A continuación, se muestra la conformación del Grupo de Comando conforme lo establecido en la Resolución Ministerial N°320-2021-PCM del 30.12.2021 "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".

5.4.1 Conformación del Grupo de Comando

Mediante Resolución de Coordinación Ejecutiva Nº 00001-2025-PNACP del 03 de enero de 2025, se aprueba la conformación del Grupo de Comando del Programa Nacional "A Comer Pescado", definido como un grupo de profesionales que tienen como función principal la elaboración, modificación e implementación del Plan de Continuidad Operativa (PCO) bajo el liderazgo del Jefe de la Unidad de Planeamiento, Presupuesto y Modernización, como titular de la unidad orgánica a cargo de la Gestión de la Continuidad Operativa.

Tiene como instancia funcional la toma de decisiones para la gestión y administración de la continuidad, permitiendo el desarrollo de las actividades críticas identificadas de la entidad.

La conformación del Grupo de Comando del PNACP se detalla a continuación:

Cuadro N° 11: Grupo de Comando del Programa Nacional "A Comer Pescado"

INTEGRANTES DEL GRUPO DE COMANDO	
RM N° 320-2021-PCM	**PNACP**
TITULAR DE LA UNIDAD ORGÁNICA A CARGO DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA (Preside)	Jefe/a de la Unidad de Planeamiento, Presupuesto y Modernización
UN REPRESENTANTE DE LA UNIDAD ORGÁNICA CUYA ACTIVIDAD HA SIDO IDENTIFICADA COMO CRÍTICA	Jefe/a de la Unidad de Promoción Jefe/a de la Unidad de Articulación Jefe/a de la Unidad de Sensibilización
UN REPRESENTANTE DE LA UNIDAD ORGÁNICA A CARGO DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA	Especialista en Presupuesto
UN REPRESENTANTE DE LA UNIDAD ORGÁNICA RESPONSABLE DE LA GESTIÓN DE RIESGOS DE DESASTRES	Sub Jefe/a de la Sub-Unidad de Recursos Humanos

UN REPRESENTANTE DE LA UNIDAD ORGÁNICA DE ADMINISTRACIÓN	Jefe/a de la Unidad de Administración y Finanzas
UN REPRESENTANTE DE LA UNIDAD DE RECURSOS HUMANOS	Sub Jefe/a de la Sub-Unidad de Recursos Humanos
UN REPRESENTANTE DE LA UNIDAD ORGÁNICA DE TECNOLOGÍAS DE LA INFORMACIÓN	Sub Jefe/a de la Sub-Unidad de Abastecimiento
UN REPRESENTANTE DE LA UNIDAD ORGÁNICA DE COMUNICACIÓN	Especialista en Comunicaciones

Fuente: RM N° 320-2021-PCM.

5.4.2 Roles y responsabilidades para el desarrollo de las actividades críticas

El Grupo de Comando para la gestión de la continuidad operativa del PNACP, conformado mediante la Resolución de Coordinación Ejecutiva Nº 00001-2025-PNACP, 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.

Cuadro N° 12: Roles y Responsabilidades

N°	MIEMBROS	RESPONSABILIDADES
1	**Unidad de Planeamiento, Presupuesto y Modernización**	Disponer la implementación de las decisiones adoptadas por el Grupo de Comando para la continuidad operativa.
		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 la Coordinación Ejecutiva del PNACP en la declaración de crisis operativa.
2	**Unidades de Línea cuya actividad ha sido identificada como crítica (UA, UP y US)**	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 la Coordinación Ejecutiva del PNACP en la declaración de crisis operativa.
3	**Unidad de Administración y Finanzas**	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 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 PNACP sede alterna, centro de cómputo, en coordinación con las unidades orgánicas responsables.
		Realizar las actividades que le sean asignadas por la Coordinación Ejecutiva del PNACP durante la declaración de crisis operativa.
4	**Sub-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 (GRD)
		Realizar las actividades que le sean asignadas por la Coordinación Ejecutiva del PNACP durante la declaración de crisis operativa.
5	**Sub-Unidad de Abastecimiento**	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 la Coordinación Ejecutiva del PNACP en la declaración de crisis operativa.
		Restablecer la operatividad y asegurar la continuidad de los sistemas e infraestructura tecnológica
6	**Sub- Unidad de Servicios Generales**	Supervisar las condiciones de la infraestructura física, mobiliario, vehículos y equipos necesarios para asegurar la operatividad institucional
		Coordinar y ejecutar acciones de mantenimiento, conservación, seguridad y reparación de las instalaciones, equipos, vehículos y demás bienes de uso del PNACP, con excepción de los vinculados a la infraestructura tecnológica.
		Supervisar y controlar el uso de los bienes muebles e inmuebles del PANCP, en el marco de la normatividad vigente.
		Realizar las actividades que le sean asignadas por la Coordinación Ejecutiva del PNACP en la declaración de crisis operativa.

		Restablecer la operatividad y asegurar la continuidad del mobiliario y el equipamiento.

Elaboración: Grupo de Comando - PNACP.

5.5 REQUERIMIENTOS

5.5.1. Requerimiento de personal

La Unidad de Administración y Finanzas, a través de la Sub-Unidad de Recursos Humanos, determinará la relación nominal y personalizada del personal prioritario mínimo indispensable (personal crítico), para asegurar la continuidad operativa del PNACP ante un evento adverso, entendiéndose a éste como el mínimo personal necesario con base a los requerimientos de cada unidad. El personal crítico identificado se presenta en el siguiente cuadro:

Cuadro N° 13: Personal Crítico del PNACP

PERSONAL PRIORITARIO	UNIDAD ORGANICA	CANTIDAD DE PERSONAS SEDE CENTRAL	CANTIDAD DE PERSONAS REGIONALES	TOTAL PERSONAL CLAVE
UNIDAD DE DIRECCION	COORDINACION EJECUTIVA	2		2
UNIDADES DE ASESORAMIENTO Y APOYO	UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	2		2
	UNIDAD DE ASESORIA LEGAL	2		2
	UNIDAD DE ADMINISTRACION Y FINANZAS	11		11
	UNIDAD DE ADMINISTRACION Y FINANZAS	2		2
	SUB UNIDAD DE RECURSOS HUMANOS	2		2
	SUB UNIDAD DE ABASTECIMIENTO	4		4
	SUB UNIDAD DE CONTABILIDAD	1		1
	SUB UNIDAD DE SERVICIOS GENERALES	1		1
	SUB UNIDAD DE TESORERÍA	1		1
UNIDADES TÉCNICAS	UNIDAD DE SENSIBILIZACIÓN	3	10	13
	UNIDAD DE PROMOCIÓN	2	25	27
	UNIDAD DE ARTICULACIÓN	3	15	18
	UNIDAD DE GESTIÓN REGIONAL	2	10	12
TOTAL		**27**	**60**	**87**

Fuente: Sub-Unidad de Recursos Humanos del PNACP

5.5.2. Requerimiento de Material y Mobiliario

La Unidad de Administración y Finanzas, a través de la Sub-Unidad de Abastecimiento, tendrá a su cargo la implementación de los requerimientos en mobiliarios, bienes, recursos y otros, para facilitar la continuidad operativa del PNACP ante un desastre de gran magnitud, para ello se establecerá los recursos en las sede alterna o receptora, que se pueden utilizar.

La Sub-Unidad de Abastecimiento y la Sub Unidad de Servicios Generales del PNACP, pondrá en ejecución la recuperación de los servicios de tecnología de información, aplicando lo establecido en el "Plan de Recuperación de los Servicios Informáticos del Ministerio de la Producción", aprobado por la Resolución Ministerial N° 00307-2022-PRODUCE; así como lo relacionado al mobiliario y equipamiento necesario para la continuidad operativa.

A efectos de contar con los materiales y equipos necesarios, se identificaron los recursos por proceso, que son necesarios para la operatividad de los procesos críticos, y que se detallan en el siguiente Cuadro:

Cuadro N° 14: Materiales y Mobiliario del PNACP

N°	META	UNIDADES	BIENES PARA LA OFICINAS Y MATERIALES					MAQUINARIA Y EQUIPOS					
			CARPAS	ESCRITORIOS	SILLAS	PAPEL BOND (MILL)	TONER	LAPTOP	IMPRESORA	UNIDAD DE TRANSPORTE	GRUPO ELECTROGENO	EXTINTORES	PROYECTOR
1	001	UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	1	2	2	1	2	1	1				
2	002	COORDINACIÓN EJECUTIVA	1	1	1	1	2	1	1				
3	003	UNIDAD DE ADMNISTRACION Y FINANZAS		2	2	1	2	2	1			1	
4	004	UNIDAD DE ASESORÍA LEGAL		1	1	1		1					
5	006	UNIDAD DE PROMOCIÓN	1	5	5	1	2	2	1				
6	007	UNIDAD DE SENSIBILIZACIÓN		5	5	1		2				1	
7	008	UNIDAD DE ARTICULACIÓN		5	5	1	2	2	1				
8	010	UNIDAD DE GESTIÓN REGIONAL		2	2	2	2	1					
9	003	SUB-UNIDAD DE ABASTECIMIENTO		5	5	6	4	2	1	7		1	
10	003	SUB-UNIDAD ABASTECIMIENTO (PATRIMONIO)	1	1	1			1					
11	003	SUB-UNIDAD DE ABASTECIMIENTO (TI)		1	1			1			1		1
12	003	SUB-UNIDAD DE CONTABILIDAD	1	3	3	1		3					
13	003	SUB-UNIDAD DE TESORERÍA		3	3	1		3					
14	003	SUB-UNIDAD DE RECURSOS HUMANOS		3	3	1	2	3	1			1	
15	003	SUB-UNIDAD DE SERVICIOS GENERALES		1	1	1							
TOTALES			**5**	**40**	**40**	**18**	**16**	**25**	**7**	**7**	**1**	**4**	**1**

Elaboración: Sub Unidad de Abastecimiento del PNACP

Para enfrentar de manera adecuada un riesgo de desastre, es fundamental contar con un conjunto de materiales y equipos que permitan responder de manera eficaz y segura. Aquí presentamos una lista de requerimientos básicos de materiales y equipos que son necesarios en caso de un desastre:

Cuadro N° 15: Requerimiento de Unidades de Línea

N°	ACTIVIDADES CRÍTICAS	UNIDAD RESPONSABLE	PROCEDIMIENTO ASOCIADO	CLIENTE DEL PROCESO	ACTIVIDADES DESARROLLADAS	MATERIAL ASIGNADO	EQUIPO ASIGNADO	PRESUPUESTO ASIGNADO	FECHA DE ACTUALIZACIÓN
1	ARTICULACIÓN COMERCIAL DE PRODUCTOS HIDROBIOLÓGICOS	UNIDAD DE ARTICULACIÓN	**Agentes de la pesca y acuicultura con apertura a nuevos mercados y consolidación de mercados existentes.** -Pedido y venta concretada de productos hidrobiológicos -Registro de colocaciones -Registro de Planes de Negocio -Registro de Estudios de Mercado	.Armadores - Pescadores artesanales - Plantas procesadoras - Acuicultores - MYPEs relacionadas a la pesca y acuicultura - Otros agentes de la pesca y acuicultura - Canales comerciales	- Articulación comercial - Asistencia técnica	- Termómetro - Ictiómetro - Folleteria y formatos - Banners	- PC, fotocopiadora, laptos	Presupuesto Institucional	21.02.2025
2	TALLERES DE SENSIBILIZACIÓN EN EDUCACIÓN ALIMENTARIA	UNIDAD DE SENSIBILIZACIÓN	Organización y ejecución de espacios e iniciativas para fomentar la comercializacion y consumo de productos hidrobiológicos	- Grupos Focalizados	- Talleres de sensibilización	- Material educativo y didactico - Banners y folleteria	- PC, fotocopiadora, laptos	Presupuesto Institucional	21.02.2025
3	PROMOCIÓN DE PRODUCTOS HIDROBIOLÓGICOS	UNIDAD DE PROMOCIÓN	Ciudadanos con mayor acceso y disponibilidad de productos hidrobiologicos ofertados por Agentes de la Pesca y Acuicultura.	.Ciudadanos	Ferias de Promoción de productos hidrobiológicos	Toldos institucionales, mesas plegables, roll screen, tacho de basura, mandil hule, papel toalla, guante descartable, plastico hule, gorro quirurgico, gel antibacterial, entre otros	Balanzas, megafonos, parlante amplificador, pc, fotocopiadora	Presupuesto Institucional	21.02.2025
Nota: Unidades de Línea consideradas como crítica									

Elaboración: Grupo del Comando del PNACP

El trámite para gestionar requerimientos de los materiales indispensables para completar las necesidades de las actividades críticas corresponde a las Unidades responsables, para lo cual deben remitir sus necesidades a la Unidad de Administración y Finanzas, así como realizar las gestiones para la ejecución de las actividades críticas, particularmente aquellas que se requieran en las sedes alternas.

Con respecto a las sedes alternas, se tomará en cuenta las necesidades para equipar a dichas sedes, así como las necesidades para operar desde infraestructura de Tipo Móvil utilizando Carpas o Módulos adecuados.

5.5.3 Requerimiento Informático

Respecto a la identificación de la cantidad de recursos humanos priorizados para poder garantizar la ejecución de las actividades críticas dentro del PNACP, es preciso indicar que, en situaciones de desastre, ya sea natural o provocado por factores externos, la asignación de recursos tecnológicos al personal se vuelve una prioridad crítica para garantizar la continuidad de las operaciones y la seguridad de los colaboradores. Los recursos tecnológicos adecuados no solo permiten una respuesta rápida y coordinada ante la emergencia, sino que también son esenciales para mantener la comunicación y la operatividad de la entidad en condiciones adversas.

Para ello, se requiere proporcionar recursos tecnológicos a veintisiete (27) colaboradores en la Sede Central y sesenta (60) colaboradores en regiones donde interviene el PNACP, con la finalidad de garantizar la continuidad operativa del Programa, identificándose los recursos necesarios para asegurar la operatividad de los servicios informáticos en situación de contingencia siguientes:

Cuadro N° 16: Equipos y servicios requeridos por el PNACP ante un desastre para continuar con la operatividad

RECURSO INFORMÁTICO	CANTIDAD	Nº USUARIOS ATENDIDOS	
		SEDE CENTRAL	REGIONES
INTERNET Y TELEFONÍA IP	1 SERVICIO	27	0
CORREO Y HERRAMIENTAS COLABORATIVAS	1 SERVICIO	27	25
SIAF	1 SISTEMA	15	0
SIGA	1 SISTEMA	15	0
OFFICE 365	1 LICENCIA	27	25
VIRTUALIZACIÓN DE SISTEMAS INFORMÁTICOS *(SISTEMA PNACP, FILESERVER, SIGA, SIAF)*	1 SERVICIO	27	0
EQUIPO DE CÓMPUTO (DESKTOP O LAPTOP)	27 DESKTOP 25 LAPTOPS	27	25
GRUPO ELECTRÓGENO DE 50 KW (1)	1 EQUIPO	27	0

Fuente: Sub Unidad de Abastecimiento del PNACP

(1) El grupo electrógeno garantizará el suministro de energía eléctrica en situaciones en las que la red eléctrica convencional se vea interrumpida debido a un evento catastrófico, como un terremoto, inundación, tormenta severa, entre otros. Por lo que se ha identificado en la plataforma

PROVEEDORES DEL ESTADO un total de trescientos noventa y cuatro (394) empresas aptas para contratar con el Estado sea adquisición o alquiler de un grupo electrógeno.

5.5.4 Requerimiento presupuestal

El Plan de Continuidad Operativa del PNACP será financiado íntegramente con cargo a los recursos presupuestales autorizados a la Unidad Ejecutora 003-1516: FOMENTO AL CONSUMO HUMANO DIRECTO - A COMER PESCADO; en el año en que se activa el PCO.

5.6 DETERMINACIÓN DE LA SEDE ALTERNA DE TRABAJO

Con fines de asegurar la ejecución del Plan de Continuidad Operativa en el menor tiempo de interrupción del funcionamiento institucional, se identificará dentro de las 24 horas, la ubicación donde se desplazarán las personas y bienes del PNACP, para seguir operando con las actividades críticas. Esto implica realizar las coordinaciones previas para que la potencial sede alterna esté preparada para disponer la implementación necesaria, de tal manera que una vez ocurrido el evento y en cuanto se haya tomado la decisión, sea la alternativa más viable para el desplazamiento.

Paralelamente, teniendo en consideración que ante el acontecimiento de un evento sísmico de gran magnitud, realmente no se puedan determinar con exactitud los daños y efectos causados en las zonas afectadas, es por ello que el propósito de este Plan de Continuidad Operativa tiene previsto contar con infraestructura de Tipo Móvil utilizando Carpas o Módulos tipificados en el “Manual de Evaluación de Daños y Análisis de Necesidades”, con el fin de ser instalados en los lugares más seguros evaluados en la conducción de las operaciones, de tal manera que asegure el desarrollo de las actividades críticas ante escenarios de incertidumbre.

SEDE ALTERNA

INSTALACIONES DEL MINISTERIO DE LA PRODUCCIÓN
Calle Uno Oeste 060 - Urbanización Córpac - Perú – 15036
Central telefónica (01) 616 2222
consultas@produce.gob.pe

5.7 ACTIVACIÓN DEL PLAN DE CONTINUIDAD OPERATIVA

La activación del Plan de Continuidad Operativa del PNACP 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 detalla los supuestos para la activación del Plan de Continuidad Operativa, que son:

- La sede central ha sido afectada total o parcialmente por un evento adverso y se ve afectada la continuidad operativa, y la sede alternativa se encuentra en condiciones de ponerse operativa.
- En caso de que el evento adverso se produjera en horas laborales, se pone en ejecución el Plan de seguridad y evacuación a zonas internas / externas.

- El Comité de Seguridad y Salud en el Trabajo (CSST) del PNACP verifica los daños en la infraestructura de la sede, a través del Formato: "Evaluación de Daños" (anexo N° 7).
- Con el Formato: "Evaluación de Daños" emitido, el responsable del Grupo de Comando propondrá al Titular de la entidad, cuando corresponda, la activación del PCO y, en consecuencia, de la sede alterna.
- El personal crítico identificado como parte de los equipos para la implementación del PCO, se encuentra disponible para realizar los trabajos de recuperación. (conforme se detalla en el cuadro N° 13 del numeral 5.5.1)

Los protocolos de actuación para la reanudación de los procesos críticos se encuentran asociados a la activación del Plan de Continuidad Operativa del PNACP, el cual se ha elaborado en tres fases (Activación, Ejecución y Desactivación), considerando las siguientes estrategias a desarrollar:

- Estrategia para la sede alterna.
- Estrategia de desarrollo de las actividades críticas.
- Trabajo presencial, remoto o trabajo mixto.
- Lineamientos para la ejecución de actividades no críticas.

Cuadro N°17: Protocolo de Activación y Desactivación de la Sede alterna

PROTOCOLO	FASES	MOMENTOS	RESPONSABLES
ACTIVACIÓN	FASE DE EJECUCIÓN (Grupo de Comando)	Verificación inicial de daños y reporte de daños	UAF/SUB-UABAS/SUB-USSGG
		Activación del Plan de Continuidad Operativa	UPPM
		Activación de la sede alterna	SUB-UABAS/SUB-USSGG/SUB-URH
		Evaluación de daños en la(s) sede(s) alterna(s)	UAF/SUB-UABAS/SUB-USSGG/SUB-URH
		Implementación con recursos materiales y equipos a la sede alterna	SUB-UABAS/SUB-USSGG
		Convocatoria del personal que ejecutará las actividades críticas.	SUB-URH
		Desarrollo de las actividades críticas (*)	US/UP/UA
DESACTIVACION	FASE DE DESACTIVACIÓN	Evaluación de los trabajos de refacción, remodelación o reconstrucción de la sede principal	UAF
		Desactivación paulatina de las actividades críticas y vuelta a la normalidad.	UPPM
NOTA: La Unidad de Gestión Regional está considerada como actividad no crítica.			

Elaboración: Grupo de Comando del PNACP

5.8 ACTIVACIÓN Y DESACTIVACIÓN DE LA SEDE ALTERNA

La activación de la sede alterna se hará efectiva a través de la aplicación del Sistema de Comunicación de Emergencia, el mismo que entra en funcionamiento inmediatamente 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 del PNACP.

En ese sentido, se busca mantener la comunicación entre el Grupo de Comando y el personal crítico y no crítico, a fin de determinar el nivel de afectación en el PNACP y proceder a activar el Plan de Continuidad Operativa.

A continuación, se detallan los supuestos y protocolos de actuación en caso de un desastre y/o emergencia:

a) Los supuestos para la activación del Plan de Continuidad Operativa serían:

- La sede central ha sido afectada total o parcialmente por un evento adverso y se ve afectada la continuidad operativa, y la sede alterna se encuentra en condiciones para ser ocupada.
- El personal crítico identificado como parte de los equipos para la implementación del PCO, se encuentra disponible para realizar los trabajos de recuperación.

b) Los protocolos de actuación para la reanudación de los procesos críticos se encuentran asociados a la activación del Plan de Continuidad Operativa del PNACP, el cual se ha elaborado en tres fases (Activación, Ejecución y Desactivación), considerando las siguientes estrategias a desarrollar:

- Estrategia para la sede alterna del PNACP.
- Estrategia de desarrollo de las actividades críticas.
- Mediante trabajo presencial, remoto o trabajo mixto.
- Lineamientos para la ejecución de actividades no críticas.

Cuadro N°18: Protocolo de Actuación del Grupo de Comando

FASES	MOMENTOS	RESPONSABLES
FASE PREVIA	Implementar en el POI la disponibilidad de recursos para la implementación de la Gestión de la Continuidad Operativa aprobada por Alta Dirección.	CE/UAF/UPPM
	Asegurar la disposición o adquisición de bienes/ servicios para la implementación de la gestión de la Continuidad Operativa	UAF/UPPM
FASE DE ACTIVACIÓN	Evaluación inicial de daños y reporte de daños	UAF/ SUB-UABAS/SUB-USSGG
	Activación del Plan de Continuidad Operativa	CE/UPPM
FASE DE EJECUCIÓN (Grupo de Comando)	Asegurar el funcionamiento y disponibilidad de recursos para la óptima ejecución de actividades críticas y no críticas.	SUB-UABAS/SUB-USSGG/ SUB-URH
	Convocatoria del personal crítico	SUB-URH

	Traslado del personal crítico implementador de las actividades críticas a la sede alterna	SUB-UABAS/SUB-USSGG
	Coordinación con proveedores internos y externos para las condiciones de seguridad del personal e instalaciones	UAF/ SUB-UABAS
	Coordinaciones con entidades de saneamiento y servicios básicos a fin de asegurar operatividad de las actividades críticas y de apoyo	UAF/ SUB-UABAS
	Coordinaciones con COEN PRODUCE, PNP, Serenazgo, Municipalidad	UAF/UPPM
	Atención de RECURSOS HUMANOS	SUB-URH
	Facilitar al personal no crítico protocolos para el trabajo remoto y/o mixto de las actividades no críticas	SUB-URH/ SUB-UABAS
	Evaluación de la afectación de la infraestructura y otros	UAF/ SUB-UABAS/SUB-USSGG
FASE DE DESACTIVACIÓN	Desactivación del Plan de Continuidad Operativa	CE/UPPM

Elaboración: Grupo de Comando del PNACP

5.9 FASES DE ACTIVACIÓN, EJECUCIÓN Y DESACTIVACIÓN DE LA SEDE ALTERNA

5.9.1. FASE ACTIVACIÓN

Esta fase se activa con el Plan de Continuidad Operativa (PCO) propiamente dicho y se activa o inicia en la gestión de la emergencia. El tiempo máximo de duración de esta fase no debe superar las 12 horas una vez activado el PCO, salvo que por razones de fuerza mayor este período se amplíe por un tiempo adicional dispuesto por el Grupo de Comando, para lo cual se deberán ajustar los recursos y presupuesto según se requiera. Los pasos en esta fase son los siguientes:

a) Activación de PCO: Sede Alterna.

- El Líder del Grupo de Comando de la Gestión de la Continuidad Operativa recibe, a través del Formato: **"Evaluación de Daños"** - (Anexo 7), la información de los daños de la estructura, cuyo resultado ayudará a la toma de decisiones, a fin de activar el PCO y el traslado o no, a una sede alterna. De ser el caso, se elige la sede alterna y se dispone que se inicie el traslado.
- El responsable de Seguridad y Defensa Nacional, o el que haga sus veces en el PNACP, informará sobre el desplazamiento de las unidades orgánicas que deberán ser trasladadas a la sede alterna que se determine con el personal priorizado y el equipamiento mínimo identificado.
- Cada jefe de las unidades orgánicas considerados en el presente plan, debe activar los procedimientos de convocatoria de su personal, utilizando la mensajería idónea con la que se cuente.
- El Comité de Seguridad y Salud en el Trabajo establece los criterios y evalúa, a propuesta de las unidades orgánicas del PNACP, el riesgo de los funcionarios y servidores civiles que realizarían el trabajo presencial, en función de la

emergencia y su estado de salud. Asimismo, se debe considerar si el servidor civil propuesto está en condiciones de realizar dicha labor, evaluando sus condiciones personales y familiares, por ejemplo, el daño de su domicilio o, deceso de familiares, familiares heridos, situación emocional, entre otros.

5.9.2. FASE DE EJECUCION

Esta fase se realiza en simultáneo a la fase de activación, que la administración del PNACP requiere llevar a cabo, inmediatamente después de ocurrido el desastre, acciones que considera procurar el bienestar de los trabajadores, así como de previsión para el repliegue del personal hacia ambientes adecuados previamente seleccionados.

Se realiza en los siguientes pasos:

a) Acondicionamiento y puesta en operaciones de la Sede Alterna (de ser necesario).

- Tomada la decisión de traslado, se debe realizar las coordinaciones y acciones con la sede alterna que se determine, para que de inmediato se entreguen los ambientes y equipamiento necesario para la continuidad de operaciones del PNACP. Es pertinente indicar que los ambientes y equipos deben haber sido identificados con anterioridad, en previsión de la posibilidad de que ocurra el evento.
- El Grupo de Comando, en un plazo máximo de 12 horas de ocurrido el desastre, coordinará con la Sub Unidad de Abastecimiento y la Sub Unidad de Servicios Generales del PNAC para el traslado a la sede alterna elegida.

b) Implementación, gestión y coordinación inicial de Sede Alterna (de ser necesario). Estará a cargo de la Sub Unidad de Abastecimiento y la Sub Unidad de Servicios Generales, en base a los requerimientos ya establecidos.

c) Inicio de Operaciones en Sede Alterna

- En cuanto se tenga la confirmación de que la sede alterna se encuentra acondicionada, con instalaciones y equipamiento mínimo indispensable, con servicios que aseguren las comunicaciones y la operatividad, el personal priorizado se desplazará a la sede alterna.
- El inicio de operaciones en la sede alterna debe realizarse en el menor tiempo posible, una vez que se ha tomado la decisión del traslado.
- Los procesos críticos de los órganos y/o unidades orgánicas reubicados en la sede inician sus operaciones, priorizando la ejecución de sus actividades críticas.

d) Indicaciones para el personal que no se desplazará a la Sede Alterna (de ser necesario).

- Para el personal que no ha sido priorizado para el desplazamiento a la sede alterna, la Sub Unidad de Recursos Humanos dispondrá medidas y la información precisa a fin de conocer su ubicación y dictar disposiciones sobre la asistencia y permanencia.
- El personal será informado sobre la implementación de otras modalidades de prestación de servicios, tales como el trabajo no presencial (remoto o teletrabajo) o mixto, a fin de garantizar su seguridad.

e) Coordinaciones con otros Sectores e Instituciones

El Grupo de Comando y la UAF son responsables de establecer las comunicaciones necesarias con las instancias del Estado correspondientes, que incluye a INDECI, la municipalidad distrital correspondiente y otras entidades que conforman el SINAGERD, entre otros, a fin de informar sobre la continuidad de operaciones del PNACP y realizar las coordinaciones necesarias respecto a las disposiciones que el Estado emita para la emergencia, en coordinación con el COE PRODUCE.

f) Evaluación y atención de los Recursos Humanos

- Sub Unidad de Recursos Humanos debe elaborar el censo de todo el personal que labora en el PNACP, según lo acontecido una vez activado el PCO en la institución.
- La Unidad de Administración y Finanzas, y la Sub Unidad de Recursos Humanos, deben disponer de los mecanismos administrativos que permitan mitigar el impacto.

g) Evaluación detallada de la Sede Institucional afectada

- Trascurrido hasta un máximo de 12 horas posteriores a la emergencia, la Unidad de Administración y Finanzas, a través del Sub Unidad de Abastecimiento, debe disponer la concurrencia del personal, así como la presencia de un Especialista en infraestructura y de gestión de riesgo y desastres, o el que haga sus veces, para realizar una evaluación sobre la situación real de la infraestructura afectada. Esta actividad se podrá realizar en coordinación con la Municipalidad Distrital de San Isidro.
- Posteriormente a la evaluación definitiva de habitabilidad y operatividad que realice la Unidad de Administración y Finanzas, en coordinación con la Unidad de Planeamiento, Presupuesto y Modernización para la disponibilidad presupuestal que requiera, emitirá su informe señalando las conclusiones y recomendaciones a que hubiera lugar, en un plazo no mayor a 48 horas de ocurridos los hechos.

h) Acondicionamiento de ambientes temporales /definitivos

La Unidad de Administración y Finanzas debe asignar un equipo específico de personal dedicado a resolver las demandas para la implementación y acondicionamiento de los nuevos ambientes dispuestos para la continuidad de las operaciones del PNACP.

i) Adquisición de bienes/servicios para adecuación de infraestructura y equipamiento en sede temporal/definitiva.

Adicionalmente a las tareas de apoyo en las operaciones de emergencia, la Unidad de Administración y Finanzas deberá asignar un equipamiento necesario al personal dedicado a resolver las demandas de la implementación de los nuevos ambientes dispuestos para la operatividad del PNACP, para lo cual deberá analizar e identificar una lista base de insumos y recursos que se necesitaría en caso de una contingencia.

j) Ocupación de instalaciones temporales y repliegue

La Unidad de Administración y Finanzas debe informar a la Coordinación Ejecutiva y al Grupo de Comando la disponibilidad de los nuevos espacios asignados para ambientes de trabajo y coordinar el repliegue progresivo.

5.9.3. FASE DE DESACTIVACION

a) Desactivación de la ejecución del PCO.

Luego de culminar la fase de Ejecución y la emergencia haya sido superada, el Grupo de Comando para la gestión de la continuidad operativa, decide la culminación de la ejecución del Plan de Continuidad Operativa del PNACP, emitiendo un informe a la Coordinación Ejecutiva sobre las acciones y gestiones realizadas, adjuntando los documentos que sean pertinentes.

VI 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 a cada una de las actividades críticas. Para tal efecto, deberá utilizar la Matriz de Seguimiento y Monitoreo de la ejecución de las Actividades Críticas del Plan de Continuidad Operativa, utilizando como formato el Cuadro N° 19 del Plan de Continuidad Operativa.

Cuadro N°19: Matriz de Seguimiento y Monitoreo de la ejecución de las Actividades Críticas

Actividad Crítica	Responsable	Actividades desarrolladas	Personal Asignado	Mater ial asigna do	Equipo Asignado	Presupuesto Asignado	Fecha de actualización	Observaciones
Actividad Crítica N° 1: Articulación comercial de productos hidrobiológicos	UA	a.						
		b.						
		c.						

Actividad Crítica	Responsable	Actividades desarrolladas	Personal Asignado	Mater ial asigna do	Equipo Asignado	Presupuesto Asignado	Fecha de actualización	Observaciones
Actividad Crítica N° 2: Talleres de sensibilización en educación alimentaria	US	a.						
		b.						
		c.						

Actividad Crítica	Responsable	Actividades desarrolladas	Personal Asignado	Mater ial asigna do	Equipo Asignado	Presupuesto Asignado	Fecha de actualización	Observaciones
Actividad Crítica N° 3: Promoción de productos hidrobiológicos	UP	a.						
		b.						
		c.						

6.1 CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Dicimebre
1	**EJERCICIO DE ACTIVACIÓN DEL PCO (*)**	**2025**											
1.1	Pruebas del implementación del PCO: ante desastres naturales												
1.2	Pruebas del implementación del PCO: ante desastres no naturales												
1.3	Simulacro de sismo de gran magnitud, seguido de Tsunami												
1.4	Simulacro nacional multipeligro según normatividad vigente												
1.5	Reporte de Resultados de pruebas y/o simulacro												
2	**EJERCICIO DE ACTIVACIÓN DEL PCO (*)**	**2026**											
2.1	Pruebas del implementación del PCO: ante desastres naturales												
2.2	Pruebas del implementación del PCO: ante desastres no naturales												
2.3	Simulacro de sismo de gran magnitud, seguido de Tsunami												
2.4	Simulacro nacional multipeligro según normatividad vigente												
2.5	Reporte de Resultados de pruebas y/o simulacro												
3	**EJERCICIO DE ACTIVACIÓN DEL PCO (*)**	**2027**											
3.1	Pruebas del implementación del PCO: ante desastres naturales												
3.2	Pruebas del implementación del PCO: ante desastres no naturales												
3.3	Simulacro de sismo de gran magnitud, seguido de Tsunami												
3.4	Simulacro nacional multipeligro según normatividad vigente												
3.5	Reporte de Resultados de pruebas y/o simulacro												

NOTA: Las Pruebas de los Ejercicios se realizarán de manera inopinada en los meses indicados y/o de acuerdo a lo programado por INDECI.

VII ANEXOS

ANEXO N° 01: PAUTAS PARA LA GESTIÓN DOCUMENTAL DEL PNACP

Situación: Caída del Sistema Informático SITRADOC

Solución: Utilizar Correo Electrónico

1. Activación del Protocolo de Contingencia

- Notificación del incidente: La Sub-Unidad de Abastecimiento informará inmediatamente, vía correo electrónico, a la Coordinación Ejecutiva, a la Unidad de Administración y Finanzas, y a las Unidades sobre la caída del sistema.
- Correo oficial de contingencia: Se cuenta con el correo institucional:

  mesadepartesvirtual@acomerpescado.gob.pe.
- Comunicado interno: Se enviará un aviso, vía correo electrónico, a todo el personal con las instrucciones, indicando que la gestión documental será vía correo electrónico.

2. Gestión Documental Vía Correo Electrónico

- **Asunto Estandarizado:** Todo correo electrónico debe tener un formato de asunto, por ejemplo:

  [CONTINGENCIA] Nombre del documento - Fecha – Unidad o Sub-Unidad
- **Remisión de documentos:**
  - Los documentos deben enviarse en PDF debidamente suscritos, de corresponder.
  - Incluir en el cuerpo del mensaje: remitente, fecha, asunto, descripción breve del documento.
- **Recepción de documentos:**
  - La Sub- Unidad de Abastecimiento configurará los correos institucionales con la opción respuesta automática para que el remitente tome conocimiento que el correo remitido ha sido recibido por el receptor.
- **Registro de envío y recepción:**
  - Cada unidad o Sub-Unidad debe llevar un **registro manual o en una hoja Excel** con:
    - Fecha y hora de envío/recepción
    - Nombre del documento
    - Emisor/receptor
    - Código provisional (si aplica)
    - Observaciones

3. Custodia y Seguridad

- Archivos adjuntos: Guardar todos los documentos recibidos en carpetas organizadas en la nube o en el equipo local (ordenados por fecha, remitente, y tipo). **No deben borrarse los correos electrónicos emitidos o recibidos de la gestión documental.**
- Copias de respaldo: Realizar copia diaria en un disco externo o en una carpeta compartida de respaldo.

- Privacidad: Utilizar sólo correos institucionales (el personal) y correos personales (locación de servicios) y evitar reenvíos innecesarios.

4. Restauración del Sistema

- **Verificación del sistema:** Cuando el sistema Informático SITRADOC vuelva a estar operativo, la Sub-Unidad de Abastecimiento informará inmediatamente, vía correo electrónico, a la Coordinación Ejecutiva, la Unidad de Administración y Finanzas, y a las Unidades.
- **Reactivación del sistema oficial de gestión documental:** operatividad del Sistema Informático SITRADOC.

5. Transcripción y Actualización

- **Ingreso de documentos al sistema:** Toda gestión documental realizada vía correo electrónico deberá cargarse oficialmente en el sistema informático SITRADOC.
- **Referencia cruzada:** Incluir en el sistema una nota del tipo:

  "Documento recibido vía correo electrónico en contingencia - Fecha - Correo De origen".
- Archivo digital de respaldo: Conservar los correos electrónicos y documentos como respaldo por un tiempo definido o de corresponder, custodiarlos.

6. Informe y Mejora del Proceso

- **Informe del área:** Cada Unidad y Sub-Unidad deberá remitir a su Jefe inmediato, un reporte de los documentos gestionados por correo electrónico indicando tiempo de respuesta, de corresponder.
- **Análisis de respuesta:** Evaluar tiempos de respuesta, problemas detectados y posibles mejoras.

ANEXO N° 02: PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SALA DE SERVIDORES

1. INTRODUCCIÓN

La administración de continuidad de los servicios de TI se encarga de prevenir y proteger a la institución de los efectos que pudiera tener una interrupción de los servicios de TI ocasionados por una falla técnica, por causas naturales como terremotos, incendios, pandemia, entre otros o por alguna persona de manera voluntaria o involuntaria.

La administración de la continuidad de los servicios de TI debe combinar equilibradamente procedimientos y pautas como son:

- **Preventivos**, medidas y procedimientos que buscan eliminar o mitigar los riesgos de la interrupción y sus posibles efectos.
- **Reactivos**, procedimientos cuyo propósito es reanudar el servicio tan pronto como sea posible después de cualquier interrupción.

Estos procedimientos y pautas deben ser enmarcados en un Plan de Contingencia que la institución debe de elaborar para ser ejecutadas en cada uno de los eventos que alteren el normal funcionamiento de los servicios críticos. Además, debe detallar los alcances conceptuales que permitirán a la persona que accede a este documento reforzar y ampliar sus capacidades para que pueda familiarizarse con el plan de contingencia para ampliar sus habilidades de reacción ante las situaciones inesperadas que pueda ocasionar la paralización de las actividades en el ámbito de las TIC.

El Plan de Contingencia también puede considerarse como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencias.

El Estado Peruano a través de la Resolución Ministerial N° 028-2015-PCM, aprobó los Lineamientos para la Gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno, donde se señala que el Plan de Continuidad Operativa comprende, entre otros planes específicos, el Plan de Contingencia y el Plan Recuperación de Servicios de Tecnología de la Información. En ese sentido, el Programa Nacional “A Comer Pescado” presenta el Plan de Contingencias que permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos para minimizar el impacto negativo sobre la misma y sus colaboradores.

2. OBJETIVOS

2.1. Objetivo General

Contribuir a la continuidad operativa del PNACP, garantizando la operatividad de los servicios críticos de Tecnologías de Información que son necesarios en el PNACP para el cumplimiento de sus objetivos, ante eventos que puedan alterar el normal funcionamiento de la entidad.

2.2. Objetivos específicos

- Asegurar la pronta recuperación de los servicios críticos de TI después de cualquier evento o desastre que afecte la Continuidad de los Servicios de TI.

- Establecer políticas, tomar medidas y desarrollar procedimientos para evitar, dentro de lo posible, las consecuencias de cualquier desastre natural o eventos accidentales o voluntarios realizados por las personas.
- Proteger los activos informáticos del PNACP.
- Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.
- Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.

3. ALCANCE

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos de la sala de servidores referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos, personal, servicios y otros administrados por la Sub Unidad de Abastecimiento, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

4. BASE LEGAL

- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo N° 111-2012-PCM, que incorpora la Política Nacional de Gestión de Riesgos de Desastres de cumplimiento obligatorio para las entidades del Gobierno Nacional.
- 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 de Coordinación Ejecutiva N° 00009-2022-PNACP se constituye el Comité de Gobierno y Transformación Digital del PNACP, asimismo, se designa al Oficial de Seguridad y confianza digital.
- "Guía práctica para el desarrollo de Planes de Contingencia de Sistemas de Información" – Elaborado por INEI el 2001.

5. DEFINICIONES

a) **Activo de información:** Comprende a cada elemento que soporta la información, es decir que la contiene, la procesa y la transporta.

b) **Amenaza**: Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

c) **Incidente**: incidente es cualquier interrupción de servicios de Tecnología de la Información que afecta desde un solo usuario hasta la Institución.

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

e) **Impacto**: Es el daño producido por la materialización de una amenaza.

f) **Contingencia**: Se define como contingencia a la alteración en la continuidad del negocio, que impacta en forma relevante el normal desarrollo de un servicio considerado crítico, teniendo su origen en la falla de uno o varios componentes o la interrupción de una tarea, sin estar necesariamente prevista.

g) **Punto de Recuperación Objetivo (RPO)**: El objetivo del punto de recuperación (RPO) se utiliza como métrica para la recuperación de los datos. También se mide en términos de tiempo, pero hace referencia a la edad o a la frescura de los datos requeridos para restaurar la operación que sigue a un acontecimiento adverso. Los datos, en este contexto, pueden también incluir la información con respecto a las transacciones no registradas o no capturadas. Como el RTO, cuanto más pequeño es el RPO, más alto son los costos de la recuperación prevista de los datos.

h) **Plan de contingencia**: Es el proceso para desarrollar, comunicar y mantener documentados y aprobadas las acciones que permitan restituir rápidamente los servicios tecnológicos de la organización ante una eventualidad que pueda paralizar, ya sea de forma parcial o total de la Institución.

i) **Probabilidad**: Grado de ocurrencia de que algún evento o contingencia se materialice.

j) **Riesgo**: Incertidumbre que podría desencadenar una interrupción indeterminada en los servicios de TI.

k) **Riesgo Operativo**: Riesgo vinculado a la administración y supervisión del personal.

l) **Riesgo Técnico**: Riesgo vinculado a fallas en los suministros de energía y servicios complementarios.

m) **Riesgo Tecnológico**: Riesgo vinculado a los servicios de tecnologías de la información.

n) **Servicio crítico**: Servicio de gran valor para el cumplimiento de los objetivos del PNACP.

o) **Tiempo de inactividad o downtime**: El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible. Los casos de downtime pueden ser Planeado o No planeados.

p) **El Tiempo de Recuperación Objetivo (RTO):** Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Debe medirse desde el momento en que ocurre la interrupción hasta que se reanude la operación.

q) **MTD:** Se define como el Tiempo de inactividad máximo tolerable que define la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

r) **Tiempo de recuperación de la red**: Es el tiempo para restaurar la comunicación de datos y voz después de un evento adverso. Esto posiblemente tendrá impacto sobre otras actividades.

6. METODOLOGÍA DE DESARROLLO DEL PLAN DE CONTINUIDAD TECNOLÓGICA

La metodología de referencia utilizada es la BCM (Business Continuity Management), la cual nos permite definir y establecer el Plan de Contingencia para reducir el impacto provocado

por una paralización total o parcial de la operación de la Institución y garantizar así, la recuperación ágil y progresiva de los servicios tecnológicos y procesos críticos afectados.

La continuidad operativa del PNACP dependerá del evento y/o desastre sucedido y ante ello se debe asegurar los procesos y servicios tecnológicos críticos, según la estrategia desarrollada.

Para la elaboración del plan de contingencia tecnológico se han establecido las siguientes fases:

- **Fase 1: Planificación:**

  Se define y prepara los esfuerzos de planificación de las actividades en cada etapa de contingencia (Prevención, Ejecución y Recuperación).

- **Fase 2: Determinación de vulnerabilidades y escenarios de contingencia:**

  Se busca minimizar las fallas generadas por los eventos en contra del normal desempeño de los sistemas de información a partir del análisis de la criticidad de los eventos identificados.

- **Fase 3: Identificador de soluciones:**

  Para reducir los costos se han establecido soluciones en la medida de lo posible, a tiempo de documentar los riesgos de fallas e interrupciones identificadas.

- **Fase 4: Estrategias:**

  Se identifican las prioridades y se determina, en forma razonable, las actividades a ser implementadas en cada etapa desarrollada (Prevención, Ejecución y Recuperación).

- **Fase 5: Documentación del proceso:**

  Desarrollo de procedimientos y/o actividades en las etapas de prevención, ejecución y recuperación desarrolladas en cada evento.

- **Fase 6: Realización de pruebas:**

  Se identifican los escenarios y/o eventos con probabilidad de recuperación aceptable por la institución a través de actividades en cada etapa de recuperación.

- **Fase 7: Monitoreo:**

  Se establecen las actividades preventivas y mantenimiento que permita reaccionar en el tiempo preciso y se tomen las acciones correctas.

  La materialización de los riesgos contrae consecuencias para la Institución, para ello es necesario identificar, determinar y evaluar los niveles de impacto que puedan afectar la continuidad operativa de la sala de servidores del PNACP.

  El Plan de Contingencia determina los posibles riesgos e impactos en la Institución considerando las áreas de impacto: operacional, legal e imagen, tal como se muestra en el siguiente cuadro:

Cuadro N° 1: Cuadro de impactos de riesgos informáticos

Nivel de Impacto	Tipos de impacto		
	Operacional	Legal	Imagen
Leve	Paralización o trastornos en las actividades. El daño se revierte inmediatamente después de lo ocurrido	-	Percepción negativa de la imagen institucional por un número reducido de usuarios finales.
Moderado	Paralización o trastornos en las actividades. El daño se revierte en un tiempo menor o igual al RTO.	Amonestación administrativa	Percepción negativa de la imagen institucional por parte de las organizaciones políticas.
Alto	Paralización o trastornos en las actividades. El daño se revierte en un tiempo mayor al RTO.	Acciones judiciales, contenciosas, civiles	Percepción negativa de la imagen institucional por parte de las organizaciones políticas y las entidades públicas.
Severo	Paralización o trastornos en las actividades. El daño se revierte en un tiempo mayor al MTD.	Denuncias penales contra funcionarios del PNACP.	Pérdida de la confianza y la credibilidad de la institución por parte de la ciudadanía en general.

Elaboración: Sub Unidad de Abastecimiento del PNACP

6.1. Descripción de los Eventos de Contingencia

TIPO		EVENTO	DESCRIPCIÓN
EXTERNO	TECNOLÓGICO	Caída o interrupción de energía eléctrica (E1)	Corresponde al corte del servicio de energía en la sede central del PNACP sito en Calle Antequera 671, San Isidro, corte eléctrico que genera interrupción del funcionamiento de los servidores donde se alojan los sistemas de información y/o aplicaciones del PNACP. Esta situación impacta en la disponibilidad de los servicios de TI.
		Infección masiva por software malicioso (E3)	Es el riesgo de infección de los equipos de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de las unidades de trabajo.
		Ataque informático (E11)	Consiste en aprovechar alguna debilidad o falla en el software o hardware, para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.
	OPERATIVO	Suspensión de las actividades por sismo, inundación o incendio (E4)	Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo o incendio que afecte la infraestructura tecnológica de la Sala de Servidores del PNACP generando suspensión total o parcial de su funcionamiento o prestación de servicios de TI
	TÉCNICO	Caída de internet (E2)	Consiste en las fallas técnicas por parte del proveedor del servicio de internet en la sala de Servidores del PNACP, lo que ocasionaría suspensión de los servicios de TI incluyendo correo, red, sistemas y aplicativos de información del PNACP.

INTERNO	TECNOLÓGICO	Falla técnica en equipos servidores (E6)	Corresponde al daño físico o lógico de un equipo servidor, que afecta el funcionamiento de un sistema de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o inestable.
		Falla técnica en equipos de comunicación (E10)	Corresponde al daño físico o lógico de un equipo de comunicación, que afecta el funcionamiento de los servicios de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o inestable.
		Falla técnica en Sistemas de Información crítico (E7)	Representa una falla técnica en alguna funcionalidad de los sistemas de información y aplicativos críticos del PNACP que se vea afectada la integridad de la información en el continuo uso de estos.
	OPERATIVO	Accesos no autorizados al Centro de Datos del PNACP – (E5)	Consiste en el acceso a la sala de servidores del PNACP de personal no autorizadas que pueden ocasionar sabotaje, robo, alteración o extracción de información que es considerada confidencial o clasificada, así como también el daño a los componentes informáticos. El impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional.
		Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes – (E8)	Corresponde a la falta o inasistencia en un momento dado, de un trabajador crítico de la Sub Unidad de Abastecimiento que realiza actividades de soporte a usuarios sobre un sistema de información crítico del PNACP por enfermedad, epidemia muerte o incapacidad, lo que genera inoperancia o inestabilidad de los sistemas de información, servidores y redes
	TÉCNICO	Calentamiento del centro de datos – (E9)	Consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos.

Elaboración: Sub Unidad de Abastecimiento del PNACP

6.2. Descripción de los Eventos de Contingencia

Para la valoración de los eventos identificados, se utiliza la matriz del Cuadro N° 1, donde se categorizan los niveles de probabilidad y niveles de impacto (consecuencias). La descripción de cada categoría se muestra a continuación:

Niveles de probabilidad

- Casi Seguro: probabilidad muy alta.
- Muy probable: probabilidad alta.
- Posible: probabilidad media.
- Poco probable: probabilidad baja.
- Raro: sería especialmente que ocurriera raramente.

Niveles de impacto (consecuencias)

- Catastrófico: pérdida de negocio o posibilidad de pérdida de vidas o lesiones graves.
- Mayor: afección grave al negocio, posibilidad de lesiones moderadas.
- Moderado: causarán problemas no significativos en el negocio, posibilidad de lesiones leves.
- Menor: muy poca influencia sobre el negocio, impacto leve.
- Despreciable: prácticamente ninguna influencia negativa sobre el negocio, pueden dejarse sin mediar.

Figura N° 1: Mapa de Calor de Riesgos (Fuente: Gestión de riesgos ISO 31000)

La valoración de los riesgos tiene 4 posibles resultados: bajo, medio, alto y muy alto. Para efectos de la formulación del presente plan de contingencia, se tomarán en cuenta los riesgos valorados como alto y muy alto. Los riesgos con valoración bajo y medio se deben mantener en lista de observación a fin de que de manera periódica se pueda evaluar si en el tiempo va cambiando dicha valoración.

En función a ello, los eventos de contingencia descritos en el numeral 6.1 precedente, tienen la siguiente valoración:

Tabla N°: 01

N°	EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN
E1	Caída o interrupción de energía eléctrica.	Poco probable	Catastrófico	ALTO
E2	Caída de internet.	Poco probable	Mayor	ALTO
E3	Infección masiva por software malicioso.	Muy probable	Mayor	ALTO
E4	Suspensión de las actividades por sismo,	Poco probable	Catastrófico	ALTO

	inundación o incendio.			
E5	Accesos no autorizados a la Sala de Servidores	Poco probable	Mayor	MEDIO
E5	Falla técnica en equipos servidores, de escritorio o de Comunicaciones.	Posible	Mayor	ALTO
E6	Falla técnica en los Sistemas de Información crítico.	Muy probable	Mayor	ALTO
E7	Ausencia de personal de la Sub-Unidad de Abastecimiento que brindan soporte y mantenimiento a los a los sistemas de información y comunicaciones.	Muy probable	Moderado	ALTO
E8	Calentamiento de la sala de servidores.	Posible	Mayor	ALTO
E09	Falla técnica en los equipos de comunicación.	Posible	Mayor	ALTO
E10	Ataque informático	Muy probable	Mayor	ALTO

7. RESULTADOS ESPERADOS

El presente Plan de Contingencia de TI buscar restablecer los servicios de TI en un margen aceptable a cada tipo de servicio que pueden ir desde 50% hasta 100% dependiendo del tipo de servicio impactado.

8. ESTRATEGIAS

8.1. Desarrollo de la estrategia para los Planes de Contingencia

Desarrollaremos las estrategias relacionadas con cada evento o incidente que provoque alto impacto en la continuidad de los servicios de TI de la Sub Unidad de Abastecimiento. Para lo cual se está dividiendo en 3 partes:

a) **Prevención**: Mecanismos para prevenir dichos eventos antes de que sucedan; ayudan a reducir el impacto y estar siempre preparados ante eventualidades de desastres.

b) **Ejecución**: Después de iniciado el evento y ayuda a la recuperación de las funciones críticas, se considera los tiempos de continuidad.

c) **Recuperación**: Procedimientos para retomar las actividades ya recuperadas en su lugar de origen.

8.2. Estrategia del Plan de Contingencia para cada evento

8.2.1. Evento N°01: Caída o interrupción de energía eléctrica - (E1)

Evento: Caída o interrupción de energía eléctrica - (E1)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Falla general del suministro de energía eléctrica por parte del proveedor de servicio. Este evento incluye los siguientes elementos mínimos identificados por el PNACP, 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 - Estaciones de Trabajo - Equipos Diversos - UPS
1.2. Objetivo
Restablecer energía eléctrica en la Sala de Servidores del PNACP ante un evento de contingencia para asegurar la continuidad operativa de los sistemas críticos de TI.
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Se delimita a la Sala de Servidores ubicado de la sede Central del PNACP
1.5. Personal encargado
● Sub Jefe de la Sub Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
● Verificar que durante las operaciones diarias de servicio u operaciones del PNACP se contará con los UPS necesarios para asegurar el suministro eléctrico en la de Servidores del PNACP. ● Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 45 minutos como mínimo. ● Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Corte de suministro de energía en la sala de servidores del PNACP por un tiempo mayor a 30 minutos.
2.2 Procesos relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones de la sede principal del PNACP.
2.3. Personal que autoriza la Contingencia
● Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado
● Especialista Informático
2.5. Descripción de los procedimientos después de activar la contingencia:

- Informar a la Jefatura de la Sub-Unidad de Abastecimiento sobre el evento presentado.
- Verificar la activación automática de los UPS.
- Comunicar a todas las Unidades del PNACP del evento y coordinar las acciones necesarias.
- En caso la interrupción de energía sea mayor a 30 minutos se deberá apagar los servidores (Virtuales y físicos) que alojen los sistemas, aplicaciones, servicios de TI y demás servidores en siguiente orden:
    - Servidores de aplicación, Base de datos, servicios TI, otros, servicio de Directorio Activo y finalmente los servidores físicos (Hypervisores)
- Apagar los servicios, los equipos de seguridad perimetral y comunicaciones. Monitorear el uso de equipos UPS para el restablecimiento de energía en los servidores de soporte a los sistemas críticos.
- Coordinar con las Unidades afectadas de tomar las medidas necesarias ante la activación del Plan de Contingencia de TI.

3. PLAN DE RECUPERACIÓN

3.1. Personal operativo encargado

- Especialista Informático o quien haga sus veces.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Verificar el estado de la infraestructura tecnológica impactada por el evento.
- Verifica el restablecimiento de la energía eléctrica y el funcionamiento de la Sala de Servidores.
- En caso de que se cuente con energía eléctrica, se procederá a la activación de los servicios en la siguiente secuencia:
    - Encendido de los equipos de comunicaciones.
    - Encendido de los servidores físicos (Hypervisores).
    - Encender servidores de Directorio Activo, Base de datos, Aplicaciones, otros.
- Analizar la necesidad de usar las copias de respaldo y backup.
- Verificar el restablecimiento de los sistemas críticos de información.
- Comunicar a las Unidades afectadas el restablecimiento de los sistemas de información críticos.
- Registrar aquellas actividades que sirva para actualizar el Plan de Contingencia de TI en caso vuelva a presentarse dicha eventualidad.
- Registrar el evento en el Formato Registro de Contingencias

3.3. Mecanismo de comprobación

- Verificar a través del software de Monitoreo que todos los servicios estén activos.
- Comunicar a todas las Unidades del PNACP a fin de constatar el correcto funcionamiento de los sistemas de información críticos en cada área de trabajo.
- Garantizar la funcionalidad de las instalaciones eléctricas en la Sede Central del PNACP.

3.4. Desactivación del Plan de Contingencia de TI

El/la Sub Jefe de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez se haya restablecido la energía eléctrica a la sala de servidores y los servicios de TI.

3.5. Informe de resultados

Elaborar un informe a la Jefatura de la Sub-Unidad de Abastecimiento sobre el problema presentado y el procedimiento usado para atender el evento.

3.6. Proceso de actualización del Plan

Se tomarán las recomendaciones formuladas en los informes presentados a la Jefatura de la Sub Unidad de Abastecimiento para la presente contingencia.

3.7. Tiempo de Recuperación

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

8.2.2. Evento N°02: Caída de Internet - (E2)

Evento: Caída de Internet – (E2)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Perdida de servicio de Internet a la conexión de la red externa del servicio principal del PNACP.
1.2. Objetivo
Restaurar los servicios críticos de comunicaciones a la red externa que soportan los servidores de la sala de servidores a través del Servicio de Internet de Contingencia.
1.3. Valoración
Restaurar los servicios críticos de comunicaciones a la red externa que soportan los servidores de la sala de servidores del Servicio de Internet de Contingencia.
1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en la sala de servidores del PNACP.
1.5. Personal encargado
● Sub Jefe de la Sub Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
● Contar con equipos de comunicación y respaldo ante posibles fallas del router principal, a través del contrato con el proveedor del servicio de Internet se contempla el reemplazo del router en caso falle. ● Contar con mantenimiento preventivo para los equipos de comunicaciones dos veces al año. (Equipo alquilado) y otro mantenimiento programado por el proveedor en su nodo de comunicaciones. ● Libreta de números de contacto del proveedor al alcance.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia.
● Falla del sistema de router principal para el servicio de Internet ● Falla de los circuitos digitales de comunicación de red externa. (Ej.Rotura de enlace de fibra u otros medios) ● Falla del nodo de comunicación del proveedor de internet del PNACP.
2.2. Procesos relacionados antes del evento.
Cualquier actividad de servicio dentro de las instalaciones del PNACP.
2.3. Personal que autoriza la Contingencia.
Sub Jefe de la Sub-Unidad de Abastecimiento
3. PLAN DE RECUPERACIÓN
3.1. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
3.2. Descripción de actividades
● Validar que los servicios y circuitos estén conforme por las áreas usuarias. ● El proveedor del servicio de Internet una vez reparado el fallo emitirá un informe a la Jefatura de la Sub-Unidad de Abastecimiento, detallando la causa origen del evento y las acciones realizadas. ● El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos. ● Se informará a la Jefatura de la Sub-Unidad de Abastecimiento sobre el evento de contingencia presentado y el procedimiento usado.
3.3. Mecanismos de comprobación
La Sub-Unidad de Abastecimiento deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones y circuitos de la red externa (Internet), los cuales se lleven a cabo semestralmente.
3.4. Desactivación del Plan de Contingencia

La Jefatura de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.
3.5. Proceso de actualización
En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red externa (Internet), se tomarán las acciones correctivas para la actualización del Plan de Contingencia.
3.6. Tiempo de Recuperación
Falla del Router: El reemplazo por el proveedor no debe exceder a 1 hora. Falla de Circuito digital: El tiempo del SLA establecido con el proveedor es 4 horas.

8.2.3. Evento N°03: Infección masiva por software malicioso - (E3)

Evento: Infección masiva por software malicioso - (E3)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Los softwares maliciosos son programas informáticos que se propagan de un equipo a otro y que interfieren en su correcto funcionamiento. Además, pueden dañar o eliminar los datos de un equipo. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación: ● Servidores ● Estaciones de trabajo (PC y Laptops) ● Software base datos. ● Aplicativos y sistemas de información del PNACP.
1.2. Objetivo
Restaurar la operatividad de los activos informáticos después de eliminar el software malicioso que causa la contingencia.
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Los activos informáticos (PC, Laptops, servidores y sistemas de información) de la Sede Central del PNACP.
1.5. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de prevención de riesgos
● Establecer políticas y normativas de seguridad que regulen el uso adecuado de los activos de información. ● Utilizar mecanismos de seguridad que restrinja el acceso a páginas de internet de contenido malicioso. ● Restringir el acceso a las grabadoras de CD y USB en las estaciones de trabajo que no lo requieran. ● Aplicar filtros para restricción de correo entrante y así prevenir la infección de los terminales de trabajo por virus.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Mensajes de error o mensajes de alerta durante la ejecución de los sistemas de información y aplicaciones. ● Lentitud o paralización de los sistemas de información y aplicaciones. ● Falla general en los activos de informáticos (PC, Laptops, servidores y sistemas de información). ● Reporte de usuarios.
2.2. Procesos relacionados antes del evento
Cualquier proceso relacionado con el uso de sistemas y aplicaciones en las. estaciones de trabajo y servidores
2.3. Personal que autoriza la Contingencia
Sub Jefe de la Sub-Unidad de Abastecimiento
2.4 Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
2.5. Descripción de actividades

- Comunicar o escalar al Sub Jefe de la Sub-Unidad de Abastecimiento para activar al equipo de respuesta de incidentes.
- Desconectar preventivamente los equipos infectados de la red del PNACP.
- Comunicar a los usuarios de los servicios de los equipos impactados.
- Verificar el estado actualizado de las firmas del software antivirus, IPS, Antimalware Verificar la infección de los equipos afectados y el alcance de este.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.) para su remisión y revisión por el fabricante de la solución antivirus y antimalware.
- Eliminar el agente viral causante de la infección.
- Escanear la red del PNACP en virtud de eliminar posibles agentes virales informáticos.
  - Formatear el equipo
  - Personalizar la estación para el usuario.
  - Conectar las estaciones o equipo servidor a la red del PNACP.
  - Efectuar las pruebas necesarias con el usuario.
  - Solicitar conformidad del servicio.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Sub Jefe de la Sub Unidad de Abastecimiento
- Especialista Informático

3.2. Descripción de actividades

- Registrar la conformidad del usuario una vez se haya eliminado la amenaza de virus en su estación de trabajo.
- Realizar pruebas de funcionamiento en las estaciones de trabajo (Sistemas de información, servicios tecnológicos y aplicaciones del PNACP).
- Coordinar con el usuario responsable el procedimiento para reanudar las labores normales en el ambiente de trabajo original.
- Dar indicaciones de seguridad y prevención a los usuarios.
- Realizar informe de las acciones tomadas durante el evento.
- Se informará a la Jefatura de la Sub-Unidad de Abastecimiento el tipo de software malicioso encontrado y el procedimiento usado para removerlo. En función a esto, se tomarán las medidas preventivas del caso.
- El evento será evaluado y registrado en el formato de registro de contingencia.

3.3. Mecanismo de comprobación

- Asegurar que el antivirus funcione correctamente y se encuentre en constante actualización.
- Verificar que el Sistema Operativo se encuentre con las actualizaciones y parches.

3.4. Desactivación del plan de continuidad

- El Sub Jefe de la Sub-Unidad de Abastecimiento desactivará el presente Plan una vez se haya eliminado la amenaza.

3.5. Proceso de actualización

- En base al informe presentado que identifica las causas de la infección de virus informático, se determinará las acciones preventivas necesarias que deberán incluirse en el presente Plan.

3.6. Tiempo de Recuperación

- La duración del evento dependerá de la eficacia en detección de infección masiva, por efecto de actualización de firmas no mayor a 24 horas, así como también el tiempo de respuesta de los fabricantes en caso infecciones de día cero.
- Los usuarios deberán esperar las indicaciones del personal de soporte para reanudar el trabajo

8.2.4. Evento N°04: Suspensión de actividades por sismo, inundación o incendio – (E4)

Evento: Suspensión de las actividades por, inundación o incendio – (E4)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Constituye la situación en la que la sala de servidores se encuentra declarada inhabitable, producto de un desastre de mayores magnitudes, pudiendo provocar derrumbe de la infraestructura, perdida de materiales, recursos informáticos y humanos. Las causas que pueden provocar este evento encontramos las siguientes: **Incendio**: Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros. **Sismo de gran intensidad en Lima**: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento errático del terreno. **Inundación**: Flujo descontrolado de agua producto de lluvias torrenciales o fugas y/o daños en el sistema hidráulico.
1.2. Objetivo
Establecer las acciones que se tomarán ante un incendio, inundación o sismo de grandes magnitudes a fin de minimizar el tiempo de interrupción de los servicios críticos de TI, establecidos en el numeral 6.1 cuadro de valoración de Alto y Muy Alto
1.3. Valoración
Este evento es considerado como alto.
1.4. Entorno
Este evento se localiza en las instalaciones de la sala de servidore del PNACP.
1.5. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de prevención de riesgos
Incendio de grandes magnitudes en uno o más ambientes: ● Realizar inspecciones de seguridad periódicamente. ● Mantener las conexiones eléctricas seguras en el rango de su vida útil. ● Asistir a charlas sobre el uso y manejo de extintores de cada uno de los tipos. ● Acatar las indicaciones de Defensa Civil, en torno al evento. ● Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal responsable de las acciones de prevención y ejecución de la contingencia. ● Verificar el funcionamiento de los detectores de humo en la sala de Servidores del PNACP. ● Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia. ● Conocer el grupo de brigadistas asignados por el PNACP. ● Identificar la ubicación de las estaciones manuales de alarma contra incendio. ● Sismo de gran intensidad en Lima ● Solicitar el plan de evacuación de las instalaciones del PNACP, el mismo que debe ser de conocimiento de todo el personal que labora. ● Participar en los simulacros de evacuación con la participación de todo el personal del PNACP.

8.2.5. Evento N°05: Acceso no autorizados a la sala de servidores– (E5)

Falla técnica en servidores (E5)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Ingreso a la sala de servidores de personal no autorizado, personal interno o externo.
1.2. Objetivo
Asegurar la seguridad de personal no autorizado
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Vulnerabilidad física de los equipos ubicados dentro de la sala de servidores del PNACP
1.5. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
● Revisión periódica física del ambiente
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Indisponibilidad de los sistemas de información
2.2. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
2.3. Descripción de los procedimientos después de activar la contingencia:
● Analizar la causa resultante o disparador del evento. ● Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del PNACP. ● Contactar a las partes interesadas que sean afectadas por la indisponibilidad de los servicios de TI.
3. PLAN DE RECUPERACIÓN
3.1. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
3.2. Descripción de actividades
● Conectar a la red el equipo ● Verificar el acceso a las unidades de red
3.3. Mecanismos de Comprobación
● Verificación física de la puerta de ingreso y servidores físicos
3.4. Desactivación del Plan de Contingencia
● El Sub Jefe de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que los servicios se encuentren restablecidos.
3.6 Tiempo de Recuperación Duración de 2-6 horas.

8.2.6. Evento N°06: Falla técnica en servidores – (E6)

Evento: Falla técnica en servidores – (E6
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Falla técnica de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del PNACP.
1.2. Objetivo
Asegurar la continuidad y operatividad de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del PNACP.
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en la sala de servidores del PNACP
1.5. Personal encargado
● Oficial de seguridad de la información ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
• Revisión periódica técnica de los servidores. • Mantener actualizada la garantía de equipos y servidores vigentes. • Copias de seguridad de los sistemas de información y aplicaciones del PNACP. • Monitoreo periódico de red del PNACP. • Seguridad periférica. • Protección física adecuada a la sala de servidores • Mecanismos de seguridad y controles de acceso. • Adecuada ventilación y refrigeración en la sala de servidores • Procedimientos para el uso correctos de los activos de información.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Falla del sistema de aire acondicionado de la sala de servidores ● Fallas en la conexión, servidores no responden. ● Falla de los servicios críticos del PNACP
2.2. Procesos relacionados antes del evento
● Cualquier actividad de servicio dentro de las instalaciones del PNACP.
2.3. Personal que autoriza la Contingencia
● Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado
● Especialista Informático
2.5 Descripción de los procedimientos después de activar la contingencia:
● Analizar la causa resultante o disparador del evento. ● Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del PNACP. ● Contactar a las partes interesadas que sean afectadas por la indisponibilidad de los servicios de TI. ● Comunicar a los proveedores del equipo servidor e informar la incidencia como parte del soporte y garantía. ● Desconectar de la red el servidor afectado. ● Activar y configurar el equipo necesario de contingencia para el levantamiento de los servicios de TI en los servidores alternos de contingencia. ● Ejecutar las restauraciones de los backup de los sistemas y aplicaciones críticos en los servidores alternos de contingencia en caso se requiera.
3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
● Especialista Informático
3.2. Descripción de actividades
● Conectar a la red el equipo inicial reparado. ● El Especialista Informático verifica el correcto desempeño de los servidores reparados y de los sistemas de información críticos que soportan. ● Se informará a la Sub-Unidad de Abastecimiento de la Información la causa del problema presentado y el procedimiento usado para atender el problema. En función a esto, se tomarán las medidas preventivas del caso. ● El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
3.3. Mecanismos de comprobación
● La Sub-Unidad de Abastecimiento deberá asegurarse que las pruebas y revisiones periódicas al sistema de ventilación de la sala de servidores se lleven a cabo semestralmente.
3.4. Desactivación del Plan de Contingencia
● La Jefatura de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.
3.5. Proceso de actualización
● En base al informe presentado por el proveedor del sistema de ventilación de la sala de servidores se tomarán las acciones correctivas para la actualización del Plan de Contingencia.
3.6. Tiempo de Recuperación
● El tiempo máximo de duración de la contingencia dependerá del proveedor del sistema del aire acondicionado, se estima un tiempo máximo de 4 a 8 horas.

8.2.7. Evento N°07: Falla técnica en Sistemas de Información Critico – (E7)

Evento: Falla en Sistemas de Información Críticos – (E7)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Es el uso defectuoso de los sistemas de información críticos del PNACP, haciendo que el uso de estos corresponda a un elevado riesgo en la integridad de la información que se procese o simplemente este último deje de funcionar.
1.2. Objetivo
Restaurar el funcionamiento de los sistemas de información y aplicaciones críticos del PNACP de acuerdo con el numeral 6.1 cuadro de valoración de Alto y Muy Alto.
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Sistemas de información y aplicativos críticos del PNACP.
1.5. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
● Copia de seguridad de la información críticos para asegurar la integridad de la información. ● También se obtienen copias de seguridad de la base de datos relacionadas. ● Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante y licencias vigentes. ● Evitar el uso de software no licenciado que pueda estar corrupto ● Revisión preventiva de los sistemas y mantenimiento general de las bases de datos. ● Directivas o procedimiento de desarrollo seguro. ● Implementar y mantener un repositorio de código fuente institucional.

2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Fallas en el uso de los sistemas de información que generen su inoperatividad. ● Información procesada no cuenta con integridad y fiabilidad.
2.2. Procesos relacionados antes del evento
● Respaldo disponible de los sistemas de información críticos.
2.3. Personal que autoriza la Contingencia
● Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado
● Personal de desarrollo de sistemas o quien haga sus veces. Administrador de base de datos o quien haga sus veces.
2.5. Descripción de las actividades después de activar la contingencia:
● Desconectar de la red el equipo afectado. ● Configurar equipo de respaldo para el sistema de información o aplicación crítica afectada. ● Restaurar la copia de seguridad más reciente del aplicativo crítico correspondiente. ● Crear los permisos a cada carpeta compartida. ● Verificar la existencia del servidor nuevo en el dominio y colocarlo en producción. ● Informar a los usuarios la nueva ruta del servidor del aplicativo
3. PLAN DE RECUPERACIÓN
3.1. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Especialista Informático
3.2. Descripción de actividades
● Revisar el sistema de Información o aplicativo dañado para determinarla falla o error lógico presentado. ● Hacer pruebas al sistema de Información o aplicativo una vez entregada la solución por el proveedor, en ambiente de pruebas. ● Realizar copia de la base de datos del sistema de Información o aplicativo que está en funcionamiento como contingencia. ● Restaurar la copia de seguridad más reciente del aplicativo afectado en el servidor inicial. ● Verificar los permisos sobre el sistema de información o aplicativo. ● Informar a los usuarios la ruta del servidor del sistema de información o aplicativo. ● Conectar a la red el equipo inicial reparado.
3.3. Mecanismos de comprobación
● El Especialista Informático presentará un informe a la Jefatura de la Sub Unidad de Abastecimiento explicando que servicio ha sido afectado y cual son las acciones tomadas.
3.4. Desactivación del Plan de Contingencia
● La Jefatura de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.
3.5. Proceso de actualización
● En base al informe presentado a la Sub-Unidad de Abastecimiento y las causas identificadas en el servicio informático se determinará las acciones a tomar.
3.6. Tiempo de Recuperación
● El tiempo máximo de duración de la contingencia será máximo en 24 horas dependiendo de la causa que originó la contingencia.

8.2.8. Evento N°08: Ausencia de personal de la Sub-Unidad de Abastecimiento que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)

Evento: Ausencia de personal de la Sub Unidad de Abastecimiento que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Ausencias del personal (enfermedad, epidemias, renuncias masivas, ceses), critico que brinda soporte y mantenimiento a los sistemas de información, servidores y redes que mediante su ausencia pueda originar paralización en las operaciones del PNACP.
1.2. Objetivo
● Reemplazar al personal crítico ausente con elementos capacitados que puedan cubrir sus funciones hasta la inserción o reemplazo del ausente.
1.3. Valoración
Este evento es considerado Alto.
1.4. Entorno
Oficina de Tecnologías de la Información.
1.5. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Oficial de seguridad de la información.
1.6. Condiciones de Prevención de Riesgo
● Asegurar la capacitación adecuada de los equipos técnicos en su especialidad, Analistas de sistemas, redes, infraestructura y Seguridad Informática y Administración de BD con el fin de que cumplan con el perfil, conocimiento y capacidad de reemplazar la ausencia de los especialistas en caso de ausencia. ● Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labor. ● Elaborar diccionarios de datos y/o manuales o procedimientos operativos de uso para facilitar las actividades del reemplazante. ● Programar chequeos preventivos médicos al personal crítico en periodos semestrales o anuales. ● Mantener operativas las herramientas de trabajo remoto.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
Inasistencia no premeditada del personal crítico.
2.2. Procesos relacionados antes del evento
La Jefatura de la Sub-Unidad de Abastecimiento tiene conocimiento de inasistencia del personal crítico.
2.3. Personal que autoriza la Contingencia
Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado
● Sub Jefe de la Sub-Unidad de Abastecimiento ● Oficial de seguridad de la información.
2.5. Descripción de las actividades después de activar la contingencia:
● Confirmada la inasistencia del personal, la Sub-Unidad de Abastecimiento de la Información asignará al reemplazo provisional del personal ausente. ● Poner a disposición los recursos necesarios para que el personal suplente lleve a cabo sus actividades efectivamente.
3. PLAN DE RECUPERACIÓN
3.1. Personal encargado

Sub Jefe de la Sub-Unidad de Abastecimiento
3.2. Descripción de actividades
● Facilitar la reinserción del personal ausente ● Regularización en los servicios pendiente durante la ausencia. ● Revisión de los servicios atendidos si fuera el caso. ● Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.
3.3. Mecanismos de comprobación
Informes de desempeño laboral, de corresponder, cuando sea requerido por la Sub Unidad de Abastecimiento
3.4. Desactivación del Plan de Contingencia
La Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.
3.5. Proceso de actualización
En base al informe presentado a la Sub-Unidad de Abastecimiento y las causas identificadas en el Servicio informático se determinará las acciones a tomar.
3.6. Tiempo de Recuperación
El tiempo máximo de duración de la contingencia dependerá de la causa que originó la ausencia temporal, sin embargo, se dispondrá de un reemplazo temporal en un plazo máximo de 24 horas.

8.2.9. Evento N°09: Calentamiento de la sala de servidores – (E9)

Evento: Calentamiento de la sala de servidores– (E9)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Aumento de temperatura dentro de la sala de servidores y falta de sistema de aire acondicionado, en la sala de servidores de PNACP o ausencia de un sistema de ventilación acorde a las necesidades del PNACP.
1.2. Objetivo
Restaurar los servicios críticos de TI que soportan los servidores de la sala de servidores del PNACP
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en la sala de servidores del PNACP
1.5. Personal encargado
● Oficial de seguridad de la información ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo
● Contar con equipos de respaldo ante posibles fallas de los servidores ● Contar con un sistema de aire acondicionado adecuado en la sala de servidores ● Contar con mantenimiento preventivo para los equipos de aire acondicionado ● Libreta de números de contacto del proveedor al alcance
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
● Falla del sistema de aire acondicionado de la sala de servidores ● Falla de los servicios críticos del PNACP
2.2. Procesos relacionados antes del evento
● Cualquier actividad de servicio dentro de las instalaciones del PNACP.
2.3. Personal que autoriza la Contingencia
● Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado

● Especialista Informático
2.5 Descripción de los procedimientos después de activar la contingencia:
● Verificar la magnitud del fallo o avería al sistema de ventilación de la sala de servidores. ● Notificar al proveedor de aire acondicionado sobre la magnitud de fallos o averías. ● Encender el aire acondicionado de contingencia. ● Instalar equipos de ventilación provisionales. ● Apagar los equipos electrónicos no críticos. ● Restablecer el sistema de aire acondicionado de la sala de servidores
3. PLAN DE RECUPERACIÓN
3.1. Personal encargado
● Especialista Informático
3.2. Descripción de actividades
● El especialista informático revisará que el sistema de Aire Acondicionado haya sido reparado y funcione con normalidad. ● Encender equipos no críticos ● El proveedor del sistema de aire acondicionado una vez reparado el fallo emitirá un informe a la Jefatura de la Sub-Unidad de Abastecimiento, detallando la causa origen del evento y las acciones realizadas. ● El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos. ● Se informará a la Sub-Unidad de Abastecimiento sobre el evento de contingencia presentado y el procedimiento usado.
3.3. Mecanismos de comprobación
● La Sub-Unidad de Abastecimiento deberá asegurarse que las pruebas y revisiones periódicas al sistema de ventilación de la sala de servidores se lleven a cabo semestralmente.
3.4. Desactivación del Plan de Contingencia
● La Jefatura de la Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.
3.5. Proceso de actualización
● En base al informe presentado por el proveedor del sistema de ventilación de la sala de servidores se tomarán las acciones correctivas para la actualización del Plan de Contingencia.
3.6. Tiempo de Recuperación
● El tiempo máximo de duración de la contingencia dependerá del proveedor del sistema del aire acondicionado, se estima un tiempo máximo de 2 horas.

8.2.10. Evento: Falla técnica de equipos de Comunicación – (E10)

Evento: Falla técnica de equipos de Comunicación – (E10)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Caída de los equipos de comunicación (Switches) o fallas en los enlaces de fibra en la sede principal
1.2. Objetivo
Restaurar los servicios críticos de comunicaciones de la red interna que soportan los Sistemas del PNACP.
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en la sala de servidores del PNACP
1.5. Personal encargado
● Oficial de seguridad de la información. ● Especialista Informático
1.6. Condiciones de Prevención de Riesgo

- Contar con equipo en configuración redundante y alta disponibilidad.
- Contar con equipos de Switches de respaldo ante posibles fallas de los equipos de comunicación.
- Enlaces redundantes entre equipos de comunicación a nivel de Switch Core
- Los Switches de distribución también estarían en configuración redundante.
- Los Switches de acceso que conecta a las PCs, se cuenta con equipos de respaldo.
- Contar con mantenimiento preventivo para los equipos de comunicación (Switch Core y Distribución).
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Falla del Switchs Core, Distribución y acceso a las PC
- Falla de los enlaces de cobre o fibra en la red interna.

2.2. Procesos relacionados antes del evento

- Cualquier actividad de servicio dentro de las instalaciones del PNACP.

2.3. Personal que autoriza la Contingencia

- Sub Jefe de la Sub-Unidad de Abastecimiento del PNACP.

2.4. Personal encargado

- Especialista Informático o quien haga sus veces

2.5. Descripción de los procedimientos después de activar la contingencia:

- Validación física de la caída de red y dimensionar el alcance del impacto (Usuarios y pisos afectados)
- Si se trata un Switch de acceso se reemplaza en caso esté en garantía, caso contrario se envía a reparación el equipo de comunicación que presenta fallas.
- Se valida el estado de los servicios por usuarios y pisos afectado.
- Si trata de fallas en los enlaces, se verifica con la herramienta de monitoreo los estados y alertas reportadas.
- Se realiza una validación física de las conexiones de fibra (Cuarto de comunicaciones), si implica algún cambio se notifica al proveedor.
- El proveedor realiza un diagnóstico para detectar falla y proceder con su reparación. Se valida que los servicios en la herramienta de monitoreo estén activos para los usuarios y pisos afectados.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista informático

3.2. Descripción de actividades

- Validar que los equipos de comunicación y enlace de la red interna estén activos para las áreas usuarias.
- El proveedor de los equipos de comunicaciones una vez reparado el fallo emitirá un informe a la Sub-Unidad de Abastecimiento, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Sub Unidad de Abastecimiento sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La Sub-Unidad de Abastecimiento deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones de la red interna se lleven a cabo semestralmente (Equipos en garantía).

3.4. Desactivación del Plan de Contingencia

La Sub-Unidad de Abastecimiento desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red interna se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación

- Falla de switches Core y Distribución, el tiempo máximo de reemplazo por el proveedor será de 1 hora.
- Switchs de accesos PC máx. 1 hora.
- En caso falla de enlace digital dependerá de los SLAs del proveedor, se estima máximos 24 horas.

8.2.11. Evento: Ataque Informático – (E11)

Evento: Ataque Informático – (E11)
1. PLAN DE PREVENCIÓN
1.1. Descripción del evento
Afectación por parte de algún sistema informático de un tipo específico de programa malintencionado que restringe el acceso mediante cifrado o determinadas partes o archivos del sistema infectado y pide un rescate (Generalmente en moneda virtual) a cambio de eliminar dicha restricción.
1.2. Objetivo
Restaurar los servicios críticos de TI que soportan las estaciones de trabajo y servidores del PNACP
1.3. Valoración
Este evento es considerado alto.
1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en la sala de servidores del PNACP
1.5. Personal encargado
● Oficial de seguridad de la información.
1.6. Condiciones de Prevención de Riesgo
● Contar con equipos de respuesta ante incidentes de seguridad ante posibles ataques informáticos en estaciones de trabajo y servidores. ● Contar con las copias de respaldo y cintas de backup probadas y actualizadas. ● Contar con antivirus actualizado en las estaciones de trabajo y servidores. Libreta de números de contacto del proveedor al alcance.
2. PLAN DE EJECUCIÓN
2.1. Eventos que activan la Contingencia
Infección de virus informáticos en las estaciones de trabajo o sala de servidores
2.2. Procesos relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones del PNACP.
2.3. Personal que autoriza la Contingencia
Sub Jefe de la Sub-Unidad de Abastecimiento
2.4. Personal encargado
Especialista Informático
2.5. Descripción de los procedimientos después de activar la contingencia:
● Detección del evento de infección de virus informático. ● Validar si trata de un ataque tipo RANSOMWARE ● Notificar al Sub Jefe de la Sub-Unidad de Abastecimiento y equipo de respuesta de ● Incidentes de Seguridad de la PCM. ● Establecer las medidas de contención para evitar su propagación a nivel toda la red. ● Validar si se puede apagar el equipo informático afectado, si es posible se procede a desconectar de la red al equipo informático. ● Si no es posible apagarlo, se verifica que no allá más equipos afectados. ● Se realiza un análisis inmediato considerando los siguientes criterios: o Riesgos e impactos en toda la red. o Clonación de discos

9. CRONOGRAMA DEL PLAN DE PRUEBAS

9.1. Plan de Pruebas:

El Plan de Contingencias de TI comprende, el desarrollo de un plan de pruebas en el cual se incluye diferentes escenarios (Priorizados según plan) para comprobar que el plan diseñado es eficaz o, en caso contrario, se le debe efectuar ajustes correspondientes.

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

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

Tabla N° 02

N°	EVENTO	2025					2026				
		ABR	JUN	AG	NOV	DIC	ABR	JUN	AG	NOV	DIC
E1	Caída o interrupción de energía eléctrica	X				X	X				X
E2	Caída de internet		X					X			
E3	Infección masiva por software malicioso			X		X			X		X
E4	Suspensión de las actividades por sismo o incendio										
E5	Acceso no autorizado a la sala de servidores										
E6	Falla técnica en servidores	X									
E7	Falla en Sistemas de Información críticos					X					X
E8	Ausencia de personal de la Sub Unidad de Abastecimiento que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes		X					X			
E9	Calentamiento del Centro de Datos		X					X			
E10	Falla técnica en equipos de comunicación		X					X			
E11	Ataque informático				X					X	

El escenario 5 (E5) no se ha considerado porque solo se van a tratar los eventos de riesgos Muy Altas y Alta para el presente Plan de Contingencia de Tecnología de Información del PNACP.

10. PRESUPUESTO PARA LA EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

El Plan de Contingencia de Tecnologías de la Información contiene actividades que serán desarrolladas por el personal de la Sub-Unidad de Abastecimiento de acuerdo con sus competencias; dichas actividades planificadas están contempladas en el presupuesto asignado a la Sub-Unidad de Abastecimiento en el presente año y en los subsiguientes años fiscales.

11. SEGUIMIENTO Y MEJORA CONTINUA

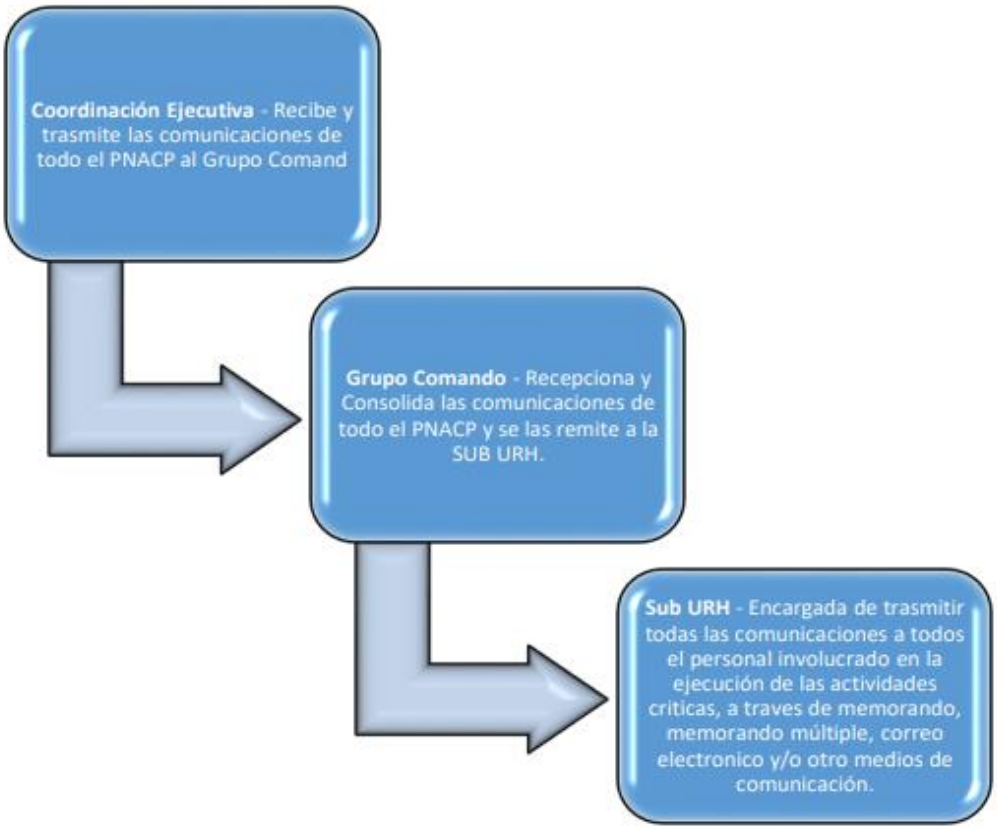
El responsable del mantenimiento y mejora continua del Plan es el Oficial de Seguridad de la Información o el que haga sus veces en la entidad. El plan debe ser revisado, probado y actualizado en su documentación y su alcance, esto quiere decir que el plan debe ser mejorado permanentemente a través de revisiones de acuerdo con los siguientes parámetros:

- Implementación de nuevos servicios críticos de TI: En caso se realicen nuevos sistemas o servicios que soporten procesos críticos de la institución, se deberá realizar un mantenimiento según el Plan de Contingencia.
- Resultados de una nueva evaluación de riesgos: Si dentro de la evaluación de riesgos se identifican nuevos escenarios de criticidad Muy Alta o Alta, se deberán desarrollar o actualizar los procedimientos de recuperación.
- Requisitos legales o contractuales: Ante nuevas regulaciones establecidos por la administración pública a través de las normativas vigentes.

ANEXO N° 03: PROCEDIMIENTOS PARA LA CONVOCATORIA DEL PERSONAL INVOLUCRADO EN LA EJECUCIÓN DE LAS ACTIVIDADES CRÍTICAS

Ejecución de la convocatoria y actividades a desarrollar:

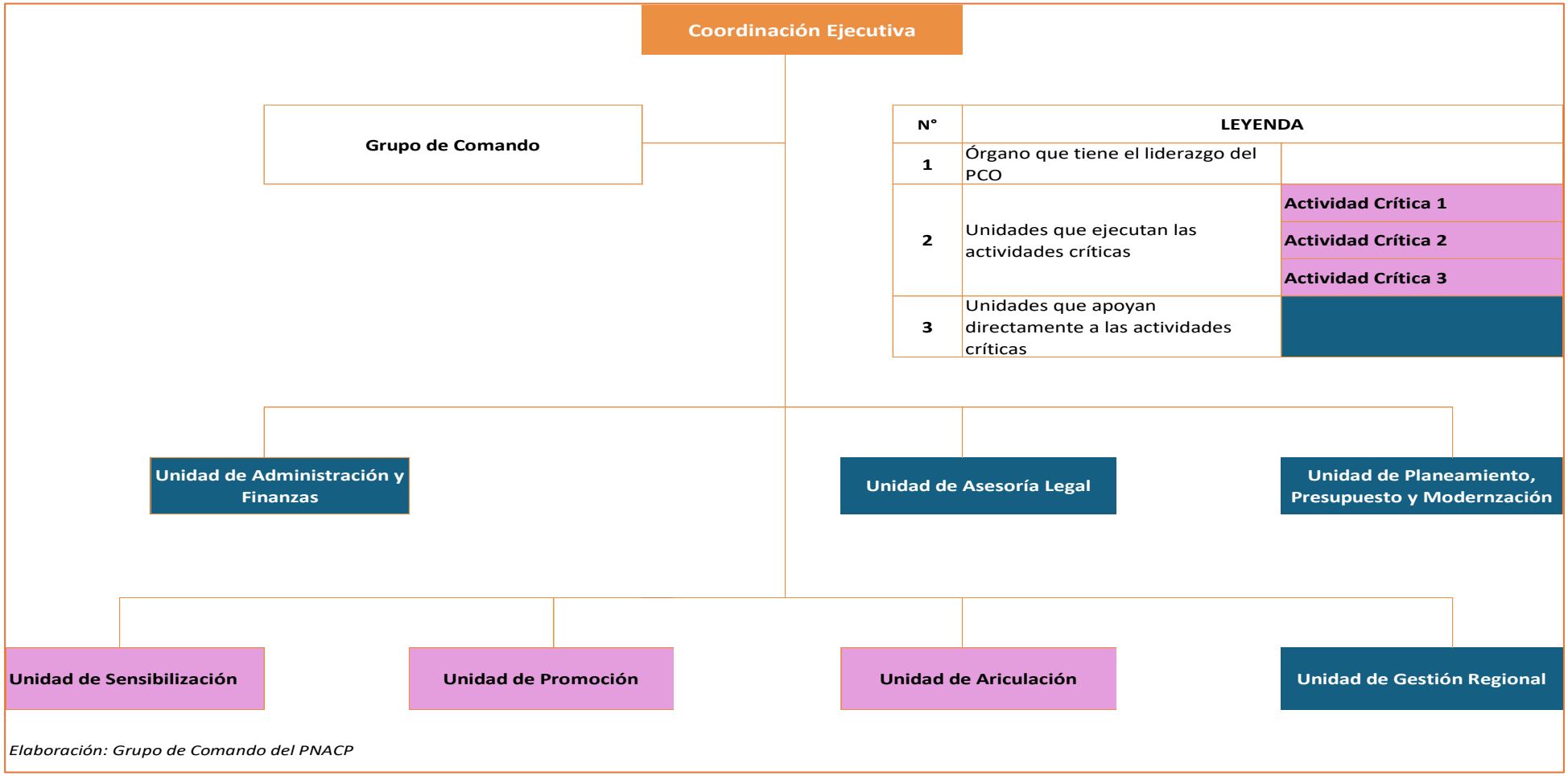
1. Una vez producido el evento de gran magnitud, la Coordinación Ejecutiva del PNACP convoca de manera inmediata al presidente del Grupo de Comando, reuniéndose en el local determinado como sede Alterna del PNACP.
2. En caso de activar el PCO, el Presidente del Grupo de Comando coordina, en sesión de Grupo de Comando, con el representante de la UAF para iniciar la movilización del personal que realizará trabajo presencial en la Sede Alterna.
3. Para realizar las comunicaciones se implementará la herramienta tecnológica que garantice la interacción remota para responder a la activación del Plan de Continuidad Operativa; asimismo, las comunicaciones se ejecutarán mediante telefonía móvil, mensajería instantánea, mensajería por correo electrónico, mensajería de voz y datos. La SUB URH y el/la Especialista en Comunicaciones de la US, se encargan de los comunicados oficiales a ser emitidos al personal o a los medios de comunicación de ser el caso, en coordinación con la CE y OCIIN del PRODUCE. De esta manera, se tomaría conocimiento 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 PNACP.
5. Reportar las novedades de personal y material al inicio de las actividades críticas de las unidades orgánicas a la Coordinación Ejecutiva, 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 PNACP, de corresponder.



ANEXO N° 04: DIRECTORIO DEL GRUPO DE COMANDO

ACTOR CLAVE	ENTIDAD	CORREO ELECTRÓNICO	CENTRAL TELEFÓNICA
Luis Andrés Millones Soriano	PNACP-UPPM	lmillones@acomerpesado.gob.pe	(01) 6148333
Percy Gastón Chumpitaz Villalobos	PNACP-UAF	pchumpitaz@acomerpesado.gob.pe	(01) 6148333/anexo 4006
Doris Javier Jiménez	PNACP-SURH	djavier@acomerpesado.gob.pe	(01) 6148333/anexo 4015
Janet Gisella Santos Cabezas de León	PNACP-SUABAST	jsantos@acomerpesado.gob.pe	(01) 6148333
Kerry Lewis García Hidalgo	PNACP-UP	kgarcia@acomerpesado.gob.pe	(01) 6148333/anexo 4014
Emanuel Augusto Montero Gómez	PNACP-UA	emontero@acomerpesado.gob.pe	(01) 6148333/anexo 4013
Carlos David Rubiños Carranza	PNACP-US	crubiños@acomerpesado.gob.pe	(01) 6148333/anexo 4012

ANEXO N° 05: ORGANIZACIÓN PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS



Elaboración: Grupo de Comando del PNACP

ANEXO N° 06: CRONOGRAMA DE IMPLEMENTACIÓN DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA

N°	ACTIVIDAD	RESPONSABLE	2025
			Enero: 1 2 3 4 5 | Febrero: 1 2 3 4 5 | Marzo: 1 2 3 4 5 | Abril: 1 2 3 4 5 | Mayo: 1 2 3 4 5 | Junio: 1 2 3 4 5 | Julio: 1 2 3 4 5 | Agosto: 1 2 3 4 5 | Setiembre: 1 2 3 4 5 | Octubre: 1 2 3 4 5 | Noviembre: 1 2 3 4 5 | Diciembre: 1 2 3 4 5
1	**CREACIÓN Y ACTIVACIÓN DEL GRUPO DE COMANDO**	**UPPM / CE**	
1.1	Envío del documento de propuesta del Grupo de Comando del PNACP	UPPMM	
1.2	Creación del Grupo de Comando	CE	
1.3	Activación del Grupo de Comando	UPPM	
2	**FORMULACIÓN DEL PCO**	**Grupo de Comando**	
2.1	Primera reunión del Grupo de Comando, donde se revisa la propuesta de PCO, y de planes similares en otras Entidades Públicas.	Grupo de Comando	
2.2	Gestión para concretar la capacitación sobre la normativa, estructura y fases del PCO	SUB-URH	
2.3	Capacitación a los miembros del Grupo de Comando sobre la normativa, estructura y fases del PCO	INDECI	
2.4	Reunión del Grupo de Comando, donde se revisa la normativa y se identifican modelos de PCO de referencia	Grupo de Comando	
2.5	Envío del borrador de PCO a INDECI, para revisión	UPPM	
2.6	Elaboración de PCO final del PNACP	Grupo de Comando	
2.7	Aprobación del PCO del PNACP	CE	
2.8	Difusión del PCO del PNACP	UPPM	
2.9	Gestión de la disponibilidad presupuestal del PCO	UPPM	
3	**IMPLEMENTACIÓN DEL PCO**	**Grupo de Comando**	
3.1	Realización del simulacro de implementación del PCO	Grupo de Comando	
3.2	Supervisión de la implementación de la gestión de la Continuidad Operativa e informar a la CE	Grupo de Comando	

Elaboración: Grupo de Comando del PNACP

Nota: Se precisa que las actividades del 2.1 al 2.6, relacionadas a la etapa 2 (Formulación del PCO) se han realizado de manera satisfactoria y oportuna de acuerdo a lo establecido en el presente cronograma.

N°	ACTIVIDAD	RESPONSABLE	2026																																																										
			Enero					Febrero					Marzo					Abril					Mayo					Junio					Julio					Agosto					Setiembre					Octubre					Noviembre					Dicimebre				
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1	**SEGUIMIENTO A LA IMPLEMENTACIÓN DEL PCO**	**Grupo de Comando**																																																										
1.1	Gestión para concretar la capacitación sobre la normativa, estructura y fases del PCO	SUB-URH																																																										
1.2	Capacitación al personal del PNACP sobre la normativa, estructura y fases del PCO	INDECI																																																										
1.3	Reunión del Grupo de Comando para efectuar el seguimiento del PCO	UPPM																																																										
1.4	Realizar el simulacro de implementación del PCO	Grupo de Comando																																																										
1.5	Supervisar la implementación de la gestión de la Continuidad Operativa e informar a la CE	Grupo de Comando																																																										

Elaboración: Grupo de Comando del PNACP

N°	ACTIVIDAD	RESPONSABLE	2027																																																										
			Enero					Febrero					Marzo					Abril					Mayo					Junio					Julio					Agosto					Setiembre					Octubre					Noviembre					Dicimebre				
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1	**SEGUIMIENTO A LA IMPLEMENTACIÓN DEL PCO**	**Grupo de Comando**																																																										
1.1	Gestión para concretar la capacitación sobre la normativa, estructura y fases del PCO	SUB-URH																																																										
1.2	Capacitación al personal del PNACP sobre la normativa, estructura y fases del PCO	INDECI																																																										
1.3	Reunión del Grupo de Comando para efectuar el seguimiento del PCO	UPPM																																																										
1.4	Realizar el simulacro de implementación del PCO	Grupo de Comando																																																										
1.5	Supervisar la implementación de la gestión de la Continuidad Operativa e informar a la CE	Grupo de Comando																																																										

Elaboración: Grupo de Comando del PNACP

ANEXO N° 07: FORMATO EVALUACIÓN DE DAÑOS

I. INFORMACIÓN GENERAL									
I-1	TIPO DE PELIGRO					I-2	FECHA DE OCURRENCIA	HORA DE OCURRENCIA	
I-3	PROVINCIA		DISTRITO		LOCALIDAD		BARRIO/SECTOR/URBANIZACIÓN	CENTRO POBLADO/CASERIO/ANEXO	
I-4	PUNTO DE REFERENCIA PARA LLEGAR A LA LOCALIDAD AFECTADA (Adjntar croquis a mano alzada del acceso a la zona de emergencia)				I-5	MEDIO DE TRANSPORTE SUGERIDO		I-6	ALTITUD (m.s.n.m)

II. DAÑOS					I-7	COORDENADAS GEOGRÁFICAS				I-8	COORDENADAS UTM
CÓDIGO		TOTAL				LATITUD		LONGITUD			
VIDA Y SALUD		NO	SÍ	CANTIDAD							
II-1	LESIONADOS (HERIDOS)				III. ACCIONES INMEDIATAS PARA LA ATENCIÓN DE EMERGENCIAS (Marcar con X)						
II-2	PERSONAS ATRAPADAS				III-1 ACTIVIDADES A REALIZAR				III-2 NECESIDADES DE APOYO EXTERNO		
II-3	PERSONAS AISLADAS										
II-4	DESAPARECIDOS										
II-5	FALLECIDOS										
SERVICIOS BÁSICOS		NO	SÍ								
II-6	AGUA										
II-7	DESAGÜE										
II-8	ENERGÍA ELÉCTRICA										
II-9	TELEFONÍA/INTERNET										
II-10	GAS										
INFRAESTRUCTURA		NO	SÍ		Observaciones:				Observaciones:		
II-11	LOCALES										
II-12	VEHÍCULOS										
II-13	EQUIPOS INFORMÁTICOS										
II-14	OTROS										
MEDIOS DE VIDA		NO	SÍ								
II-15	TIPO:										

NOMBRES Y APELLIDOS Y DNI DEL EVALUADOR			
TELÉFONO DE CONTACTO		COE-PRODUCE RECIBIDO POR (FRIMA Y POSFIRMA/DNI)	REPRESENTANTE DEL COMITÉ DE SEGURIDAD Y SALUD EN EL TRABAJO (CSST) - PNACP