

RESOLUCIÓN EJECUTIVA REGIONAL

N° 0223-2026-GRJ/GR

Huancayo, 24 SEP 2026

EL GOBERNADOR DEL GOBIERNO REGIONAL JUNÍN

VISTO:

El Reporte n.° 739-2026-GRJ/ORAJ, de fecha 16 de setiembre de 2026; la Opinión Legal n.° 50-2026-GRJ/ORAJ-REHO, de fecha 15 de setiembre de 2026; el Informe Técnico n.° 026-2026-GRJ/GRRNGMA/SGDC, de fecha 10 de setiembre de 2026; el Reporte n.° 1422-2026-GRJ/ORAF/ORH de fecha 08 de setiembre de 2026; el Reporte n.° 483-2026-GRJ/GRRNGMA/SGDC, de fecha 20 de agosto de 2026; la Resolución Ejecutiva Regional n.° 0192-2026-GRJ/GR, de fecha 12 de agosto de 2026; y,

CONSIDERANDO:

Que, el artículo 191° de la Constitución Política del Perú reconoce a los gobiernos regionales autonomía política, económica y administrativa en los asuntos de su competencia; asimismo, el artículo 2° de la Ley N.° 27867, Ley Orgánica de Gobiernos Regionales, establece que son personas jurídicas de derecho público;

Que, el artículo 61° de la Ley N.° 27867 establece funciones de los gobiernos regionales en materia de defensa civil, las cuales se ejercen en concordancia con el marco normativo del Sistema Nacional de Gestión del Riesgo de Desastres;

Que, la Ley n.° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD, establece el marco institucional y normativo orientado, entre otros aspectos, a fortalecer las capacidades de preparación y respuesta de las entidades públicas frente a situaciones de emergencia o desastre;

Que, en desarrollo del marco normativo del Sistema Nacional de Gestión del Riesgo de Desastres, mediante Decreto Supremo n.° 038-2021-PCM se aprobó la Política Nacional de Gestión del Riesgo de Desastres al 2050, orientada al fortalecimiento de las capacidades institucionales frente a situaciones de riesgo, emergencia y desastre;

Que, mediante Resolución Ministerial n.° 320-2021-PCM se aprobaron 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 establecen disposiciones para la implementación de la gestión de la continuidad operativa y la formulación de los respectivos planes;

Que, de acuerdo con los citados Lineamientos, el Plan de Continuidad Operativa establece las acciones y mecanismos para mantener o recuperar las actividades críticas y los servicios esenciales de la entidad ante eventos que afecten su funcionamiento, por lo que debe responder a sus condiciones institucionales y operativas vigentes;

Que, mediante Resolución Gerencial General Regional n.° 239-2024-JUNIN/GRR, de fecha 30 de diciembre de 2024, se aprobó el Plan de Continuidad Operativa del Gobierno

GOBERNACIÓN	
DOC. N°	11070204
EXP. N°	07247114



Gobierno Regional Junín



Regional Junín correspondiente al año 2024, instrumento cuya actualización se plantea en el presente expediente;



Que, mediante Resolución Ejecutiva Regional n.° 0192-2026-GRJ/GR, de fecha 12 de agosto de 2026, se designó a la Gerencia General Regional como unidad orgánica responsable de la Gestión de la Continuidad Operativa y se actualizó la conformación del Grupo de Comando del Gobierno Regional Junín;



Que, mediante Reporte n.° 1422-2026-GRJ/ORAF/ORH, de fecha 8 de setiembre de 2026, la Oficina Regional de Recursos Humanos emitió opinión favorable sobre el proyecto del Plan de Continuidad Operativa – Versión 2026, sin formular observaciones en los aspectos comprendidos dentro del ámbito de sus competencias;



Que, mediante Informe Técnico n.° 026-2026-GRJ/GRRNGMA/SGDC, de fecha 10 de setiembre de 2026, la Subgerencia de Defensa Civil señaló que, encontrándose formalizadas la unidad orgánica responsable de la Gestión de la Continuidad Operativa y la conformación del Grupo de Comando, corresponde continuar con el proceso de actualización y aprobación del Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026; asimismo, sustentó la necesidad de adecuar dicho instrumento a las condiciones institucionales y operativas vigentes, conforme a los Lineamientos aprobados por Resolución Ministerial n.° 320-2021-PCM;



Que, el literal f) del numeral 6.1.1 de los Lineamientos aprobados por Resolución Ministerial n.° 320-2021-PCM establece que corresponde al titular de la entidad aprobar el Plan de Continuidad Operativa y disponer su activación cuando corresponda, a propuesta del Grupo de Comando;



Que, mediante Reporte n.° 739-2026-GRJ/ORAJ, de fecha 16 de setiembre de 2026, la Oficina Regional de Asesoría Jurídica remitió la Opinión Legal n.° 50-2026-GRJ/ORAJ-REHO, en la que concluye que resulta jurídicamente procedente aprobar el Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026, conforme a los fundamentos y precisiones contenidos en dicha opinión;

De conformidad con la Ley n.° 27867, Ley Orgánica de Gobiernos Regionales; la Ley n.° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres; y los Lineamientos aprobados por Resolución Ministerial n.° 320-2021-PCM; con las visaciones de la Gerencia General Regional, la Gerencia Regional de Recursos Naturales y Gestión Ambiental, la Subgerencia de Defensa Civil y la Oficina Regional de Asesoría Jurídica, en el ámbito de sus respectivas competencias;

SE RESUELVE:

ARTÍCULO PRIMERO. - **APROBAR** el *Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026*, que, como Anexo, forma parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO. - **DEJAR SIN EFECTO**, a partir de la entrada en vigencia de la presente Resolución, el Plan de Continuidad Operativa del Gobierno Regional Junín aprobado mediante Resolución Gerencial General Regional n.° **239-2024-GR-JUNIN/GRR**, de fecha 30 de diciembre de 2024.

ARTÍCULO TERCERO. - **DISPONER** que la Gerencia General Regional, en su condición de unidad orgánica responsable de la Gestión de la Continuidad Operativa,



Gobierno Regional Junín



conduzca y coordine la implementación del Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026, con la participación del Grupo de Comando y de las unidades orgánicas comprendidas en dicho Plan, conforme a sus respectivas funciones.

ARTÍCULO CUARTO. - ENCARGAR a la Subgerencia de Defensa Civil que, en el ámbito de sus competencias, brinde asistencia técnica y efectúe el seguimiento de las acciones de implementación del Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026, e informe a la Gerencia General Regional sobre los avances, dificultades identificadas y medidas que recomiende adoptar.

ARTÍCULO QUINTO. - NOTIFICAR la presente Resolución y el Plan de Continuidad Operativa del Gobierno Regional Junín – Versión 2026, que forma parte integrante de ella, a la Gerencia General Regional, la Gerencia Regional de Recursos Naturales y Gestión Ambiental, la Subgerencia de Defensa Civil, los integrantes del Grupo de Comando y las demás unidades orgánicas comprendidas en su implementación, para conocimiento y cumplimiento en el ámbito de sus respectivas funciones.

ARTÍCULO SEXTO.- DISPONER la publicación de la presente resolución en el Portal Institucional del Gobierno Regional de Junín (www.regionjunin.gob.pe), conforme a la normativa vigente.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

GOBIERNO REGIONAL JUNÍN

Mg. ZÓSIMO CÁRDENAS MUJE
GOBERNADOR REGIONAL

GOBIERNO REGIONAL JUNÍN
La Secretaría General que suscribe, Certifica
que la presente es copia fiel de su original.

HYO. 28 SEP 2026

Abg. Ena M. Bonilla Pérez
SECRETARÍA GENERAL (a)



GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



PLAN DE CONTINUIDAD OPERATIVA 2026





GOBIERNO REGIONAL JUNÍN



PLAN DE CONTINUIDAD OPERATIVA - 2026

ÍNDICE

I. INTRODUCCION:	3
II. BASE LEGAL:	6
III. OBJETIVOS:	7
IV. IDENTIFICACIÓN DE RIESGO Y RECURSOS	8
V. ACCIONES PARA LA CONTINUIDAD OPERATIVA	17
VI. CRONOGRAMA DE EJERCICIOS DE CONTINUIDAD OPERATIVA	29
VII. ANEXOS	29





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



I. INTRODUCCION:

El Plan de Continuidad Operativa (PCO) constituye un instrumento de gestión orientado a garantizar la continuidad de las funciones críticas de una entidad pública frente a la ocurrencia de emergencias o desastres, mediante la implementación de estrategias, procedimientos y acciones que permitan minimizar los impactos negativos en la prestación de los servicios esenciales. Este instrumento se formula en el marco de lo dispuesto por la Ley N.º 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), así como de la Resolución Ministerial N.º 320-2021-PCM, que aprueba los lineamientos para la gestión de la continuidad operativa y la formulación de los Planes de Continuidad Operativa en las entidades públicas.

El Gobierno Regional de Junín, como entidad responsable de conducir el desarrollo integral de su jurisdicción, orienta su accionar institucional en base a su misión de promover el desarrollo sostenible, competitivo e inclusivo de la región, mediante una gestión eficiente, transparente y descentralizada, priorizando el bienestar de la población. Asimismo, su visión institucional se proyecta a consolidar una región ordenada, segura, competitiva y con igualdad de oportunidades, con acceso adecuado a servicios básicos y con un desarrollo articulado en sus diferentes provincias.

En cuanto a su ubicación, el Gobierno Regional de Junín tiene su sede principal en la ciudad de Huancayo, provincia de Huancayo, departamento de Junín, ejerciendo competencia en todo el ámbito regional, el cual comprende diversas provincias y distritos con características geográficas, sociales y económicas diversas, lo que implica la necesidad de garantizar la continuidad de los servicios públicos en todo su territorio, especialmente en contextos de emergencia.

En ese sentido, el Plan de Continuidad Operativa tiene como finalidad asegurar la prestación ininterrumpida de los servicios públicos esenciales ante situaciones adversas, reducir la vulnerabilidad institucional frente a posibles interrupciones, y establecer mecanismos de respuesta inmediata y recuperación oportuna de las actividades críticas. Asimismo, busca proteger los recursos humanos, materiales, tecnológicos y de información, fortaleciendo la capacidad de resiliencia institucional frente a eventos que puedan afectar su normal funcionamiento.





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



La implementación del PCO en el ámbito del Gobierno Regional implica un proceso integral que comprende la identificación y priorización de las funciones críticas y servicios esenciales, la evaluación de riesgos y escenarios que puedan afectar la continuidad operativa, así como la definición de medidas preventivas, de respuesta y recuperación. Del mismo modo, involucra la designación de responsables y equipos encargados de su ejecución, la garantía de disponibilidad de recursos necesarios, la implementación de mecanismos de comunicación interna y externa durante situaciones de emergencia, y la realización de simulacros y procesos de actualización permanente del plan.

En este contexto, el Gobierno Regional, en el marco del SINAGERD, desempeña un rol fundamental en la gestión de la continuidad operativa, siendo responsable de liderar la implementación del PCO en sus diferentes dependencias y entidades adscritas, así como de garantizar la continuidad de los servicios públicos regionales, especialmente en sectores críticos como salud, transporte, infraestructura y gestión ambiental.

Asimismo, le corresponde coordinar de manera articulada con los gobiernos locales, entidades del nivel nacional y demás actores involucrados, supervisar y monitorear la ejecución de las acciones previstas en el plan, asignar los recursos necesarios para su implementación y promover una cultura de prevención y gestión del riesgo de desastres en el ámbito regional.

A continuación, se presenta un cuadro resumen que contiene la información general del Gobierno Regional de Junín, con la finalidad de sistematizar y facilitar la identificación de los principales datos institucionales necesarios para la adecuada formulación e implementación del Plan de Continuidad Operativa, en concordancia con lo establecido en la Ley N.º 29664 y la Resolución Ministerial N.º 320-2021-PCM. Este cuadro permitirá contar con una visión clara y ordenada de los aspectos básicos de la entidad, contribuyendo a una mejor planificación de las acciones de continuidad operativa.





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



**INFORMACIÓN GENERAL DE LA SEDE CENTRAL DEL GOBIERNO REGIONAL
DE JUNÍN**

Nombre de la institución	Gobierno Regional de Junín
Gobernador Regional	Mg. Zosimo Cárdenas Muje
Vicegobernadora regional	CPC. Milagros Inche Arias
Página Web	https://www.regionjunin.gob.pe/index.php
Ubicación	Jr. Loreto N°363, Huancayo, Huancayo, Junín

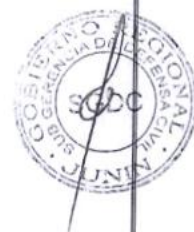
**MAPA DE UBICACIÓN DE LA SEDE CENTRAL DEL GOBIERNO REGIONAL
JUNÍN**





II. BASE LEGAL:

- Constitución Política del Perú.
- Ley N.º 32513, Ley de Presupuesto del Sector Público para el Año Fiscal 2026.
- Resolución Ejecutiva Regional que aprueba el Presupuesto Institucional de Apertura (PIA) 2026 del Gobierno Regional de Junín.
- Ley N.º 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N.º 048-2011-PCM, que aprueba el Reglamento de la Ley N.º 29664.
- Decreto Supremo N.º 060-2024-PCM, que modifica el Reglamento de la Ley N.º 29664.
- Decreto Supremo N.º 111-2012-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres.
- Decreto Supremo N.º 038-2021-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022-2030.
- Ley N.º 28522, Ley del Sistema Nacional de Planeamiento Estratégico y del Centro Nacional de Planeamiento Estratégico (CEPLAN).
- Decreto Supremo N.º 095-2022-PCM, que aprueba la Política Nacional de Desarrollo al 2050.
- Resolución Jefatural N.º 000158-2025-INDECI/JEF, que aprueba los lineamientos para la organización, ejecución y evaluación de los ejercicios de simulación de continuidad operativa para el periodo 2025–2027.
- Resolución Ministerial N.º 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la formulación de los Planes de Continuidad Operativa (PCO).





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



III. OBJETIVOS:

3.1 Objetivo general:

Garantizar que el Gobierno Regional de Junín cuente con la capacidad de asegurar la continuidad de sus operaciones, servicios y actividades esenciales ante la ocurrencia de eventos inesperados o situaciones de emergencia que puedan interrumpir su funcionamiento normal, tales como inundaciones, sismos, tormentas u otros eventos adversos de origen natural o antrópico. En ese sentido, el presente Plan de Continuidad Operativa tiene como finalidad permitir a la entidad responder de manera oportuna, ágil y efectiva frente a dichas contingencias, asegurando que los servicios críticos se mantengan operativos o, en su defecto, sean restablecidos en el menor tiempo posible, minimizando los impactos en la población y en la gestión institucional.

3.1 Objetivo específico:

- Identificar y priorizar las funciones críticas y servicios esenciales del Gobierno Regional de Junín, cuya continuidad debe ser asegurada ante situaciones de emergencia o desastre.
- Establecer procedimientos y acciones para la respuesta inmediata, continuidad y recuperación progresiva de las operaciones institucionales frente a eventos adversos.
- Determinar los recursos humanos, logísticos, tecnológicos y de infraestructura necesarios para garantizar la continuidad operativa de la entidad.
- Definir los roles y responsabilidades del personal involucrado en la implementación del Plan de Continuidad Operativa, asegurando una adecuada coordinación interna.
- Implementar mecanismos de comunicación y coordinación institucional que permitan una respuesta oportuna y eficiente durante situaciones de emergencia.
- Fortalecer la capacidad de respuesta institucional mediante la ejecución de simulacros, evaluaciones y actualización periódica del Plan de Continuidad Operativa.





IV. IDENTIFICACIÓN DE RIESGO Y RECURSOS

La identificación de riesgos constituye la etapa inicial del proceso de gestión de la continuidad operativa y consiste en reconocer, analizar y evaluar todos aquellos eventos, situaciones o circunstancias que podrían afectar negativamente la operatividad del Gobierno Regional de Junín, interrumpiendo el desarrollo de sus funciones esenciales y la prestación de servicios a la población. Estos riesgos pueden originarse a partir de diversas fuentes, incluyendo fenómenos naturales, fallas tecnológicas, eventos antrópicos o situaciones externas que comprometan el normal funcionamiento institucional.

En este contexto, el riesgo se define como la probabilidad de que se produzcan pérdidas o afectaciones en un determinado elemento o sistema como consecuencia de la ocurrencia de un peligro en condiciones específicas de vulnerabilidad. En términos conceptuales, el riesgo (R) es función del peligro (P) y la vulnerabilidad (V), siendo el resultado de la interacción de ambos factores.

Por su parte, el peligro se entiende como la probabilidad de ocurrencia de un fenómeno potencialmente dañino en un lugar específico, con una determinada intensidad, frecuencia y periodo de recurrencia. De acuerdo con su origen, los peligros pueden clasificarse en aquellos de origen natural, como sismos, inundaciones o lluvias intensas, y aquellos inducidos por la acción humana, tales como incendios, fallas estructurales o interrupciones de servicios básicos.

La identificación de riesgos permite determinar los eventos que, al materializarse, podrían afectar los objetivos institucionales, estrategias, planes, programas, proyectos y servicios que forman parte de la misión del Gobierno Regional de Junín, constituyéndose en un insumo clave para la adopción de medidas de prevención, respuesta y recuperación.

En ese sentido, considerando la información técnico-científica disponible sobre eventos disruptivos en la provincia de Huancayo, el Gobierno Regional de Junín focaliza su análisis y prioriza sus acciones en dicho ámbito geográfico, debido a la concentración de sus principales funciones administrativas y operativas en la sede central, lo que implica una mayor exposición al riesgo ante la ocurrencia de emergencias o desastres.



	GOBIERNO REGIONAL JUNÍN PLAN DE CONTINUIDAD OPERATIVA - 2026		
---	--	---	---

4.1 Matriz de riesgo e identificación del peligro

La matriz de riesgo constituye una herramienta fundamental para la gestión de la continuidad operativa, ya que permite identificar, analizar y valorar los riesgos que podrían afectar el funcionamiento de la entidad. Esta matriz se basa en la identificación de los peligros y las vulnerabilidades presentes en la institución, con el propósito de estimar el nivel de riesgo asociado a cada evento potencial.

El riesgo (R) se determina a partir de la interacción entre el peligro (P) y la vulnerabilidad (V), lo que permite establecer una valoración cualitativa que facilite la priorización de acciones de prevención, reducción y respuesta. En este sentido, la matriz de riesgo orienta la toma de decisiones para asegurar la continuidad de las funciones críticas de la entidad ante situaciones adversas.

En el contexto de la Región Junín, la identificación de peligros se sustenta en la información histórica y en los escenarios de riesgo definidos en el Plan de Gestión Reactiva, considerando aquellos eventos con mayor recurrencia y capacidad de generar interrupciones prolongadas en las operaciones institucionales.

Entre los principales peligros identificados se encuentran:

- **Heladas**, que ocupan el primer lugar en ocurrencia con 498 eventos registrados, afectando principalmente a poblaciones vulnerables y generando impactos en infraestructura y servicios.
- **Lluvias intensas**, con 361 ocurrencias, las cuales provocan inundaciones, daños en vías de acceso y afectación a la operatividad institucional.
- **Sismos**, considerados un peligro latente debido a la presencia de fallas geológicas activas, como la del Huaytapallana, con potencial de generar daños significativos en infraestructura.
- **Movimientos en masa (deslizamientos y huaicos)**, frecuentes en zonas de selva y laderas, que pueden interrumpir vías de comunicación y acceso a servicios.
- **Incendios urbanos e industriales**, con alta recurrencia histórica, representando un riesgo importante para instalaciones, equipos y personal.

La evaluación de estos peligros, en conjunto con el análisis de las vulnerabilidades institucionales, permitirá establecer niveles de riesgo que servirán como base para la formulación de estrategias de continuidad operativa.

Tabla 1- NIVEL DE RIESGO POR PELIGRO

Peligro	Nivel de Peligro (P)	Vulnerabilidad Institucional (V)	Nivel de Riesgo (R)	Sustento
Sismos	Muy Alto	Alta	Muy Alto	La zona central de Huancayo presenta acumulación de energía sísmica y cercanía a la falla del Huaytapallana. Un edificio de 7 pisos aumenta la vulnerabilidad por la complejidad de la evacuación vertical y posibles fallas estructurales o no estructurales que interrumpirían la operación.
Incendios Urbanos	Alto	Alta	Alto	Es el tercer peligro más recurrente en la región (266 eventos registrados). Al estar en el centro comercial de Huancayo y tener 7 niveles, el riesgo de propagación e interrupción por daños en infraestructura eléctrica o de TI es elevado.
Lluvias Intensas	Alto	Media	Alto	Huancayo registra alta recurrencia de lluvias intensas (361 eventos). La vulnerabilidad se centra en posibles filtraciones en techos o inundación de sótanos donde operan servicios críticos como servidores o archivos.
Heladas	Muy Alto	Baja	Medio	Es el peligro más frecuente en la región. Si bien no afecta estructuralmente el edificio, impacta en la salud del personal (incremento de IRAs y neumonías), lo que puede causar ausentismo crítico y afectar la continuidad operativa.
Vientos Fuertes	Alto	Baja	Medio	Peligro recurrente en el Valle del Mantaro (248 eventos). Podría afectar ventanales de los pisos altos y sistemas de comunicación (antenas) en la azotea del edificio, causando interrupciones menores



La asignación de los niveles de peligro y vulnerabilidad permitió determinar los valores correspondientes a los distintos escenarios de riesgo, identificándose niveles "Muy Alto", "Alto" y "Medio", según el tipo de evento evaluado.

Destaca el riesgo sísmico como el de mayor criticidad (Muy Alto), debido a la combinación de alta peligrosidad geológica y elevada vulnerabilidad estructural y operativa. Este resultado es consistente con la información histórica contenida en la



GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



base de datos de emergencias y daños ocurridos en el Perú (2003–2020), así como con el catálogo sísmico 1960–2021 del Instituto Geofísico del Perú.

Para el análisis de la recurrencia e impacto, los eventos han sido organizados según su origen y distribución territorial, permitiendo identificar zonas con mayor exposición al riesgo. En el caso específico del riesgo sísmico, se han empleado herramientas de Sistemas de Información Geográfica (SIG) para evaluar la susceptibilidad y vulnerabilidad del territorio, aplicando criterios técnicos del CENEPRED.

Estos resultados constituyen un insumo fundamental para la toma de decisiones orientadas a la planificación de medidas de prevención, reducción del riesgo y aseguramiento de la continuidad operativa en el ámbito institucional.

Con la finalidad de complementar la identificación de riesgos, se incorpora el análisis de vulnerabilidad sísmica a partir de la información geoespacial disponible, la cual permite visualizar la susceptibilidad del territorio frente a eventos sísmicos.



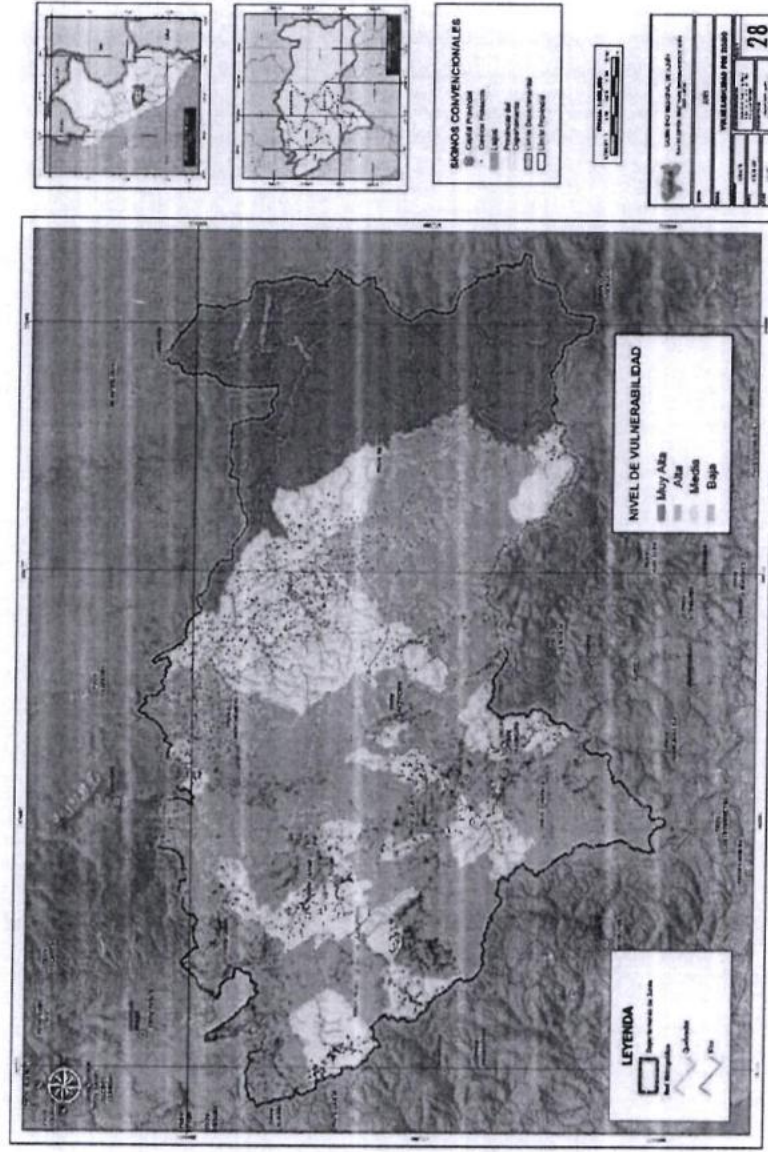


GOBIERNO REGIONAL JUNÍN



PLAN DE CONTINUIDAD OPERATIVA - 2026

MAPA N° 1 – VULNERABILIDAD POR SISMO



Fuente: Plan de Prevención y Reducción del Riesgo de Desastre del Departamento de Junín 2024- 2030



El mapa de vulnerabilidad sísmica presenta la distribución espacial de los niveles de exposición ante sismos, identificando zonas clasificadas en niveles de vulnerabilidad baja, media, alta y muy alta, en función de factores como características del suelo, densidad urbana, tipología constructiva y proximidad a fallas geológicas activas.

En el ámbito de influencia de la entidad, se observa que:

- Existen zonas con vulnerabilidad alta y muy alta, asociadas a suelos inestables y alta concentración de edificaciones.
- La cercanía a la falla geológica del Huaytapallana incrementa la probabilidad de afectación severa ante un evento sísmico.
- La infraestructura institucional, al ubicarse en zona urbana consolidada y contar con edificación de varios niveles, presenta condiciones que incrementan la vulnerabilidad operativa ante un sismo de gran magnitud.

4.1 Determinación de nivel de impacto

La determinación del nivel de impacto tiene como finalidad establecer las consecuencias que generaría la interrupción de los procesos críticos de la entidad, considerando aspectos operativos, legales y funcionales. Este análisis permite identificar la criticidad de cada unidad orgánica y definir prioridades para la recuperación de los servicios esenciales.

En este contexto, se define el Período Máximo Tolerable de Interrupción (PMTI) como el tiempo máximo durante el cual un proceso puede permanecer interrumpido sin generar consecuencias inaceptables para la entidad. La determinación del PMTI permite orientar la planificación de estrategias de continuidad operativa y recuperación.

Para las unidades orgánicas analizadas, el impacto de la interrupción no solo es de carácter operativo, sino también legal y administrativo, dado que muchas de sus funciones están vinculadas a la gestión de emergencias, asignación de recursos y toma de decisiones críticas.



TABLA 2 - DETERMINACIÓN DEL NIVEL DE IMPACTO Y PMTI

UNIDAD ORGÁNICA / PROCESO CRÍTICO	IMPACTO CUALITATIVO	PMTI (TIEMPO LÍMITE)	JUSTIFICACIÓN DEL IMPACTO
Oficina Regional de Desarrollo Institucional Tecnologías de la Información (ORDITI)	BAJO	24 < 72 horas	La interrupción de los servidores y la conectividad genera la pérdida de acceso a sistemas críticos como SISDORE, SIAF, SIGA SIGRID, SINPAD y plataformas internas, imposibilitando la operatividad de todas las demás unidades orgánicas.
Oficina regional de Administración y finanzas / Oficina Regional de Abastecimiento y Servicios Auxiliares	MEDIO	24 < 72 horas	La paralización de este proceso impide la contratación de servicios de emergencia, adquisición de bienes de ayuda humanitaria y cumplimiento de pagos (planillas y proveedores), afectando la respuesta institucional.
Gerencia General / Oficina Regional de Asesoría Jurídica	ALTO	24 < 72 horas	La interrupción limita la emisión de resoluciones ejecutivas necesarias para declarar situaciones de emergencia, autorizar intervenciones y disponer recursos institucionales.
Gerencia Regional de Planeamiento, Presupuesto y Acontecimiento Territorial	MUY ALTO	24 < 72 horas	La inoperatividad impide realizar modificaciones presupuestales (como PP068 o FONDES), lo que restringe el financiamiento oportuno de acciones de respuesta ante desastres.



Del análisis realizado se identifica que las unidades orgánicas vinculadas a tecnologías de la información y gestión administrativa presentan el mayor nivel de criticidad, debido a su rol transversal en el funcionamiento institucional.

En particular, la Oficina Regional de Desarrollo Institucional Tecnologías de la Información destaca como el proceso más crítico, con un PMTI de hasta 4 horas, debido a que su interrupción afecta de manera inmediata la operatividad de todos los sistemas institucionales y la capacidad de respuesta ante emergencias.

Asimismo, las áreas de Administración, Gerencia General y Planeamiento presentan niveles de impacto alto a muy alto, debido a su responsabilidad en la toma de decisiones, asignación de recursos y sostenimiento de las operaciones institucionales.

Estos resultados permiten priorizar la implementación de estrategias de continuidad operativa, enfocadas en asegurar la disponibilidad de los sistemas críticos, la gestión



oportuna de recursos y la capacidad de respuesta institucional ante situaciones de emergencia.

4.2 Identificación de Recursos

La identificación de recursos para la continuidad operativa tiene como finalidad determinar los medios indispensables que requiere la entidad para asegurar el funcionamiento de sus procesos críticos ante una interrupción, incluyendo escenarios en los que sea necesario operar desde una sede alterna.

En este contexto, no solo se consideran los recursos disponibles en la sede institucional principal, sino también aquellos que permiten garantizar la operatividad de las unidades orgánicas críticas en condiciones de emergencia.

Un elemento relevante en este análisis es la disponibilidad de infraestructura alternativa, como el ambiente del Centro de Operaciones de Emergencia Regional (COER), el cual, al contar con una edificación de un solo nivel, presenta menor vulnerabilidad estructural ante eventos sísmicos, constituyéndose en una opción viable para la continuidad de operaciones.

Los recursos identificados se clasifican en recursos humanos, tecnológicos, de comunicaciones, logísticos y de infraestructura alternativa.

a) Recursos Humano:

Se identifican como recursos humanos críticos a los funcionarios y equipos técnicos responsables de la toma de decisiones y ejecución de acciones durante situaciones de emergencia:

- Los 15 integrantes del Grupo de Trabajo para la Gestión del Riesgo de Desastres (GTGRD), incluyendo al Gobernador Regional y Gerentes.
- Personal técnico especializado de cada unidad orgánica crítica (TI, Administración, Planeamiento, Infraestructura).
- Equipos de soporte operativo encargados de garantizar la continuidad de los servicios esenciales.

b) Recursos tecnológicos:

Los recursos tecnológicos son esenciales para la continuidad de los procesos institucionales:

- Equipos de cómputo identificados como críticos para la operación.





- Servidores institucionales y acceso a sistemas como SIGA, SIAF, SISDORE, SIGRID y SINPAD.
- Implementación de copias de seguridad (backups) externas, especialmente de información crítica de Administración y Presupuesto.
- Posibilidad de acceso remoto o uso de entornos alternos que permitan operar desde otra ubicación.

c) Recursos de Comunicación:

Las comunicaciones son fundamentales para asegurar la coordinación institucional:

- Teléfonos satelitales, que garantizan comunicación ante caída de redes convencionales.
- Radios operativos, para coordinación interna y enlace con las provincias.
- Sistemas alternativos que aseguren la comunicación entre la sede de operaciones y las 9 provincias.

d) Recursos Logísticos:

Los recursos logísticos permiten ejecutar acciones de respuesta y rehabilitación:

- Pool de maquinaria pesada, conformado por:
 - Cargadores frontales
 - Volquetes
 - Retroexcavadora
- Equipos destinados a la atención de emergencias y recuperación de infraestructura.
- Capacidad de gestión de estos recursos por parte de la Gerencia de Infraestructura desde una ubicación segura.

e) Infraestructura alternativa para la continuidad de operaciones:

Se cuenta con el ambiente del Centro de Operaciones de Emergencia Regional (COER) como infraestructura alternativa para la continuidad operativa.

Esta instalación, al ser de un solo nivel, presenta menor exposición a daños estructurales ante eventos sísmicos, en comparación con edificaciones de varios pisos.

Permite la instalación temporal de funciones críticas, especialmente de:

- Gerencia General
- Oficina de Tecnologías de la Información





- Coordinación de emergencias

Facilita la continuidad del comando, control y toma de decisiones en situaciones de desastre.

En este sentido, el COER se configura como una sede alterna estratégica, con capacidad para albergar operaciones esenciales en caso de inoperatividad de la sede principal.

V. ACCIONES PARA LA CONTINUIDAD OPERATIVA

5.1 Determinación de actividades críticas

En el marco del análisis de riesgos e identificación de recursos, se ha determinado la necesidad de asegurar la continuidad de las funciones críticas de la entidad mediante su traslado a una sede alterna en caso de interrupción de la sede principal.

En este contexto, el ambiente del Centro de Operaciones de Emergencia Regional (COER), ubicado en la provincia de Concepción, se establece como sede alterna estratégica, debido a que su infraestructura de un solo nivel presenta menor vulnerabilidad ante el riesgo sísmico, identificado como el escenario de mayor impacto para edificaciones de varios niveles en la ciudad de Huancayo.

En caso de activación del plan de continuidad operativa, se priorizará el traslado inmediato de las siguientes actividades críticas:

- a) Monitoreo y conducción de emergencias Centro de Operaciones de Emergencia regional
 - Operatividad continua (24/7) de los sistemas de monitoreo y gestión de emergencias.
 - Recepción, procesamiento y análisis de información proveniente de las provincias.
 - Coordinación interinstitucional para la atención de emergencias.

Esta actividad constituye el eje central de la respuesta operativa, asegurando el flujo de información y la toma de decisiones en tiempo real.

- b) Soporte tecnológico encargado por la Oficina Regional De Desarrollo Institucional De Tecnología De La Información.
 - Garantizar el acceso a plataformas críticas como SIAF, SIGA, SISDORE, SIGRID y SINPAD.





- Activación de servidores de respaldo y sistemas alternos.
- Soporte técnico para la operatividad de los equipos en la sede alterna.

El restablecimiento de los servicios tecnológicos es prioritario, considerando su carácter transversal para todas las áreas.

- c) Gestión administrativa y financiera encargado por la Oficina Regional de Administración y Finanzas.
- Ejecución de procesos de contratación de emergencia.
- Adquisición y distribución de bienes de ayuda humanitaria.
- Movilización de recursos financieros, incluyendo los provenientes de programas presupuestales como el PP068.

Esta actividad garantiza la disponibilidad de recursos necesarios para la respuesta inmediata.

- d) Toma de decisiones estratégicas a cargo de Gobernación Regional y Gerencia General del Gobierno Regional
- Emisión de actos resolutivos para la declaratoria y atención de emergencias.
- Dirección y supervisión de la respuesta institucional.
- Coordinación con autoridades regionales y nacionales.

Esta función asegura la conducción política y administrativa de la respuesta ante desastres.

5.2 Aseguramiento de acervo documentario a cargo de Secretaria General del Gobierno Regional Junín

El aseguramiento del acervo documentario tiene como objetivo salvaguardar la documentación indispensable para el funcionamiento de las actividades críticas del Gobierno Regional de Junín, considerando que gran parte de la información administrativa vigente se encuentra en soporte físico en la sede principal ubicada en Jr. Loreto.

Este componente cobra especial relevancia en el contexto del riesgo sísmico identificado, así como ante eventos como incendios, los cuales podrían comprometer la integridad y disponibilidad de la documentación necesaria para la continuidad operativa.

- a) Diagnóstico de vulnerabilidad del acervo documentario



El acervo documentario institucional se clasifica en dos bloques principales, con distintos niveles de riesgo:

- Archivo Central (Sede externa):
Contiene documentación histórica y de archivo. Presenta un menor impacto inmediato sobre la continuidad operativa; sin embargo, requiere medidas básicas de seguridad física y control.
- Acervo técnico-administrativo actual (Sede Jr. Loreto):
Contiene expedientes de contratación, planillas, resoluciones y documentación en trámite

Debido a su ubicación en una edificación de 7 niveles y a la ausencia de digitalización, presenta una **vulnerabilidad muy alta** ante eventos como sismos o incendios, pudiendo generar la pérdida de información crítica para la gestión institucional.

b) Estrategias de protección del acervo documentario

Dado que actualmente no se cuenta con un proceso integral de digitalización, se implementarán medidas de protección física y operativa:

- Ubicación estratégica
Los archivos de gestión de las oficinas críticas deberán almacenarse en mobiliario resistente al fuego (archivadores ignífugos), debidamente rotulados y ubicados en niveles de fácil acceso, a fin de facilitar su recuperación en situaciones de emergencia.
- Kit de evacuación de documentos (Maletín de Documentos Vitales)
Cada unidad orgánica crítica contará con un maletín que contenga los documentos priorizados, el cual deberá ser retirado por el personal designado y trasladado hacia la sede alterna en caso de evacuación, siempre que las condiciones de seguridad lo permitan.
- Custodia en sede alterna (COER)
Se habilitará un espacio seguro en la sede alterna del COER en Concepción para la recepción, resguardo y administración temporal de la documentación crítica evacuada.

5.3 Acción de mejora prioritaria: digitalización del acervo crítico

Como parte de la mejora continua del Plan de Continuidad Operativa, se implementará progresivamente un proceso de digitalización del acervo documentario, priorizando:



- Documentos con valor legal vigente
- Información financiera y presupuestal
- Expedientes administrativos en curso

Esta acción será liderada por la Oficina de Tecnologías de la Información en coordinación con la Oficina de Administración, con el objetivo de contar con copias digitales de respaldo almacenadas en ubicaciones seguras o externas a la sede principal.

5.4 Roles y Responsabilidades

- Jefes de Unidades Orgánicas del Gobierno Regional Junín
Responsables de identificar, clasificar y rotular los documentos de "Prioridad 1", así como asegurar su disponibilidad para evacuación.
- Subgerencia de Defensa Civil:
Responsable de coordinar y ejecutar simulacros que incluyan el procedimiento de evacuación del acervo documentario crítico.
- Oficina Regional de Desarrollo Institucional y Tecnologías de la Información:
Responsable de implementar y gestionar el proceso de digitalización y respaldo de la información institucional.

5.5 Requerimientos

Los requerimientos para la continuidad operativa comprenden el conjunto de recursos mínimos indispensables que deben ser asegurados para garantizar la ejecución de las actividades críticas en la sede alterna, así como la respuesta institucional ante situaciones de emergencia.

Estos requerimientos se estructuran en función de los recursos humanos, materiales, tecnológicos y presupuestales necesarios para mantener la operatividad del Gobierno Regional de Junín.

a) Requerimientos de personal

Se identifica el personal mínimo indispensable que deberá movilizarse a la sede alterna (COER Concepción) o, de ser el caso, activar modalidades de trabajo remoto:

- **Toma de decisiones:**
 - Los 15 integrantes del Grupo de Trabajo para la Gestión del Riesgo de Desastres (GTGRD), encabezados por el Gobernador Regional y los Gerentes Regionales.



- **Operatividad de emergencia:**
 - Equipo de la Subgerencia de Defensa Civil y equipo de Evaluación de Daños de otras dependencias.
 - Personal de monitoreo del COER (6 personas).
- **Soporte administrativo y técnico:**
 - Personal clave de las oficinas de Administración, Abastecimiento y Tecnologías de la Información (TI), necesario para:
 - Gestión de contrataciones de emergencia.
 - Ejecución de recursos del Programa Presupuestal 0068.
 - Soporte y recuperación de servicios informáticos.

Este personal constituye el núcleo operativo para la continuidad institucional.

b) **Requerimientos de material y equipo**

Para asegurar el funcionamiento de la sede alterna, se deberá contar con los recursos materiales, mobiliario, equipos informáticos y demás bienes indispensables para el desarrollo de las funciones críticas. La provisión y disponibilidad de dichos recursos estará a cargo de la Oficina de Patrimonio, dependencia de la Oficina Regional de Administración, la cual adoptará las acciones necesarias para su asignación y uso oportuno durante la activación de la sede alterna.

- **Mobiliario y equipamiento básico:**
 - Mínimo de 12 escritorios operativos.
 - Equipamiento de oficina (sillas, archivadores, suministros básicos).
- **Logística de respuesta:**

Para la atención de emergencias y la continuidad de las operaciones críticas, se contará con el acceso al pool de maquinaria del Gobierno Regional de Junín, administrado por la Gerencia Regional de Infraestructura, el cual comprende, entre otros, los siguientes equipos:

- 18 cargadores frontales.
- 56 camiones volquete.
- 18 motoniveladoras.

Estos recursos constituyen un soporte logístico estratégico para la atención de emergencias, permitiendo ejecutar acciones de respuesta inmediata, rehabilitación de



vías de comunicación, remoción de escombros y recuperación de la transitabilidad en las zonas afectadas.

Sistemas de Respaldo (UPS): La Oficina Regional de Desarrollo Institucional y Tecnologías de la Información es la responsable de la administración y gestión de los sistemas de respaldo de energía (UPS), garantizando su operatividad para proteger los servidores, equipos de comunicación y demás infraestructura tecnológica crítica.

Asimismo, se prevé la disponibilidad y/o adquisición de sistemas UPS de alta capacidad, con la finalidad de asegurar el suministro ininterrumpido de energía y evitar interrupciones o apagados abruptos durante el tiempo de conmutación y puesta en funcionamiento del grupo electrógeno, preservando la continuidad de los servicios informáticos y de comunicaciones de la entidad.

- **Equipos de campo:**

- 15 kits de Equipos de Protección Personal (EPP).
- Chalecos de identificación para brigadistas y personal técnico encargado de evaluaciones de daños post-evento.

- c) **Requerimientos de recursos informáticos**

Los recursos informáticos constituyen el soporte crítico para la gestión de información y la toma de decisiones basada en evidencia:

- **Hardware:**

- Mínimo de 12 computadoras operativas interconectadas en la sede alterna.

- **Sistemas y software:**

Licencias activas de:

- ArcGIS (2)
- QGIS (1)
- AutoCAD (2)

Herramientas necesarias para análisis geoespacial, modelamiento de escenarios y evaluación de daños.

- **Comunicaciones de emergencia:**

Operatividad de:

- 8 radios
- 4 teléfonos satelitales



	GOBIERNO REGIONAL JUNÍN PLAN DE CONTINUIDAD OPERATIVA - 2026		
---	--	---	---

Conexión a internet estable en la sede alterna, indispensable para la gestión de información.

- **Acceso a plataformas institucionales:**

Credenciales vigentes para administradores de:

- SIGRID
- SINPAD
- SIAF
- SIGA

Permitiendo el registro oficial y seguimiento de emergencias.

5.6 Determinación de la Sede Alterna de Trabajo

La entidad ha determinado como sede alterna al Centro de Operaciones de Emergencia Regional (COER) Junín, el cual será utilizado para garantizar la continuidad de las funciones críticas en caso de inoperatividad de la sede principal.

- Ubicación política: Chimapamarca S/N, distrito de Matahuasi, Provincia de Concepción, departamento de Junín
- Altitud: 3,286 m s. n. m.
- Seguridad estructural: A diferencia de la sede principal ubicada en Jr. Loreto (Huancayo), que cuenta con una edificación de 7 niveles, el COER es una infraestructura de un solo nivel, lo que reduce significativamente la vulnerabilidad ante eventos sísmicos de gran magnitud.
- Infraestructura especializada para la gestión de crisis: El COER está diseñado específicamente para facilitar la administración, procesamiento e intercambio de información técnico-política durante situaciones de emergencia, permitiendo una respuesta oportuna y coordinada.
- Accesibilidad y ubicación estratégica: Su ubicación en el Valle del Mantaro permite mantener la conectividad con las 9 provincias de la región, facilitando la articulación territorial y la gestión descentralizada de la respuesta.

5.7 Activación del plan de continuidad operativa

El presente apartado establece los criterios, autoridades y procedimientos para la activación del Plan de Continuidad Operativa (PCO), a fin de garantizar una respuesta oportuna ante eventos que generen la inoperatividad de la sede principal.



La activación del PCO implica la declaratoria formal de interrupción de operaciones en la sede principal y el traslado de las actividades críticas hacia la sede alterna (COER Junín – Concepción).

a) Criterios de activación

El Plan de Continuidad Operativa se activará ante la ocurrencia de un evento adverso —principalmente sismos de gran magnitud o incendios— que genere una interrupción de las operaciones superior al Período Máximo Tolerable de Interrupción (PMTI) definido en el numeral 4.2.

Se establecen como criterios específicos de activación los siguientes:

- **Daño estructural:**

Colapso parcial o total de la sede principal ubicada en Jr. Loreto (7 niveles) o de sedes descentralizadas (6 niveles), que comprometa la seguridad del personal y la operatividad institucional.

- **Inaccesibilidad**

Imposibilidad de acceso a las instalaciones debido al riesgo de colapso de edificaciones colindantes o condiciones de inseguridad en el entorno urbano de Huancayo.

- **Falla tecnológica crítica:**

Interrupción de los servidores centrales o sistemas de información de la Oficina de Tecnologías de la Información que no pueda ser restablecida en un periodo menor a 4 horas.

- **Colapso de servicios básicos**

Corte prolongado de energía eléctrica, telecomunicaciones u otros servicios esenciales que imposibiliten la gestión administrativa y la respuesta institucional.

b) Autoridad de activación

De conformidad con la normativa vigente, la activación del PCO se realizará bajo las siguientes responsabilidades:

- **Titular de la Entidad (Gobernador Regional):**

Autoridad competente para aprobar la activación del Plan de Continuidad Operativa.

- **Grupo de Comando:**





Responsable de evaluar la situación institucional y proponer la activación del PCO al Titular de la Entidad, en función del nivel de afectación.

c) Protocolo de activación

Ante la ocurrencia de un evento que comprometa la operatividad institucional, se seguirá el siguiente flujo de acciones:

- **Evaluación rápida de daños:**

El Grupo de Comando, liderado por la Gerencia General y la Subgerencia de Defensa Civil, evalúa el nivel de afectación de la sede principal y determina la capacidad de operación.

- **Declaratoria de inoperatividad**

En caso de identificarse una interrupción prolongada, el Grupo de Comando comunica la situación al Gobernador Regional, recomendando la activación del PCO.

- **Orden de movilización:**

El Gobernador Regional dispone la activación del PCO y ordena el traslado inmediato del personal clave (GTGRD y equipos técnicos) hacia la sede alterna en Concepción.

- **Notificación externa:**

Se comunica la activación del plan al INDECI y a las 9 provincias de la región, informando el cambio de sede operativa para garantizar la coordinación interinstitucional.

- **Inicio de operaciones en sede alterna**

Se activan las actividades críticas en el COER, priorizando:

- Conectividad a plataformas SIAF, SIGA, SIGRID y SINPAD
- Monitoreo de emergencias
- Gestión de recursos del Programa Presupuestal 0068

d) Escenario de activación inmediata

Considerando que la sede alterna (COER Concepción) no cuenta actualmente con un grupo electrógeno, se establecen medidas temporales para garantizar la operatividad inicial:

- Movilización inmediata de equipos de iluminación portátiles.
- Abastecimiento de combustible para equipos de emergencia disponibles.





- Coordinación para el uso de fuentes de energía alternas en la zona.

Estas acciones permitirán asegurar la operatividad básica del COER hasta la implementación de la Acción de Cierre de Brechas (ACB) correspondiente a la adquisición de un generador eléctrico permanente.

5.8 Activación y desactivación de la sede alterna

El presente apartado establece los procedimientos para la ocupación (activación) y desocupación (desactivación) de la sede alterna, garantizando la continuidad de las operaciones críticas y el retorno progresivo a la normalidad operativa.

a) Activación (ocupación de la sede alterna)

La activación de la sede alterna se produce cuando la sede principal ubicada en Jr. Loreto pierde su capacidad operativa o representa un riesgo para la seguridad del personal y el cumplimiento de la misión institucional.

➤ Orden de ocupación

El Gobernador Regional, en su calidad de Titular de la Entidad, emite la orden de traslado inmediato hacia la sede alterna en la provincia de Concepción, previa recomendación del Grupo de Comando.

➤ Protocolo de desplazamiento

Se movilizan:

- Los 15 integrantes del Grupo de Trabajo para la Gestión del Riesgo de Desastres (GTGRD).
- Personal técnico clave de las áreas de Tecnologías de la Información, Administración y Presupuesto.

Se prioriza:

- El retiro y traslado del acervo documentario crítico, mediante los "Maletines de Documentos Vitales".
- Esta acción es especialmente relevante debido a la ausencia de digitalización certificada del acervo institucional.
- Instalación y operatividad

Se habilitan los espacios de trabajo en el COER; se activan:

- 12 computadoras operativas.





- Sistemas de comunicación (radios y 4 teléfonos satelitales).

Se inicia la ejecución de las actividades críticas, incluyendo:

- Monitoreo de emergencias
- Acceso a plataformas SIAF, SIGA, SIGRID y SINPAD
- Gestión de recursos para la atención de la emergencia
- Contingencia energética

Ante la ausencia de un grupo electrógeno fijo en la sede alterna, se implementarán medidas temporales para garantizar la operatividad:

- Movilización de equipos de energía portátiles.
- Abastecimiento de combustible para asegurar autonomía operativa.
- Priorización del uso de energía para sistemas críticos (servidores, comunicaciones).

b) Desactivación (retorno a la sede principal o permanente)

La desactivación de la sede alterna corresponde al proceso de cierre de operaciones en el COER y retorno progresivo a la sede principal o a una nueva sede permanente segura.

- Criterios de desactivación
- Seguridad estructural:

Verificación por parte del Grupo de Comando de que la sede de Jr. Loreto es estructuralmente segura o que se ha habilitado una nueva infraestructura adecuada.

- Restablecimiento de servicios:

Confirmación de que los sistemas tecnológicos (servidores, redes) y servicios básicos (energía, comunicaciones) se encuentran plenamente operativos en Huancayo.

- Protocolo de cierre
- Consolidación de la información: Todos los documentos generados durante la operación en la sede alterna deberán ser organizados, foliados y resguardados. Incluye registros administrativos y operativos, así como información registrada en plataformas como SIGRID y SINPAD.
- Traslado de retorno: Se realizará de manera progresiva y planificada, se garantizará que no exista interrupción de los servicios durante el proceso de traslado del personal y recursos desde Concepción hacia Huancayo.





PLAN DE CONTINUIDAD OPERATIVA - 2026

- Reinstalación operativa: Reubicación de equipos, personal y documentación en la sede principal o definitiva.
- Evaluación post-incidente

Una vez concluido el proceso de retorno, el Grupo de Comando elaborará un Informe de Resultados, el cual deberá incluir:

- Evaluación del desempeño del Plan de Continuidad Operativa.
- Identificación de brechas y limitaciones.
- Lecciones aprendidas durante la emergencia.
- Recomendaciones para la actualización y mejora del plan.

5.9 Desarrollo de las actividades críticas:

➤ Gestión tecnológica y de información (Oficina de TI)

Objetivo: Restablecer la conectividad y acceso a sistemas críticos en un plazo no mayor a 4 horas.

Responsable: Jefe de la Oficina de Tecnologías de la Información.

Acciones principales:

- Verificar conectividad a internet y redes de comunicación.
- Habilitar equipos informáticos y acceso a SIGRID y SINPAD.
- Activar sistemas de energía temporal ante la ausencia de grupo electrógeno.
- Recuperar información mediante copias de seguridad (backups).

➤ Monitoreo y respuesta a emergencias (Defensa Civil / COER)

Objetivo: Mantener el monitoreo permanente y coordinar la respuesta en las provincias.

Responsable: Subgerente de Defensa Civil.

Acciones principales:

- Activar el equipo de monitoreo 24/7.
- Consolidar información EDAN de las zonas afectadas.
- Elaborar mapas de daños con herramientas SIG.
- Gestionar el Sistema de Alerta Temprana (SAT).

➤ Gestión administrativa y financiera

Objetivo: Garantizar la disponibilidad de recursos en las primeras 24-48 horas.

Responsables: Director de Administración y Gerente de Planeamiento y Presupuesto.





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



Acciones principales:

- Revisar documentación crítica evacuada.
- Activar recursos del PP0068.
- Ejecutar contrataciones de emergencia.
- Gestionar abastecimiento de bienes de ayuda humanitaria.

➤ Conducción y rehabilitación de infraestructura

Objetivo: Asegurar la toma de decisiones y la rehabilitación de vías afectadas.

Responsables: Gerente General y Gerente de Infraestructura.

Acciones principales:

- Instalar el GTGRD para la toma de decisiones.
- Emitir resoluciones para la atención de la emergencia.
- Desplegar maquinaria pesada para rehabilitación de vías.
- Gestionar apoyo adicional ante el INDECI si es necesario.

VI. CRONOGRAMA DE EJERCICIOS DE CONTINUIDAD OPERATIVA

Actividades	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Aprobación del PCO								
Socialización del PCO								
Sensibilización del personal								
Capacitación técnica								
Simulación de continuidad (15 julio)								
Evaluación preliminar								
Informe de lecciones aprendidas								
Implementación de mejoras								
Verificación de sede alterna								
Evaluación y actualización del PCO								

VII. ANEXOS

Anexo 1. Plan de Recuperación de los servicios informáticos

Anexo 2. Procedimientos para la Convocatoria del Personal involucrado en la ejecución de las Actividades Críticas

Anexo 3. Directorio del Grupo de Comando

Anexo 4. Organización para el desarrollo de las Actividades Críticas

Anexo 5. Sistema de Comunicaciones de Emergencia

Anexo 6. Cronograma para la implementación de la Gestión de la Continuidad Operativa



ANEXO 1: PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS.

En atención al Memorando N.º 915-2026-GRJ/GGR/DRDITI, la Dirección Regional de Desarrollo Institucional y Tecnología de la Información (DRDITI) ha elaborado el **Plan de Recuperación de los Servicios Informáticos**, con el propósito de garantizar la continuidad operativa de los servicios tecnológicos del Gobierno Regional Junín ante eventos que afecten la infraestructura física o tecnológica de la entidad.

El plan establece las acciones, procedimientos y mecanismos necesarios para la recuperación y restablecimiento oportuno de los sistemas informáticos que soportan los procesos críticos institucionales, previamente identificados por las Direcciones de Línea y de Apoyo.

Asimismo, el documento contempla los siguientes componentes:

- Identificación de servicios críticos.
- Análisis de riesgos.
- Estrategias de recuperación y continuidad.
- Procedimientos de respuesta y recuperación ante incidentes.

El Plan de Recuperación de los Servicios Informáticos se adjunta al presente documento y cuenta con una copia de respaldo en el acervo documentario de la Dirección Regional de Desarrollo Institucional y Tecnología de la Información (DRDITI).





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



ANEXO 1: PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS.

ÍNDICE

I. INTRODUCCION:.....	32
II. BASE LEGAL:	33
III. OBJETIVOS:	34
IV. ALCANCE.....	34
V. IDENTIFICACIÓN DE SERVICIOS CRITICOS	35
VI. RIESGOS IDENTIFICADOS.....	37
VII. ESTRATEGIAS DE RECUPERACIÓN.....	45
VIII. PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES	53
IX. RESPONSABLES.....	54
X. RECURSOS NECESARIOS	56
XI. PRUEBAS Y ACTUALIZACIÓN DEL PLAN	58





I. INTRODUCCION:

El Gobierno Regional Junín, en cumplimiento de los principios de continuidad operativa, modernización de la gestión pública y fortalecimiento de la seguridad de la información, reconoce que los servicios informáticos y las tecnologías de la información constituyen recursos estratégicos indispensables para el desarrollo de las funciones institucionales, la gestión administrativa y la prestación eficiente de los servicios públicos a la ciudadanía.

En el contexto actual, caracterizado por una creciente dependencia de la infraestructura tecnológica y de los sistemas de información institucionales, la Entidad se encuentra expuesta a diversos riesgos y amenazas que podrían comprometer la disponibilidad, integridad, confidencialidad y operatividad de los servicios informáticos, tales como fallas de hardware y software, interrupciones de energía eléctrica, incidentes de ciberseguridad, errores humanos, pérdida de conectividad, así como eventos naturales o situaciones de emergencia que afecten el normal funcionamiento de la infraestructura tecnológica institucional.

En atención a ello, el presente Plan de Recuperación de Servicios Informáticos constituye un instrumento de gestión técnico-administrativo orientado a establecer las disposiciones, lineamientos, procedimientos y mecanismos de actuación necesarios para garantizar la recuperación, restauración y restablecimiento oportuno de los servicios informáticos críticos del Gobierno Regional Junín ante situaciones de contingencia, incidentes o desastres que afecten la continuidad operativa institucional.

Asimismo, el presente documento define las responsabilidades funcionales, las estrategias de contingencia, los mecanismos de respaldo y recuperación de información, así como las acciones de respuesta y rehabilitación tecnológica destinadas a minimizar el impacto operativo, administrativo y funcional derivado de eventos adversos, asegurando la continuidad de los procesos institucionales y la adecuada prestación de los servicios públicos, en concordancia con la





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



normativa vigente en materia de gobierno digital, seguridad de la información y gestión de continuidad operativa en las entidades de la administración pública.

II. BASE LEGAL:

- Constitución Política del Perú.
- Ley N.º 32513, Ley de Presupuesto del Sector Público para el Año Fiscal 2026.
- Resolución Ejecutiva Regional que aprueba el Presupuesto Institucional de Apertura (PIA) 2026 del Gobierno Regional de Junín.
- Resolución Ministerial N.º 320-2021-PCM.
- Ley N.º 27658 – Ley Marco de Modernización de la Gestión del Estado.
- Decreto Legislativo N.º 1554, Modifica la Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado
- Ley N.º 29733 – Ley de Protección de Datos Personales.
- Ley N.º 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N.º 048-2011-PCM, que aprueba el Reglamento de la Ley N.º 29664.
- Decreto Supremo N.º 060-2024-PCM, que modifica el Reglamento de la Ley N.º 29664
- Decreto Supremo N.º 034-2014-PCM, que modifica el Reglamento de la Ley N.º 29664.
- Decreto Supremo N.º 111-2012-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres.
- Decreto Supremo N.º 038-2021-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022-2030.
- Resolución Ministerial N.º 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la formulación de los Planes de Continuidad Operativa (PCO).





III. OBJETIVOS:

Establecer las disposiciones normativas, lineamientos institucionales, procedimientos técnicos especializados y mecanismos de respuesta necesarios para garantizar la recuperación, restauración y restablecimiento oportuno y eficiente de los servicios informáticos críticos del Gobierno Regional Junín, asegurando la continuidad operativa de los procesos estratégicos, misionales, administrativos y de soporte de la Entidad ante la ocurrencia de incidentes de seguridad de la información, fallas de infraestructura tecnológica, interrupciones de servicios, ciberataques, errores operativos, desastres naturales o cualquier evento adverso que pueda comprometer la disponibilidad, integridad, confidencialidad y operatividad de los sistemas de información, plataformas digitales, redes de comunicación, infraestructura tecnológica y demás recursos informáticos institucionales.

Contribuyendo de esta manera a minimizar el impacto operativo, administrativo, funcional y reputacional, así como a garantizar el adecuado cumplimiento de los objetivos institucionales, funciones y competencias asignadas al Gobierno Regional Junín, en concordancia con la normativa vigente en materia de gobierno digital, seguridad de la información y continuidad operativa en la administración pública.

IV. ALCANCE

El presente Plan de Recuperación de Servicios Informáticos es de aplicación obligatoria para todas las dependencias, órganos y unidades orgánicas del Gobierno Regional Junín que utilizan, administran o brindan soporte a los servicios tecnológicos e informáticos institucionales.



Comprende la protección, recuperación y restablecimiento de los activos tecnológicos críticos, esto incluye:

- Infraestructura de Tecnologías de la información
- Servidores físicos y/o virtuales
- Sistemas de información institucionales
- Bases de datos
- Plataformas digitales
- Redes y comunicaciones
- Servicios de conectividad
- Correo electrónico institucional
- Equipos de cómputo

Asimismo, el presente plan abarca las acciones de prevención, respuesta, contingencia, recuperación y restauración frente a incidentes de seguridad de la información, fallas tecnológicas, errores operativos, interrupciones de servicios, ataques informáticos, desastres naturales y cualquier evento que pueda afectar la disponibilidad, integridad y operatividad de los servicios informáticos institucionales.

V. IDENTIFICACIÓN DE SERVICIOS CRÍTICOS

La identificación de los servicios informáticos críticos permite determinar aquellos recursos tecnológicos y sistemas de información cuya interrupción podría afectar significativamente la continuidad operativa, administrativa y funcional del Gobierno Regional Junín, comprometiendo el cumplimiento de sus funciones institucionales y la prestación de los servicios públicos.

En ese sentido, se consideran servicios críticos aquellos cuya disponibilidad resulta indispensable para el normal desarrollo de las actividades institucionales y cuya recuperación debe ejecutarse con carácter prioritario ante situaciones de contingencia o desastre.

Servicios Informáticos Críticos Identificados





GOBIERNO REGIONAL JUNÍN

PLAN DE CONTINUIDAD OPERATIVA - 2026



Nº	Servicio Informático Crítico	Descripción	Nivel de Criticidad	Tiempo Objetivo de Recuperación (RTO)
1	Sistema de Trámite Documentario	Plataforma utilizada para el registro, seguimiento y gestión de documentos institucionales.	CRITICO	4 horas
2	Servidor de Base de Datos Institucional	Servicio que almacena y administra la información crítica institucional.	CRITICO	2 hora
3	Servicio de Correo Electrónico Institucional	Medio oficial de comunicación interna y externa de la Entidad.	CRITICO	6 horas
4	Servicios de Red y Conectividad	Infraestructura de red, internet y comunicaciones institucionales.	CRITICO	4 horas
5	Plataforma Web Institucional	Portal institucional y servicios digitales orientados a la ciudadanía.	CRITICO	8 horas
6	Sistema de Gestión Administrativa	SIGA -SIAF	CRITICO	6 horas



7	Servicios de Virtualización	Plataforma destinada a la generación y restauración de copias de seguridad.	CRITICO	4 horas
8	Servicios de Seguridad Informática	Antivirus corporativo, firewall, monitoreo y control de accesos.	CRITICO	4 horas

• **CLASIFICACIÓN DE CRITICIDAD**

- Crítico: Servicios indispensables cuya interrupción afecta directamente la continuidad operativa institucional y requiere recuperación inmediata.
- Alto: Servicios necesarios para el adecuado funcionamiento institucional, cuya interrupción genera impacto significativo en las operaciones.
- Medio: Servicios complementarios cuya afectación no compromete de manera inmediata las funciones esenciales de la Entidad.



VI. RIESGOS IDENTIFICADOS

En el marco del Plan de Recuperación de Servicios Informáticos, se han identificado los riesgos que podrían afectar la continuidad operativa de los servicios tecnológicos del Gobierno Regional Junín, comprometiendo la disponibilidad, integridad y confidencialidad de la información institucional.

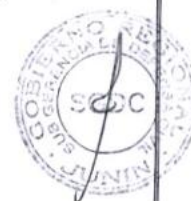
La identificación de estos riesgos permite establecer mecanismos de prevención, respuesta y recuperación orientados a minimizar el impacto de eventos adversos sobre los procesos críticos de la entidad.



- **RIESGOS DE INFRAESTRUCTURA TECNOLÓGICA**

Este tipo de Riesgos se refiere a los posibles eventos relacionados con la indisponibilidad o deterioro de los componentes de hardware, estos pueden ser:

- Fallas de hardware en servidores, equipos de almacenamiento, dispositivos de red o infraestructura tecnológica crítica.
- Errores o fallas de software que ocasionen la interrupción de aplicaciones y servicios institucionales.
- Corrupción, pérdida o alteración de bases de datos y archivos de información.
- Obsolescencia de hardware que limite la capacidad de recuperación de los servicios.
- Fallas de servidores físicos o virtuales.
- Pérdida de información por errores de software.
- Fallas de almacenamiento (discos).
- Interrupciones de servicios en la nube.
- Obsolescencia o software crítico.



- **RIESGOS DE SUMINISTRO ELÉCTRICO**

Son aquellos eventos que puedan afectar la disponibilidad, estabilidad y continuidad del suministro de energía eléctrica requerido para la operación de la infraestructura tecnológica institucional.

La ocurrencia de dichos eventos puede ocasionar la indisponibilidad de los sistemas de información, la interrupción de los servicios tecnológicos y afectar la continuidad de las operaciones institucionales, comprometiendo la integridad de los datos y la continuidad de los procesos institucionales críticos.

En este contexto, se identifican los siguientes riesgos:



PLAN DE CONTINUIDAD OPERATIVA - 2026

- Interrupciones prolongadas, recurrentes o imprevistas del suministro eléctrico provenientes de la red de distribución externa.
- Fallas, insuficiencia operativa o indisponibilidad de los sistemas de respaldo energético, incluyendo sistemas de alimentación ininterrumpida (UPS), bancos de baterías y grupos electrógenos.
- Variaciones de tensión eléctrica, sobretensiones, caídas de voltaje y otras anomalías en la calidad del suministro que puedan ocasionar daños o afectaciones en los equipos tecnológicos.
- Deficiencias en la infraestructura eléctrica interna que limiten la adecuada alimentación de los recursos tecnológicos críticos.
- Capacidad insuficiente de los mecanismos de respaldo para garantizar la continuidad operativa durante períodos prolongados de contingencia.



• **RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

Eventos que comprometan la confidencialidad, integridad o disponibilidad de la información institucional del Gobierno Regional Junín, esto puede incluir:

- Accesos no autorizados
- Fuga de información, Pérdida, Divulgación o manipulación indebida de información sensible o crítica.
- Vulneración de sistemas críticos.
- Ataques cibernéticos, incluyendo ransomware, malware, phishing
- Vulneración de sistemas debido a configuraciones inseguras o explotación de vulnerabilidades.

• **RIESGOS DE FALLAS EN LOS SERVICIOS DE TELECOMUNICACIONES**

Comprenden aquellos eventos que afecten la disponibilidad, capacidad, estabilidad o calidad de los servicios de telecomunicaciones necesarios para el funcionamiento de la infraestructura tecnológica institucional. La



materialización de estos riesgos puede ocasionar interrupciones en la conectividad, afectar el acceso a los sistemas de información y limitar la prestación de los servicios tecnológicos que soportan las actividades institucionales, se identifican los siguientes riesgos:

- Interrupciones parciales o totales de los servicios de conectividad a Internet proporcionados por operadores externos.
- Fallas en los enlaces de comunicación de datos que interconectan sedes, centros de datos y servicios externos.
- Saturación de ancho de banda, bajo rendimiento de la red debido a congestión, o deficiencias en la infraestructura de comunicaciones.
- Fallas en equipos de red, tales como routers, switches, firewalls, puntos de acceso inalámbrico y demás componentes de telecomunicaciones.
- Interrupciones de servicios de telecomunicaciones ocasionadas por incidentes en la infraestructura de proveedores externos.
- Configuraciones inadecuadas o errores operativos que afecten la disponibilidad y el desempeño de los servicios de red.
- Daños físicos en medios de transmisión, cableado estructurado, fibra óptica o equipamiento de comunicaciones.

• **RIESGOS DE ERRORES OPERATIVOS Y HUMANOS**

Corresponde a eventos originados por acciones involuntarias, omisiones o procedimientos inadecuados ejecutados por el personal responsable de la administración, operación, soporte o mantenimiento de los sistemas de información y la infraestructura tecnológica, estos pueden ser:

- Errores humanos durante la operación, administración o mantenimiento de sistemas.
- Eliminación accidental o modificación no autorizada de datos.



- Ejecución incorrecta o incompleta de procedimientos de respaldo y recuperación.
- Ausencia o indisponibilidad de personal clave durante situaciones de contingencia.
- Uso de procedimientos, manuales o documentación técnica desactualizada.
- Configuración incorrecta de servidores, aplicaciones, bases de datos o equipos de red.

• **RIESGOS DE DEPENDENCIA DE PROVEEDORES EXTERNOS**

Son eventos asociados a la indisponibilidad, incumplimiento, suspensión o interrupción de los servicios prestados por proveedores externos que soportan la operación de los servicios informáticos institucionales, incluyendo servicios de telecomunicaciones, conectividad a Internet, alojamiento de sistemas, licenciamiento y otros recursos críticos para la continuidad operativa de la entidad. La materialización de este riesgo puede afectar la disponibilidad de los sistemas de información, limitar la capacidad de respuesta ante incidentes y generar interrupciones en los servicios esenciales brindados a los usuarios internos y externos.

- Incumplimiento de los Acuerdos de Nivel de Servicio (SLA) establecidos contractualmente.
- Interrupción o disminución de los servicios de telecomunicaciones y conectividad.
- Quiebra, cierre de operaciones o indisponibilidad de proveedores críticos.
- Dependencia excesiva de un único proveedor para servicios esenciales.
- Retrasos en la atención de incidentes o requerimientos de soporte técnico especializado.





- Incumplimiento de contratos de mantenimiento preventivo y correctivo.
- Suspensión de servicios por vencimiento contractual o falta de renovación oportuna.
- Fallas en plataformas de servicios en la nube o centros de datos externos.
- Restricciones de acceso a recursos, licencias o servicios administrados por terceros.

• **RIESGOS DE EVENTOS NATURALES Y ANTRÓPICOS**

Comprende la ocurrencia de fenómenos naturales o eventos originados por la acción humana que puedan afectar total o parcialmente la infraestructura tecnológica, las instalaciones físicas, los sistemas de información, las comunicaciones y los recursos necesarios para la continuidad de los servicios informáticos dentro del Gobierno Regional Junín y limitaciones para el acceso del personal responsable de la operación y recuperación de los servicios.

- Incendios que afecten las instalaciones, centros de datos o áreas donde se encuentra la infraestructura tecnológica.
- Inundaciones ocasionadas por fenómenos climáticos, fallas en sistemas de drenaje o roturas de tuberías.
- Sismos u otros desastres naturales que comprometan la infraestructura física y tecnológica.
- Cortes prolongados de servicios básicos derivados de emergencias o desastres.
- Actos de vandalismo, sabotaje o daños intencionales contra los activos tecnológicos de la entidad.
- Disturbios sociales, conflictos internos o situaciones de orden público que afecten el normal funcionamiento del Gobierno Regional Junín.





- Emergencias sanitarias, epidemias o pandemias que restrinjan la presencia física del personal.
- Eventos extraordinarios que impidan el acceso a las instalaciones institucionales o a los centros de procesamiento de datos.

• **RIESGOS DE INSUFICIENCIA O FALLO DE LOS MECANISMOS DE RESPALDO Y RECUPERACIÓN**

Viene a ser la posibilidad de que las copias de seguridad, procedimientos de recuperación, infraestructura alterna, recursos de contingencia o mecanismos implementados para la continuidad de los servicios informáticos resulten insuficientes, ineficaces o indisponibles al momento de una contingencia.

La materialización de este riesgo puede generar pérdida parcial o total de información, interrupciones prolongadas de los servicios críticos, incumplimiento de los objetivos de recuperación (RTO) y pérdida de disponibilidad de los sistemas que soportan los procesos institucionales.

- Generación de copias de seguridad incompletas, corruptas o no verificadas.
- Fallas en los procesos de respaldo automático o manual.
- Imposibilidad de restaurar la información dentro de los tiempos de recuperación definidos por la entidad.
- Ausencia de procedimientos documentados y actualizados para la recuperación de servicios.
- Falta de pruebas periódicas que validen la efectividad de los mecanismos de respaldo y recuperación.
- Indisponibilidad de los sitios alternos o de la infraestructura destinada a la continuidad operativa.
- Pérdida, deterioro o inaccesibilidad de los medios de almacenamiento utilizados para los respaldos.





- Capacidad insuficiente de almacenamiento para la conservación de copias de seguridad.
- Dependencia de personal especializado para ejecutar procesos de recuperación.
- Incompatibilidad entre los respaldos disponibles y las plataformas tecnológicas requeridas para su restauración.

VALORACIÓN GENERAL DEL RIESGO

Los riesgos identificados en la presente, se encuentran asociados a factores tecnológicos, operativos, humanos, ambientales y externos que podrían afectar la disponibilidad, integridad y continuidad de los servicios informáticos que soportan los procesos críticos de la entidad.

Considerando que los sistemas de información, las plataformas tecnológicas, los servicios de comunicaciones y la infraestructura informática constituyen recursos estratégicos para el cumplimiento de los objetivos institucionales y la prestación de los servicios a los ciudadanos, la materialización de cualquiera de los riesgos identificados podría generar impactos significativos en la operatividad institucional, el acceso a la información, la continuidad de los procesos administrativos y la atención de los servicios públicos.

En tal sentido, la valoración general de los riesgos se considera con un impacto de media a alta, dependiendo de la naturaleza de los activos afectados, el nivel de dependencia de los servicios comprometidos y el tiempo requerido para su recuperación. Por ello, resulta indispensable la implementación y mantenimiento de controles preventivos, detectivos, correctivos y de recuperación orientados a reducir la probabilidad de ocurrencia de incidentes y minimizar sus efectos sobre la operación institucional.





Asimismo, la entidad deberá asegurar la disponibilidad de recursos humanos, tecnológicos, financieros y organizacionales que permitan ejecutar oportunamente las acciones de contingencia y recuperación previstas en el presente Plan, garantizando el restablecimiento de los servicios informáticos dentro de los tiempos de recuperación definidos.

La identificación, evaluación, monitoreo y tratamiento de riesgos constituye una actividad permanente dentro del proceso de gestión de continuidad operativa y recuperación de servicios informáticos; por lo que el presente análisis deberá ser revisado y actualizado periódicamente, o cuando se produzcan cambios significativos en la infraestructura tecnológica, los procesos institucionales, el entorno operativo o el marco normativo aplicable, con la finalidad de mantener su vigencia, efectividad y alineamiento con los objetivos estratégicos del Gobierno Regional Junín.



VII. ESTRATEGIAS DE RECUPERACIÓN

Las estrategias de recuperación deberán asegurar la continuidad de los servicios informáticos institucionales y garantizar la recuperación oportuna de los recursos tecnológicos ante la ocurrencia de incidentes, contingencias o desastres que comprometan la operatividad de la entidad, se establecen las siguientes estrategias de recuperación, las cuales deberán ser ejecutadas de manera coordinada por las áreas responsables de la gestión y administración de las tecnologías de la información, Las estrategias de recuperación deberán estar orientadas a:

- ✓ Proteger la información institucional y garantizar su disponibilidad, integridad y confidencialidad.
- ✓ Restablecer prioritariamente los servicios informáticos considerados críticos para la operación institucional.
- ✓ Minimizar los tiempos de interrupción de los servicios tecnológicos.



- ✓ Reducir el impacto operativo, financiero y reputacional generado por una contingencia.
- ✓ Garantizar la continuidad de los procesos institucionales esenciales.
- ✓ Optimizar el uso de los recursos humanos, tecnológicos y financieros disponibles durante la recuperación.

- **ESTRATEGIAS DE RECUPERACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA**

- Activación de equipos de respaldo o sustitución temporal de equipos afectados.
- Reconfiguración de servidores, dispositivos de red y servicios esenciales.
- Utilización de infraestructura alternativa disponible para garantizar la continuidad operativa.
- Restablecimiento progresivo de los servicios de acuerdo con el nivel de criticidad definido.
- Coordinación con proveedores para la reposición o reparación de equipos afectados.



- **ESTRATEGIAS DE RECUPERACIÓN DEL SUMINISTRO ELÉCTRICO**

- Activar los sistemas de respaldo energético disponibles ante la interrupción del suministro eléctrico comercial.
- Ejecutar procedimientos de apagado controlado de servidores y equipos críticos cuando el tiempo de autonomía de los sistemas UPS resulte insuficiente para mantener la operación.
- Verificar el estado de los equipos tecnológicos una vez restablecido el suministro eléctrico, asegurando la integridad de los sistemas antes de su puesta en funcionamiento.
- Restablecer progresivamente los servicios informáticos de acuerdo con el orden de prioridad definido por la entidad.



- Validar el correcto funcionamiento de las bases de datos, aplicaciones, servicios de red y sistemas de almacenamiento luego de la recuperación.
- Registrar y documentar los eventos ocurridos, así como las acciones ejecutadas durante el proceso de recuperación.

- **ESTRATEGIAS DE RECUPERACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

- Restaurar la información y los servicios afectados utilizando respaldos previamente validados.
- Reconfigurar los sistemas comprometidos y corregir las vulnerabilidades identificadas.
- Restablecer gradualmente los servicios informáticos, priorizando aquellos considerados críticos para la operación institucional.
- Verificar la integridad, disponibilidad y correcto funcionamiento de los sistemas recuperados antes de su reincorporación al entorno operativo.
- Validar que las medidas correctivas implementadas eliminen o mitiguen las causas que originaron el incidente.
- Mantener un monitoreo reforzado de los servicios recuperados para detectar posibles eventos recurrentes o residuales.



- **ESTRATEGIAS DE RECUPERACIÓN DE SISTEMAS DE INFORMACIÓN**

- Restauración de aplicaciones y plataformas desde respaldos previamente validados.
- Recuperación de configuraciones, parámetros y componentes críticos de los sistemas.



- Validación funcional de los sistemas antes de su puesta en producción.
- Priorización de la recuperación de los sistemas que soportan procesos críticos institucionales.
- Monitoreo permanente del desempeño y estabilidad de los servicios recuperados.
- Ejecución periódica de copias de seguridad de bases de datos, sistemas, configuraciones y documentos electrónicos.
- Almacenamiento de respaldos en medios seguros y ubicaciones alternas.
- Verificación periódica de la integridad de las copias de seguridad.
- Restauración de la información utilizando los respaldos más recientes y validados.
- Validación de la consistencia e integridad de los datos recuperados.

• **ESTRATEGIAS DE RECUPERACIÓN DE SERVICIOS DE TELECOMUNICACIONES**

- Activar los enlaces de comunicación alternos ante la interrupción del enlace principal de telecomunicaciones.
- Coordinar de manera inmediata con los proveedores de servicios la atención y resolución de incidencias que afecten la conectividad institucional.
- Reconfigurar los equipos de red (routers, switches, firewalls u otros) para la utilización de rutas alternativas de comunicación.
- Priorizar la recuperación de los servicios de red críticos que soportan sistemas de información esenciales para la entidad.
- Habilitar mecanismos alternativos de comunicación institucional (telefonía móvil, mensajería segura u otros canales autorizados) durante la contingencia.





- Verificar progresivamente la restauración de los servicios de conectividad antes de su normalización operativa.

- **ESTRATEGIAS DE RECUPERACIÓN DE ERRORES OPERATIVOS Y HUMANOS**

- Identificar el alcance del error operativo o humano y determinar los sistemas o información afectada.
- Detener o revertir las operaciones que hayan generado la incidencia, cuando ello sea técnicamente posible.
- Restaurar la información afectada a partir de copias de seguridad previamente validadas.
- Revertir configuraciones o cambios mediante el uso de respaldos de configuración o versiones anteriores de los sistemas.
- Validar la integridad y consistencia de la información recuperada antes de su reincorporación al entorno de producción.
- Reprocesar las transacciones afectadas, cuando corresponda, con la finalidad de restablecer la continuidad operativa.
- Coordinar con las áreas usuarias la verificación de la información restaurada y la confirmación de la normalización del servicio.
- **RECUPERACIÓN DEL PERSONAL**
 - Designación de personal titular y alterno para cada función crítica.
 - Disponibilidad de directorios de contacto actualizados.
 - Capacitación periódica del personal involucrado en la recuperación de servicios.
 - Implementación de mecanismos de trabajo remoto cuando las condiciones de la contingencia lo requieran.
 - Transferencia y documentación del conocimiento técnico para evitar dependencias de personal específico.





- **ESTRATEGIAS DE RECUPERACIÓN DE DEPENDENCIA DE PROVEEDORES EXTERNOS**

- Activar los procedimientos contractuales establecidos ante incumplimientos, caídas del servicio o indisponibilidad de proveedores.
- Escalar de manera inmediata los incidentes conforme a los canales formales de atención definidos en los contratos o SLA.
- Coordinar con proveedores alternos previamente identificados la provisión temporal del servicio afectado, cuando sea viable.
- Implementar soluciones de contingencia internas o temporales que permitan la continuidad mínima de los servicios críticos.
- Migrar temporal o definitivamente los servicios afectados hacia plataformas alternativas o infraestructura institucional, de ser posible.
- Priorizar la recuperación de los servicios esenciales para la continuidad de los procesos institucionales.



- **ESTRATEGIAS DE RECUPERACIÓN DE EVENTOS NATURALES Y ANTRÓPICOS**

- Activar de manera inmediata el Plan de Recuperación de Servicios Informáticos ante la ocurrencia del evento.
- Evaluar el nivel de afectación de la infraestructura tecnológica, servicios de información y comunicaciones.
- Priorizar la recuperación de los servicios críticos para la operación institucional.
- Trasladar la operación a infraestructura alterna o entornos de contingencia previamente establecidos, cuando corresponda.
- Restaurar la información institucional a partir de copias de seguridad disponibles y validadas.



- Coordinar la rehabilitación de los ambientes físicos afectados con las áreas competentes de infraestructura y gestión de riesgos.
 - Habilitar mecanismos de acceso remoto seguro para la continuidad de las operaciones, cuando las condiciones lo permitan.
 - Comunicar de manera oportuna el estado de los servicios a las áreas usuarias y autoridades competentes.
-
- **ESTRATEGIAS DE RECUPERACIÓN DE INSUFICIENCIA O FALLO DE LOS MECANISMOS DE RESPALDO Y RECUPERACIÓN**
 - Identificar el alcance del fallo en los mecanismos de respaldo, determinando los sistemas y periodos de información afectados.
 - Activar mecanismos alternativos de recuperación de información disponibles, incluyendo respaldos históricos, copias redundantes o repositorios secundarios.
 - Restaurar los sistemas y bases de datos a partir de las copias de seguridad válidas más recientes.
 - Validar la integridad, consistencia y completitud de la información recuperada antes de su reincorporación al entorno productivo.
 - Priorizar la recuperación de los servicios críticos conforme a su nivel de impacto institucional.
 - Coordinar con los usuarios responsables la verificación funcional de los sistemas restaurados.
 - Documentar las incidencias ocurridas durante el proceso de recuperación para su análisis posterior.

 - **ESTRATEGIAS DE RECUPERACIÓN MEDIANTE SITIOS ALTERNOS**
 - Cuando la magnitud del incidente impida operar desde las instalaciones principales, se podrá considerar:





- Utilización de ambientes alternos para la operación temporal de los servicios críticos.
- Habilitación de infraestructura tecnológica de contingencia.
- Uso de servicios en la nube o plataformas externas si es que las hubiera
- Implementación de mecanismos de acceso remoto seguro para usuarios y administradores.

PRIORIZACIÓN DE LA RECUPERACIÓN

La recuperación de los servicios informáticos deberá realizarse de manera progresiva y priorizada, en función del nivel de criticidad de los servicios y su impacto en la continuidad de las operaciones institucionales, conforme al orden que se detalla a continuación:

- Servicios de red y comunicaciones.
- Servicios de autenticación y directorio institucional.
- Bases de datos institucionales.
- Sistemas de gestión documental y trámite documentario.
- Sistemas administrativos y financieros.
- Servicios de correo electrónico institucional.
- Portales web y servicios de atención al ciudadano.
- Otros servicios de apoyo institucional.

La priorización podrá ser ajustada de acuerdo con el impacto operativo y las necesidades institucionales identificadas durante la contingencia. Las estrategias de recuperación deberán ser evaluadas periódicamente mediante pruebas, simulacros y revisiones técnicas, con el fin de verificar su efectividad, identificar oportunidades de mejora y asegurar su alineamiento con la infraestructura tecnológica, los procesos institucionales y los riesgos vigentes.





VIII. PROCEDIMIENTO DE RESPUESTA ANTE INCIDENTES

El procedimiento de respuesta ante incidentes se aplicará a todos los sistemas de información, servidores, redes, aplicaciones, bases de datos, servicios en la nube, estaciones de trabajo y recursos tecnológicos utilizados por el Gobierno Regional Junín, podemos definir algunos términos:

- **Incidente:** Evento que afecta o puede afectar la confidencialidad, integridad o disponibilidad de los activos de información.
- **Incidente Crítico:** Evento que genera interrupción total o parcial de servicios esenciales para la operación institucional.
- **Recuperación:** Proceso de restauración de servicios y sistemas a su estado operativo normal.
- **Equipo de Respuesta ante Incidentes:** Grupo responsable de gestionar y coordinar las acciones de respuesta y recuperación.

COMUNICACIÓN DEL INCIDENTE

- **Comunicación Interna**
 - Responsable de TI.
 - Dirección o Gerencia.
 - Usuarios afectados.
- **Comunicación Externa**
 - Proveedores tecnológicos.
 - Entidades reguladoras (cuando aplique).
 - Clientes o usuarios externos afectados.

DOCUMENTACIÓN Y CIERRE

Al finalizar el incidente se deberá elaborar un informe que incluya:

- Fecha y hora del incidente.
- Descripción del evento.
- Servicios afectados.
- Causa raíz identificada.
- Acciones realizadas.



- Tiempo total de recuperación.
- Impacto generado.
- Lecciones aprendidas.
- Acciones preventivas y correctivas.

IX. RESPONSABLES

GERENCIA REGIONAL GENERAL

- Aprobar la activación del Plan de Recuperación de Servicios Informáticos cuando la magnitud del incidente lo requiera.
- Proporcionar el respaldo institucional y los recursos necesarios para la ejecución de las actividades de recuperación.
- Supervisar el restablecimiento de los servicios críticos que soportan los procesos institucionales.



OFICINA REGIONAL DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍA DE LA INFORMACIÓN

- Administrar, mantener y actualizar el Plan de Recuperación de Servicios Informáticos.
- Coordinar las acciones de respuesta, recuperación y restablecimiento de los servicios tecnológicos afectados.
- Evaluar el impacto de los incidentes y determinar las prioridades de recuperación.
- Informar oportunamente a la Alta Dirección sobre el estado de los servicios afectados y las acciones implementadas.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Participar en la gestión y análisis de los incidentes que afecten la seguridad de la información.
- Coordinar la identificación de las causas del incidente y las medidas de mitigación correspondientes.



- Verificar que las acciones de recuperación no comprometan la confidencialidad, integridad y disponibilidad de la información institucional.

ADMINISTRADORES DE SISTEMAS Y BASES DE DATOS

- Ejecutar las actividades de recuperación de servidores, aplicaciones, bases de datos y plataformas tecnológicas.
- Restaurar la información institucional a partir de los respaldos disponibles y validados.
- Verificar la integridad y operatividad de los sistemas recuperados.

ADMINISTRADORES DE REDES Y COMUNICACIONES

- Restablecer los servicios de conectividad y comunicaciones institucionales.
- Implementar medidas de contención y recuperación en la infraestructura de red afectada.
- Monitorear la estabilidad de los servicios de comunicación durante el proceso de recuperación.
- Propietarios de los Sistemas de Información
- Validar la correcta operación de los sistemas y servicios recuperados.
- Participar en las pruebas funcionales posteriores a la recuperación.
- Comunicar los requerimientos de continuidad de los procesos bajo su responsabilidad.

USUARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Reportar oportunamente incidentes o interrupciones de los servicios informáticos.
- Colaborar con las actividades de recuperación cuando sea requerido.



- Cumplir las disposiciones emitidas por la Oficina Regional de Tecnologías de la Información y Comunicaciones durante la atención del incidente.

EQUIPO DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

- Ejecutar las actividades definidas en el presente Plan.
- Coordinar la recuperación de los servicios tecnológicos afectados de acuerdo con los niveles de prioridad establecidos.
- Documentar las acciones realizadas, los resultados obtenidos y las lecciones aprendidas derivadas del incidente.

X. RECURSOS NECESARIOS

Para garantizar la ejecución efectiva del Plan de Recuperación de Servicios Informáticos, el Gobierno Regional Junín deberá disponer de los recursos humanos, tecnológicos, de infraestructura y de soporte necesarios para la atención de incidentes y la recuperación oportuna de los servicios afectados.

RECURSOS HUMANOS

Se deberá de contar con personal técnico y administrativo debidamente designado para participar en las actividades de respuesta y recuperación, entre ellos:

- Director de la Oficina Regional Desarrollo Institucional y Tecnología de la Información.
- Responsable de Seguridad de la Información.
- Administradores de sistemas y servidores.
- Administradores de bases de datos.
- Administradores de redes y comunicaciones.
- Personal de soporte técnico.
- Responsables funcionales de los sistemas de información.
- Proveedores especializados cuando la situación lo requiera.





RECURSOS TECNOLÓGICOS

- Servidores físicos y/o virtuales para la restauración de servicios.
- Equipos de almacenamiento para la recuperación de información.
- Sistemas de respaldo y recuperación de datos.
- Equipos de comunicaciones y conectividad de red.
- Estaciones de trabajo para la gestión de incidentes.
- Herramientas de monitoreo y administración de infraestructura tecnológica.
- Herramientas de seguridad informática para la detección y mitigación de incidentes.
- Software de gestión de respaldos y recuperación.
- Licencias de software necesarias para la operación de los servicios institucionales.



RECURSOS DE INFRAESTRUCTURA

- Centro de datos institucional o infraestructura tecnológica equivalente.
- Sistemas de energía eléctrica y respaldo energético (UPS y grupos electrógenos, según corresponda).
- Sistemas de climatización para ambientes tecnológicos.
- Acceso seguro a las instalaciones donde se encuentran los recursos tecnológicos.
- Espacios físicos alternos para la continuidad de las operaciones, cuando resulte necesario.

RECURSOS DE INFORMACIÓN

- Inventario de activos tecnológicos.
- Inventario de sistemas de información institucionales.
- Inventario de servidores y equipos de comunicaciones.
- Procedimientos de recuperación y restauración de servicios.



- Planes de contingencia y continuidad operativa.
- Manuales técnicos y documentación de configuración.
- Directorio de contactos de emergencia y proveedores.

RECURSOS DE COMUNICACIONES

- Correo electrónico institucional.
- Telefonía fija y móvil.
- Herramientas de mensajería y colaboración autorizadas por la entidad.
- Directorio actualizado de responsables internos y proveedores externos.
- Mecanismos alternativos de comunicación en caso de indisponibilidad de los servicios principales.

RECURSOS FINANCIEROS

- La contratación de servicios especializados de soporte o recuperación.
- La adquisición o reposición de equipamiento tecnológico.
- La renovación de licencias y servicios críticos.
- La ejecución de acciones de recuperación ante incidentes de alta criticidad.
- La implementación de mejoras derivadas de las lecciones aprendidas y evaluaciones posteriores a los incidentes.



XI. PRUEBAS Y ACTUALIZACIÓN DEL PLAN

Realizar pruebas semestrales de recuperación.

- Actualizar el plan anualmente o cuando exista cambio tecnológico relevante.
- Registrar incidencias y resultados de pruebas.



ANEXO 2: PROCEDIMIENTO PARA LA CONVOCATORIA DEL PERSONAL INVOLUCRADO EN LA EJECUCIÓN DE LAS ACTIVIDADES CRÍTICAS.

Los procedimientos de comunicación han sido diseñados para operar con capacidad y efectividad. Las prioridades de empleo de medios serán:

- a. Telefonía Celular y fija.
- b. Mensajes de WhatsApp y/o de texto por celular.
- c. Redes sociales y correos electrónicos.
- d. Radiofonía.

Los medios señalados en los literales a) y b) deberán utilizarse de manera simultánea para garantizar la recepción de las comunicaciones y la rápida activación del personal convocado.

1. Procedimiento de reporte inicial

El reporte inicial se efectuará una vez identificado el evento que afecte la continuidad de las operaciones y comprenderá la comunicación entre las siguientes instancias:

- a. Subgerencia de Defensa Civil (SGDC)
- b. Gobernación Regional (GR)
- c. Oficina Regional de Administración y Finanzas
- d. Dirección Regional de Desarrollo Institucional y Tecnología de la Información (DRDITI)

2. Procedimiento de convocatoria

Activado el PCO, se procederá a la convocatoria inmediata del personal involucrado mediante los medios de comunicación prioritarios establecidos. Los mensajes emitidos deberán ser claros, breves y contener las instrucciones necesarias para la movilización del personal.

La disposición inicial de la convocatoria estará a cargo de quien presida el Grupo de Comando o de su representante, de acuerdo con la línea de sucesión establecida, a través del Coordinador del COER Junín (Jefe de la Subgerencia de Defensa Civil).

Las cadenas de convocatoria serán las siguientes:

- a. **Grupo de Comando:** La convocatoria será realizada por quien preside el Grupo de Comando o por quien asuma dicha función conforme a la línea de sucesión establecida.





b. **Personal clave:** La convocatoria será efectuada por los directores o responsables de cada área al personal encargado de implementar y restablecer las actividades críticas bajo su responsabilidad

CONVOCATORIA	MENSAJE	A LA RECEPCIÓN DEL MENSAJE
GRUPO DE COMANDO	Reunión del Grupo de Comando	El personal integrante del Grupo de Comando del Gobierno Regional Junín deberá encontrarse en las inmediaciones del Centro de Operaciones de Emergencia regional - COER (Carretera Chimpamarca S/N) sede alterna.
PERSONAL CLAVE	Reunión del Personal Clave	El personal integrante del Grupo de Comando del Gobierno Regional Junín deberá encontrarse en las inmediaciones del Centro de Operaciones de Emergencia regional - COER (Carretera Chimpamarca S/N) sede alterna.



El presente procedimiento forma parte integrante del Plan de Continuidad Operativa y será aplicado ante la ocurrencia de eventos que comprometan el normal funcionamiento de las operaciones institucionales.

**GOBIERNO REGIONAL JUNÍN****PLAN DE CONTINUIDAD OPERATIVA - 2026****ANEXO 03. DIRECTORIO DEL GRUPO DE COMANDO**

N°	UNIDAD ORGANICA	REPRESENTANTE	Correo Institucional
01	OFICINA REGIONAL DE ADMINISTRACIÓN Y FINANZAS	CPC. IRIS POVIS RAMOS	ipovis@regionjunin.gob.pe
02	OFICINA REGIONAL DE DESARROLLO INSTITUCIONAL DE TECNOLOGÍA DE LA INFORMACIÓN	ING. EDWIN ERNESTO RAMON QUISPE	eramon@regionjunin.gob.pe
03	OFICINA REGIONAL DE COMUNICACIONES	LIC. FLOR BEHTSI ASPARREN BROCOS	fasparren@regionjunin.gob.pe
04	GERENCIA DE PLANEAMIENTO Y ACONDICIONAMIENTO TERRITORIAL	MG. PERCY DAVID TIZA FELIX	ptiza@regionjunin.gob.pe
05	SUB GERENCIA DE DEFENSA CIVIL	ARQ. JOSE AUGUSTO VASQUEZ LOAIZA	jvasquez@regionjunin.gob.pe
06	SUB DIRECCIÓN DE RECURSOS HUMANOS	LIC. JUAN JOSEPH CHAVÉZ SÁNCHEZ	jchavez@regionjunin.gob.pe
07	SUB DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS	CPC. IRIS POVIS RAMOS	ipovis@regionjunin.gob.pe
08	SUB DIRECCIÓN DE ABASTECIMIENTOS Y SERVICIOS AUXILIARES	C.P.C. MARCIAL MANSUETO POMACHAGUA VEGA	mmansueto@regionjunin.gob.pe





GOBIERNO REGIONAL JUNÍN

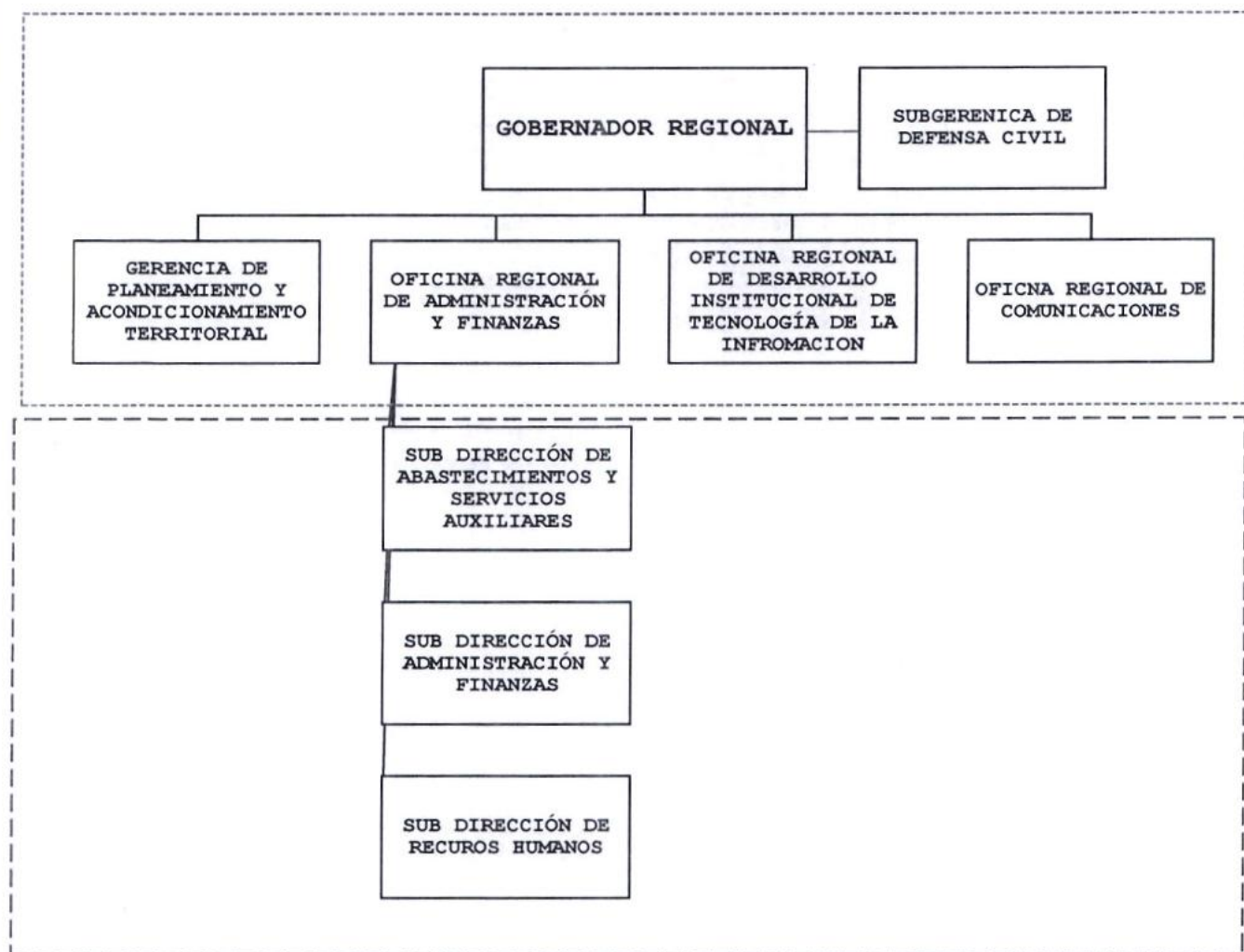
PLAN DE CONTINUIDAD OPERATIVA - 2026



ANEXO 04. ORGANIZACIÓN PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS



Área de toma de decisiones



Desarrollo de los procesos y actividades críticas



ANEXO 05. SISTEMA DE COMUNICACIONES DE EMERGENCIA.

El Sistema de Comunicaciones de Emergencia tiene como finalidad garantizar la coordinación y el intercambio oportuno de información entre la Alta Dirección, las dependencias orgánicas y los responsables de la continuidad operativa del Gobierno Regional Junín durante situaciones de emergencia o desastre que afecten el normal desarrollo de las actividades institucionales.

Como mecanismo alternativo de comunicación, se contará con la **Red Especial Satelital de Comunicaciones en Emergencias (REDSAT)**, sistema de alcance nacional sustentado en el servicio público móvil por satélite contratado por el Estado, conforme a lo establecido en el Decreto Supremo N.º 012-2010-MTC y su modificatoria aprobada mediante Decreto Supremo N.º 004-2018-MTC.

La REDSAT permite mantener las capacidades de coordinación, dirección, supervisión y respuesta de las autoridades ante situaciones de emergencia, desastres naturales o eventos ocasionados por la acción humana que comprometan la disponibilidad de los servicios convencionales de comunicación.

De acuerdo con la Resolución Ministerial N.º 251-2018-PCM, que aprueba la relación de Altas Autoridades y Autoridades de Primera Respuesta que cuentan con el servicio público móvil por satélite, el Gobierno Regional Junín dispone de este recurso estratégico para asegurar la continuidad de las comunicaciones institucionales.

En consecuencia, la REDSAT constituye el medio alternativo de comunicación que será empleado cuando los servicios públicos de telecomunicaciones se encuentren interrumpidos o presenten limitaciones que afecten la gestión de la emergencia y la continuidad operativa institucional.



6. Cronograma de implementación de la Gestión de la Continuidad Operativa.

Nº	Actividades	INDICADOR	RESPONSABLE	FECHA
1	PREPARACION			
1.1	Fortalecimiento de capacidades de los servidores y funcionarios del Grupo de Comando en la Gestión de la Continuidad Operativa	Capacitación	Subgerencia de defensa Civil	junio
2	ENTRENAMIENTO			
2.1	Ejecución de los procedimientos en el ejercicio de Simulación Regional	Informe	Grupo de comando	julio
2.2	Pruebas de los procedimientos de comunicación y verificación de los proveedores críticos.	Documento	Grupo de comando	julio
3	SEGUIMIENTO			
3.1	Realizar el seguimiento a las acciones de implementación.	Encuesta	Grupo de comando	agosto
3.2	La Oficina de Defensa Nacional realizará el seguimiento a las acciones de implementación.	Documento	Subgerencia de defensa Civil	Setiembre / Octubre

