Plan de Continuidad Operativa

Versión 2024

OGRAMA NACIONAL DE EMPLEO “JÓVENES PRODUCTIVOS”
PO DE COMANDO

ÍNDICE

Plan de Continuidad Operativa del Programa Nacional de Empleo “Jóvenes Productivos”

1. Información General

Sobre el Programa

El Programa Nacional de Empleo “Jóvenes Productivos” en adelante el Programa, es una Unidad Ejecutora del Ministerio de Trabajo y Promoción del Empleo que, en concordancia con lo dispuesto en el *artículo 2 del Decreto Supremo N°010-2023- TR*, tiene por objetivo *“Fortalecer y mejorar la empleabilidad de las personas de 15 años a más, con énfasis en la población juvenil, en situación de pobreza, pobreza extrema y/o vulnerabilidad sociolaboral a través de la capacitación laboral, promoción del autoempleo productivo y certificación de las competencias laborales, que responda a la demanda laboral”.* Asimismo, tiene las siguientes funciones:

a) Brindar capacitación laboral en sus distintas modalidades: presencial, no presencial o semipresencial, orientada al fortalecimiento de las competencias laborales para la población en situación de pobreza extrema, pobreza y/o vulnerabilidad sociolaboral.
b) Desarrollar acciones para la certificación de las competencias laborales.
c) Desarrollar acciones de promoción para el autoempleo productivo a través de capacitación, asistencia técnica y acompañamiento para los beneficiarios.
d) Ejecutar acciones de acercamiento empresarial focalizado y acompañamiento especializado a los beneficiarios del Programa, orientadas a su inserción en el mercado laboral.
e) Supervisar, monitorear y evaluar los resultados del programa en coordinación con los órganos competentes del Ministerio de Trabajo y Promoción del Empleo.

En ese sentido, el Programa, interviene a través de los siguientes servicios:

- **Capacitación Laboral**, brindada con la finalidad de que los beneficiarios adquieran o fortalezcan habilidades y competencias necesarias para su inserción en el mercado laboral formal.
- **Capacitación y Asistencia Técnica para el Autoempleo Productivo**, conjunto de acciones y/o actividades que busca desarrollar y/o fortalecer las competencias de gestión en las personas a través de capacitación y asistencia técnica para el autoempleo.
- **Certificación de Competencias Laborales**, proceso voluntario de comprobación de los conocimientos, habilidades y actitudes de una persona, obtenidos a lo largo de su experiencia laboral, independientemente de la forma en que los adquirió, de acuerdo con un estándar de competencia laboral. La evaluación y certificación de competencias laborales se gestiona a través de los centros de certificación de competencias laborales autorizados por el MTPE.
- **Servicio de acompañamiento e Inserción laboral**, comprende el conjunto de acciones que el Programa desarrolla y que están orientadas a promover y fortalecer las capacidades de un grupo de beneficiarios que se encuentren recibiendo o hayan culminado los servicios de manera satisfactoria, a fin de que mejoren sus niveles de empleabilidad.

El Manual de Operaciones del Programa, fue aprobado mediante la *Resolución Ministerial N.º 095-2024-TR*, en este documento se establece la estructura orgánica básica del Programa, como se muestra a continuación:

De igual manera, en dentro del Manual de Operaciones del Programa, en el marco de la gestión por procesos, se aprobó el Mapa de Procesos del Programa, siendo los procesos misionales de la entidad, identificados los siguientes:

- **M01.01** Gestión de la Capacitación Laboral
- **M01.02** Gestión de la Capacitación y Asistencia Técnica para el Autoempleo Productivo
- **M01.03** Gestión de la Certificación de Competencias Laborales
- **M02.01** Gestión de Acompañamiento e inserción laboral

Sobre las sedes del Programa

La Sede Central del Programa se encuentra ubicada en Av. Gral. Salaverry 655, Piso 9, Jesús María, Lima, Perú. En esta sede funcionan la Alta Dirección, las Unidades Funcionales de Asesoramiento y Apoyo, y las Unidades Funcionales de Línea.

Asimismo, a nivel nacional, el Programa cuenta con nueve (08) Unidades Territoriales, donde operan las Unidades Desconcentradas, distribuidas de la siguiente manera:

- **Unidad Territorial Arequipa:** Calle Los Picaflores 128-130, Urb. El Carmen – 2do. Piso. Cercado de Arequipa (Ref.: Frente de la puerta de ingeniería de La UNSSA) - Arequipa - Arequipa - Arequipa – Perú.

- **Unidad Territorial Ayacucho:** Jr. Raúl Porras Barrenechea N.º 403 - Ayacucho - Huamanga - Jesús Nazareno – Perú.

- **Unidad Territorial Cusco:** Av. Micaela Bastidas y Alcides Vigo 301 Wanchaq- Cusco. - Cusco - Cusco - Cusco – Perú.

- **Unidad Territorial Ica:** Av. Grau N° 148 - Ica - Ica - Ica – Perú.

- **Unidad Territorial Junín:** Jr. Arequipa 530 El Tambo/ Dirección Regional De Trabajo - Junín - Huancayo - El Tambo – Perú.

- **Unidad Territorial La Libertad:** Calle Santa Lucia Mz: V, Lt. 19 urbanización La Merced III Etapa – Trujillo, La Libertad - La Libertad - Trujillo - Trujillo – Perú.

- **Unidad Territorial Lambayeque:** Calle Pan Americana N.º 123 - Piso 2. Urb. Los Libertadores - Lambayeque - Chiclayo - Chiclayo – Perú.

- **Unidad Territorial Piura:** Av. Luis Montero N.º 439 Y-2, Referencia - Piura - Piura - Castilla – Perú.

Sobre el Plan de Continuidad Operativa

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

Los peligros identificados a los que está expuesto el Programa Nacional de Empleo “Jóvenes Productivos”, son los siguientes:

- Sismo de Gran Magnitud
- Incendios
- Ataque informático
- Grave alteración del orden público
- Epidemia - Pandemia

Al respecto, la implementación de la Continuidad Operativa requiere de un alto grado de participación y compromiso de los servidores y de la Alta Dirección de la Institución, que permita lograr un resultado eficiente y eficaz en la capacidad de respuesta del Programa, previniendo anticipadamente y disminuyendo el factor sorpresa de las emergencias.

2. Ámbito de Aplicación

El presente Plan de Continuidad Operativa es de aplicación y cumplimiento obligatorio en el Programa Nacional de Empleo "Jóvenes Productivos", que involucra todos sus órganos y unidades orgánicas de la Sede Central, y su implementación progresiva y gradual en las Unidades Territoriales conforme a la identificación de actividades críticas.

3. Base Legal

- Ley N°29664, Ley del Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD y su reglamento
- Decreto Supremo N.º 010-2023-TR, en el cual se modifica la denominación del Programa Nacional para la Empleabilidad por la de Programa Nacional de Empleo "Jóvenes Productivos".
- Resolución Ministerial N°320-2021-PCM, Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno.
- Resolución Ministerial N.º 095-2024-TR, que aprueba el Manual de Operaciones del Programa Nacional para la Empleabilidad (en adelante PNEJP).
- Resolución Directoral N.º 0018-2024-MTPE/3/24.2 que aprueba la conformación del Grupo de Comando del Programa Nacional de Empleo "Jóvenes Productivos".

4. Definiciones

- **Actividades criticas:** Están constituidas por las actividades que la entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias señaladas en las normas vigentes sobre la materia.
- **Peligro:** Situación o característica intrínseca de algo capaz de ocasionar daños a las personas, equipos, procesos y ambiente.
- **Riesgo:** Probabilidad de que un peligro se materialice en determinadas condiciones y genere daños a las personas, equipos y al ambiente.
- **Incidente:** Suceso acaecido en el curso del trabajo o en relación con el trabajo, en el que la persona afectada no sufre lesiones corporales, o en el que éstas sólo requieren cuidados de primeros auxilios.
- **Grupo de Comando:** Es el conjunto de profesionales que se encarga de la elaboración del Plan de Continuidad Operativa de la entidad y de la toma de decisiones respecto a la implementación de dicho plan.
- **Desastre:** Conjunto de daños y pérdidas, en la salud, fuentes de sustento, hábitat físico, infraestructura, actividad económica y medio ambiente, que ocurre a consecuencia del impacto de un peligro o amenaza cuya intensidad genera graves alteraciones en el funcionamiento de las unidades sociales, sobrepasando la capacidad de respuesta local para atender eficazmente sus consecuencias, pudiendo ser de origen natural o inducido por la acción humana.
- **Procesos críticos:** Conjuntos de actividades y tareas críticas que se desarrollan al interior de las diferentes instancias de una institución para garantizar la puesta en marcha de los procesos identificados como indispensables que sustentan su misión institucional.
- **Sede alterna de la entidad pública:** Espacio físico o infraestructura segura y accesible, determinada con anterioridad y de disponibilidad inmediata, que permite la ejecución de los servicios o actividades críticas señaladas en el Plan de Continuidad Operativa de la ▪ entidad. Para ello cuenta con el equipamiento necesario y servicios indispensables, que opera con autonomía y de conectividad. La sede alterna se ocupa cuando la sede principal de la entidad ha colapsado o su condición de operatividad ha sido afectada y pone en riesgo la seguridad del personal, pudiéndose establecer sedes alternas compartidas, que albergan a dos o más entidades públicas.
- **Pandemia:** Epidemia de presentación global o que afecta un área muy amplia, cruzando las fronteras internacionales y usualmente afectando a gran número de personas.
- **Protocolo de actuación en casos de desastres:** Son los acuerdos establecidos

relacionadas con la atención de emergencias para realizar las operaciones de respuesta durante una situación de crisis, las cuales deben integrarse en procesos que ayuden a la toma de decisiones, al desarrollo de las funciones y a la coordinación durante la respuesta ante la emergencia o desastre.

- **Trabajo remoto:** Prestación de servicios subordinada que realiza un(a) trabajador(a) que se encuentra físicamente en su domicilio o en el lugar de aislamiento domiciliario. Se realiza a través de medios o equipos informáticos, de telecomunicaciones y análogos (internet, telefonía u otros), así como cualquier otra naturaleza que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita.

5. Objetivos

5.1. Objetivo general

Garantizar la continuidad de las operaciones del Programa Nacional de Empleo "Jóvenes Productivos" ante la ocurrencia de una emergencia o desastre de gran magnitud u otro evento que interrumpa sus actividades habituales, ejecutando actividades críticas identificadas previamente hasta lograr su recuperación en el menor plazo posible, permitiendo así la continuidad de sus servicios y procesos.

5.2. Objetivos específicos

5.2.1. Objetivo específico 1 (OE1)

Identificar las actividades críticas que deben ejecutarse de manera continua y sin interrupciones en caso de desastres u otros eventos que puedan afectar de forma prolongada las operaciones.

5.2.2. Objetivo específico 2 (OE2)

Determinar los recursos humanos, materiales, equipos, infraestructura y sistemas informáticos y de telecomunicaciones necesarios para mantener dichas actividades.

5.2.3. Objetivo específico 3 (OE3)

Definir los roles y responsabilidades necesarias para la ejecución de las actividades críticas.

6. Identificación de Riesgos y Recursos

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

Asimismo, se define el peligro como la probabilidad de que un fenómeno, potencialmente dañino, se presente en un lugar específico, con una cierta intensidad y en un período de tiempo y frecuencia definidos.

El peligro, según su origen, puede ser de dos clases: los generados por fenómenos de origen natural; y, los inducidos por la acción humana. El peligro, según su origen, puede ser de dos clases:

- Generados por fenómenos de origen natural
- Inducidos por la acción humana.

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

6.1. Matriz de riesgos

Para evaluar la probabilidad y la gravedad del riesgo asociado a los peligros que afectaría al Programa, ocasionado por un evento disruptivo, se ha tomado en cuenta la metodología emitida por la RM N.º 320-2021-PCM, la cual se realiza tomando en cuenta la intersección del peligro y la vulnerabilidad, tal como indica la matriz siguiente:

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

Fuente: Elaboración propia

6.1.1. Identificación y descripción de peligros identificados

El Programa ha identificado aquellos eventos que podrían causar la interrupción total o parcial de los servicios, afectando la infraestructura, los recursos, y la vida humana. En particular, se han considerado aquellos riesgos que impactarían las principales actividades administrativas y económicas que son fundamentales para el cumplimiento de los objetivos misionales de la institución, especialmente dentro del ámbito de Lima Metropolitana. Los peligros identificados son los siguientes:

6.1.1.1. Sismo de gran magnitud

Los sismos son fenómenos que representan la liberación de energía interna de la tierra mediante la ruptura de las capas de corteza y que se manifiesta como movimientos ondulatorios que pueden llegar a alcanzar magnitudes variadas.

En el caso del Perú, la probabilidad de ocurrencia de sismo es continua en el tiempo y cada año se registra y reporta en promedio 150 a 200 sismos percibidos por la población con intensidades mínimas de II – III (MM) y magnitudes ML => 4.01.

De acuerdo con los datos reportados por Instituto Geofísico del Perú (IGP), durante el año 2023, en el territorio, se han reportado cuatrocientos sesenta y tres (463) sismos[1]. Asimismo, es preciso indicar que, solo en el caso de Lima, ante la ocurrencia de un sismo, la población potencialmente que se vería expuesta ascendería a un aproximado de diez millones, cuatrocientos setenta y un mil, ochocientos doce (10’ 471,812), es decir el 53.15% de la población territorial[2].

En ese sentido un evento de tal magnitud, indefectiblemente, afectaría la infraestructura de las edificaciones, incurriendo en algunos casos hasta en el colapso. Asimismo, se registrarían problemas en los servicios básicos de suministro de energía, agua y saneamiento, así como ocasionaría problemas de accesibilidad, entre otros, que configuran una situación de emergencia.

6.1.1.2. Incendios

La ocurrencia de un incendio puede afectar las estructuras de la sede y a los trabajadores por la exposición directa al fuego y calor, la inhalación, intoxicación y asfixia por humo o la muerte por aplastamiento o presión de las mismas personas atrapadas en los accesos y salidas de las edificaciones.

[1] Disponible en la sección de reportes del Instituto Geofísico del Perú: http://ultimosismo.igp.gob.pe/ultimo-sismo/sismosreportados
[2] Política Nacional de Gestión del Riesgo de Desastres al 2050. Sección Resumen Ejecutivo – III. Situación actual del problema público, página 20.

Existe una probabilidad de ocurrencia de un incendio en los locales institucionales durante horas laborables, debido al aumento de los espacios dedicados a oficinas, la instalación de equipos eléctricos, electrónicos y la alta concentración de material inflamable en algunos de los locales, como es el caso de los Almacenes.

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

6.1.1.3. Ataque informático

Un ataque informático se puede describir como una actividad hostil contra un sistema, un instrumento, una aplicación o un elemento que tenga un componente informático.

Hasta el momento, no se ha reportado un ataque informático en el Programa. Sin embargo, la actual situación de la infraestructura tecnológica con la que opera el sistema informático institucional puede ser vulnerada debido a los acelerados avances tecnológicos y obsolescencia de las medidas informáticas, atentando contra la confidencialidad, integridad y disponibilidad que son principios básicos de la seguridad informática.

La Ley N.º 30096 señala que los delitos contra datos y sistemas informáticos comprenden el i) acceso ilícito, el que acceda sin autorización legal a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo; ii) atentado contra la integridad de datos informáticos, el que a través de tecnologías de la información o comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos; y, el atentado contra la integridad de los sistemas informáticos, el que, a través de tecnologías de la información y comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de servicios.

6.1.1.4. Grave alteración del orden público

Se considera alteración del orden público a la acción perpetrada por grupos de personas que atentan contra el orden público, realizando delitos de hurto, destrucción de bienes materiales por medio de una instigación o agitación de la violencia de una masa o grupo de personas. Esta situación puede generar la ocupación indebida de las instalaciones, impedimento de acceso de personal, sabotaje a los sistemas de suministro de energía, comunicaciones u otros que impidan al Programa cumplir con sus funciones. En ese contexto, es necesario prever la activación del Plan de Continuidad Operativa.

6.1.1.5. Epidemia - Pandemia

Una epidemia es el aumento extraordinario del número de casos de una enfermedad infecciosa a nivel mundial, la cual ya existe en una región o población determinada y se produce cuando el nuevo virus infecta a la población que no cuenta con inmunidad. Puede referirse también a la aparición de un número importante de casos de una enfermedad infecciosa en una región o población habitualmente libre de la enfermedad.

Se considera como peligro porque puede conllevar a la supresión de la capacidad del recurso humano si es que se presenta con un rápido contagio y/o alta tasa de letalidad, sin contar con tratamiento o cura, o requiere de tratamiento prolongado.

Este peligro toma relevancia con la aparición en Wuhan – China, en el año 2019, de una enfermedad infecciosa causada por el virus SARS-Cov-2 "COVID-19", el cual produce una enfermedad respiratoria como la gripe (influenza) con diversos síntomas (tos, fiebre, etc.) que, en casos graves, puede producir una neumonía y ser letal. Su expansión ha llegado a plantear una emergencia sanitaria a nivel mundial.

Las epidemias pueden estar causadas por patógenos o tipos de virus de reciente aparición (que por zoonosis transmiten la enfermedad de animales a humanos), o por enfermedades altamente contagiosas (tuberculosis, meningitis meningocócica, influenza, etc.).

El grado de peligrosidad o mortalidad de la enfermedad depende de cada virus, bacteria o parásito que la genera, de las condiciones de salud de la persona, de la existencia o no de tratamiento, de la existencia o no de una vacuna, o del tiempo que dure su tratamiento.

En el caso de que la enfermedad sea nueva para los humanos, no existirán personas inmunes a ella, ni se contará de inmediato con la respectiva vacuna. Estas condiciones ocasionarían que un gran número de personas se enfermen rápidamente.

6.1.2. Determinación del nivel de impacto

Consiste en establecer los daños y pérdidas asociados al evento disruptivo y por consiguiente la interrupción prolongada de los procesos que soportan el cumplimiento de la misión del Programa.

En el siguiente cuadro se observa la estimación del nivel de impacto que afectaría a la institución relacionando el peligro con variables de operatividad determinados para el presente plan.

V / P		Peligros				
		Sismo de gran magnitud	**Incendios**	**Ataque informático**	**Grave alteración del orden público**	**Epidemia - Pandemia**
Variables de Operatividad	Colapso total y/o parcial de infraestructura	Riesgo Muy Alto	Riesgo Alto	Riesgo Bajo	Riesgo Medio	Riesgo Bajo
	Colapso del suministro de energía eléctrica	Riesgo Muy Alto	Riesgo Muy Alto	Riesgo Bajo	Riesgo Alto	Riesgo Bajo
	Colapso de suministro de los servicios de agua	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Riesgo Alto	Riesgo Bajo
	Operatividad de equipos sistemas y medios informáticos	Riesgo Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Bajo	Riesgo Bajo
	Operatividad de equipos y tecnología de comunicaciones	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Bajo
	Disponibilidad de Recursos Humanos especializados en la operación de las actividades criticas	Riesgo Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Medio	Riesgo Muy Alto
	Disponibilidad de recursos financieros	Riesgo Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Medio	Riesgo Muy Alto

Fuente: Elaboración propia

De acuerdo con el cuadro anterior se determina el nivel de impacto que tendría la entidad frente a los peligros identificados teniendo una relación directa con el nivel de riesgo determinado.

En ese sentido, de acuerdo a los peligros identificados y la vulnerabilidad de la infraestructura, se determina la matriz de riesgos:

Peligros	Nivel de Impacto
Sismo de Gran Magnitud	Riesgo Muy Alto
Incendios	Riesgo Muy Alto
Grave alteración del orden público	Riesgo Alto
Ataque informático	Riesgo Alto
Epidemia - Pandemia	Riesgo Medio

6.2. Identificación de recursos

Con la determinación de los peligros y los niveles de impacto que ocasionaría algún evento disruptivo es necesario precisar que el Programa cuenta con recursos para la respuesta que permitirá responder ante la situación de emergencia o desastre, y en caso amerite la evacuación del local, ser trasladados con el equipamiento o en su defecto prever contar con equipamiento para la Sede Alterna. Es importante anotar que el uso de estos recursos debe estar relacionado con la identificación del evento y otros efectos colaterales que se generen.

7. Acciones para la Continuidad Operativa

7.1. Determinación de las Actividades Críticas

Matriz de Actividades Críticas del plan de Continuidad Operativa

Proceso	Actividad crítica	Impacto	Unidad Responsable
Gestión de la Capacitación Laboral	Planificar, ejecutar y monitorear la capacitación laboral	Incumplimiento con la capacitación laboral a los beneficiarios del Programa	Unidad Técnico Operativa de los Servicios para la Empleabilidad
Gestión de la Capacitación y Asistencia Técnica para el Autoempleo Productivo	Planificar, ejecutar y monitorear la Capacitación y Asistencia Técnica para el Autoempleo Productivo	Incumplimiento con la Capacitación y Asistencia Técnica para el Autoempleo Productivo a los beneficiarios del Programa	Unidad Técnico Operativa de los Servicios para la Empleabilidad
Gestión de la Certificación de Competencias Laborales	Planificar, ejecutar y monitorear la Certificación de Competencias Laborales	Incumplimiento con la Certificación de Competencias Laborales a los beneficiarios del Programa	Unidad Técnico Operativa de los Servicios para la Empleabilidad
Gestión de Acompañamiento e inserción laboral	Planificar, ejecutar y monitorear el Acompañamiento e inserción laboral	Incumplimiento con el Acompañamiento e inserción laboral a los beneficiarios del Programa	Unidad de Acompañamiento e Inserción Laboral
Gestión del Empleo, Compensaciones, Capacitación, Rendimiento y de las Relaciones Humanas y Sociales	Ejecutar el pago de planillas y beneficios	Incumplimiento del pago de la remuneración a todos los servidores.	Unidad de Administración y Finanzas
Gestión de Abastecimiento	Provisión de Bienes y Servicios a demanda (incluye pago a proveedores)	Interrupciones en la entrega de productos o servicios	Unidad de Administración y Finanzas
Gestión de la Infraestructura Tecnológica y Soporte Técnico	Mantener la operatividad de los sistemas informáticos, plataformas tecnológicas, servicios y páginas web críticos identificados por las áreas usuarias, con la finalidad de garantizar el procesamiento, la generación y la publicación de los datos y productos	Interrupciones en la operatividad diaria.	Unidad de Planeamiento, Modernización y Presupuesto

7.2. Aseguramiento del Acervo Documentario

Realidad archivística del Programa

Organización

El Sistema Institucional de Archivos de Programa está integrado por:

a) Archivo Central encargado de custodiar el acervo documentario del Programa. Está ubicado en Jr. Rodolfo del Campo N° 281, distrito de La Victoria.

b) Archivos Periféricos están a cargo de las unidades del Programa que cuentan con un espacio destinado a los archivos a su cargo y un responsable de su gestión. Podemos citar aquí a los archivos de las Unidades Territoriales.

c) Archivos de Gestión que comprende los archivos secretariales y técnicos de todas las Unidades del Programa.

Órgano de Administración de Archivos

De acuerdo al Manual de Operaciones, la Unidad de Administración y Finanzas es la encargada de la administración y supervisión del Archivo Central en concordancia con la política institucional en materia archivística y los lineamientos del Archivo General de la Nación.
En ese sentido el responsable del Órgano de Administración de Archivos (OAA) es la Jefatura de la Unidad de Administración y Finanzas.

A fin de brindar seguridad en la custodia del acervo documentario del Programa, el local del Archivo Central cuenta con lo siguiente:

- Sistema de red contra incendio de agua.
- Detectores de humo.
- Extintores portátiles y rodantes.
- Cámaras de video en el exterior.
- Sistema de ascensor.
- Vigilancia las 24 horas.

Evaluación de riesgos

Revisión continua de las condiciones óptimas en la custodia de los documentos tales como el orden en los repositorios donde se custodia el acervo documentario, que los documentos se encuentren ordenados dentro de cajas archiveras para su adecuada conservación, que se realice una limpieza continua de los repositorios para evitar el polvo, la aparición de agentes biológicos y otros factores contaminantes.

Seguridad física

El personal del archivo es el único que cuenta con llaves de acceso a la Oficina y a los repositorios del Archivo Central, y solo se permite el acceso a personal del Programa que esté previamente autorizado.

Digitalización de los documentos

Digitalización gradual de los documentos más solicitados y que tienen un valor permanente.

Se ha creado una carpeta \\192.168.204.20\archivo-central en el servidor del Programa para guardar una copia de los documentos digitalizados.

7.3. Ejecución del Plan de Recuperación de los servicios informáticos

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad de las operaciones, minimizar el riesgo y

maximizar el retorno de las actividades. Ante todo, la seguridad de la información se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en ordenadores y transmitida a través de las redes a otros ordenadores.

Se proponen las posibles soluciones de recuperación de los escenarios de riesgos, incluyendo estrategias preventivas y correctivas. Se han seleccionado alternativas para los escenarios de amenaza identificados que cumplen con los tiempos de recuperación identificados en el Análisis de Impacto de Negocio. A continuación, se indican las posibles estrategias de recuperación:

a. Destrucción de los recursos informáticos alojados en el centro de datos como resultado de un sismo, inundación o incendio.

- Implementar un Centro de Datos de contingencia en las instalaciones de un proveedor de hosting, además que en caso se presente un escenario de sismo, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos.
- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
- Realizar copias de respaldo de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Almacenar las copias de respaldo diarias en un ambiente separado del Centro de Datos.
- Contratar el servicio de almacenamiento de las copias de respaldo a cargo de proveedor externo, con un periodo mínimo semanal de retiro de copias de respaldo hacia las instalaciones externas.
- Asegurarse de contar con enlaces redundantes con el Centro de Datos alterno.
- Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI para uso de Core y Distribución.
- Implementar sistema de extinción de incendio en el Centro de Datos.
- Eliminar todo material inflamable del ambiente de Centro de Datos y cuarto de UPS.
- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías.

b. Indisponibilidad de servidores críticos por falla de hardware o software

- Implementar alta disponibilidad en los servidores virtualizados.
- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
- Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos
- Programación de revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

c. Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque

- Mantener actualizado los parches de seguridad en servidores y estaciones de trabajo.
- Mantener actualizado el software de protección antimalware en cada servidor y estación de trabajo.
- Mantener controles de seguridad perimetral como Firewall.
- Contratar el servicio de seguridad de aplicaciones Web como WAF.
- Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos.
- Mantener el monitoreo del rendimiento y consumo de los recursos en los servidores.

- Realizar pruebas anuales de Hacking Ético de terceros especializados.

d. <u>Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos</u>

- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías.
- Implementar un tablero de transferencia automático (Bypass) en el Centro de Datos para asegurar la continuidad eléctrica ante fallas del sistema de UPS.
- Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y quipos críticos del Centro de Datos.
- Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías.
- Realizar el apagado de los equipos, mientras se cuente con energía del UPS.
- Evaluar contar con un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento.
- Evaluar el implementar un generador eléctrico para proveer energía al Centro de Datos en casos de falla de la red eléctrica pública.

e. <u>Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico</u>

- Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol, de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto.
- Entrenar al personal del Área de Estadística e informática en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos del Área de Estadística e informática, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
- Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

f. <u>Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones</u>

- Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado del Centro de Datos.
- Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones.
- Mantener los Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de Datos.

7.4. Roles y Responsabilidades para el Desarrollo de las Actividades Críticas

Para asegurar la continuidad de las operaciones en el Programa se han establecido tres niveles de organización según el nivel de responsabilidad:

- **Tomadores de Decisiones o Gestión Estratégica:** Definido por establecer las acciones de dirección, coordinación y articulación institucional, se basan en las directrices estratégicas y operativas para enfrentar la crisis ante el evento disruptivo y mantener la continuidad de las operaciones del Programa. Está integrado por la Dirección Ejecutiva del Programa.
- **Unidades de Apoyo:** Consiste en establecer mecanismos que permitan el desarrollo de las actividades críticas brindando el soporte en los recursos logísticos y humanos

principalmente. Está integrado por las Unidades de Administración y Finanzas y la Unidad de Planeamiento, Modernización y Presupuesto.

- **Unidades Operativas:** Determinado por la misión de la institución, son quienes brindan servicios al ciudadano, propone a la Dirección Ejecutiva acciones correctivas y prospectivas para asegurar la continuidad operativa en situación de crisis hasta lograr su restablecimiento.

Conformación del Grupo Comando

Definido como un equipo de profesionales, cuyo objetivo principal es la elaboración e implementación del Plan de Continuidad Operativa (PCO), bajo la dirección del jefe de la Unidad de Planeamiento, Modernización y Presupuesto. Este liderazgo se ejerce en su calidad de titular de la "Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa", designado mediante ***Memorándum N.º 000095-2024-MTPE/3/24.2*** del 02 de mayo de 2024.

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

La conformación del Grupo de Comando del Programa se visualiza a continuación:

- Jefe de la Unidad de Planeamiento, Modernización y Presupuesto quien lo preside.
- Jefe de la Unidad Técnica Operativa de los Servicios para la Empleabilidad
- Jefe de la Unidad de Acompañamiento e Inserción Laboral
- Jefe de la Unidad de Administración y Finanzas.
- Jefe/a del Área de Informática.
- Jefe/a del Área de Recursos Humanos.

El cual fue definido mediante la ***Resolución Directoral N.º 000018-2024-MTPE_3_24.2*****,** el 21 de mayo de 2024.

7.5. Requerimientos

7.5.1. Requerimientos de Personal

Para garantizar la continuidad operativa de los servicios y procesos críticos identificados, se contará con personal clave que será convocado para llevar a cabo las actividades esenciales en caso de que la infraestructura se vea afectada. En esta situación, se restringirá el acceso a las oficinas, promoviendo la modalidad de teletrabajo. Si la infraestructura se vuelve inoperativa, se procederá a trasladar al personal clave a la sede alterna designada.

7.5.2. Requerimiento de Material y equipo

Son aquellos mobiliarios y bienes mínimos requeridos para facilitar las labores de las actividades críticas previamente identificadas.

7.5.3. Requerimiento de recursos informáticos

Se deberá asegurar la disponibilidad de los equipos informáticos (Software y Hardware) ya sea para el teletrabajo como para las actividades que se ejecutarán en las sedes alternas de activarse, se considerarán los equipos informáticos mínimos necesarios para el personal clave y de apoyo que se convocará para la continuidad operativa del Programa.

7.5.4. Requerimiento Presupuestal

Las actividades previstas en el presente plan, dada la naturaleza de los servicios priorizados para mantener la Continuidad Operativa, serán cubiertos inicialmente con recursos asignados a cada Centro de Costo del Programa, ya que estos obedecen principalmente al accionar administrativo de la entidad, que se pueden operativizar de manera virtual.

En ese sentido la Unidad de Planeamiento, Modernización y Presupuesto, en el marco de sus competencias y de la normativa legal vigente podrá realizar modificaciones presupuestales para garantizar, de ser el caso, el financiamiento

del desarrollo de las actividades críticas en base a los acuerdos tomados por el Grupo de Comando en el momento de la ocurrencia de algún evento descrito en la presente.

Recursos mínimos para la continuidad operativa

N.°	Actividad crítica	Unidad Responsable	Personal	Escritorios	Sillas personales	Pc /Laptop	Impresoras
1	Planificar, ejecutar y monitorear la capacitación laboral	Unidad Técnico Operativa de los Servicios para la Empleabilidad	3	3	3	3	1
2	Planificar, ejecutar y monitorear la Capacitación y Asistencia Técnica para el Autoempleo Productivo	Unidad Técnico Operativa de los Servicios para la Empleabilidad	2	2	2	2	-
3	Planificar, ejecutar y monitorear la Certificación de Competencias Laborales	Unidad Técnico Operativa de los Servicios para la Empleabilidad	2	2	2	2	-
4	Planificar, ejecutar y monitorear el Acompañamiento e inserción laboral	Unidad de Acompañamiento e Inserción Laboral	3	3	3	3	1
5	Ejecutar el pago de planillas y beneficios	Unidad de Administración y Finanzas	3	3	3	3	1
6	Provisión de Bienes y Servicios a demanda (incluye pago a proveedores)	Unidad de Administración y Finanzas	4	4	4	4	1
7	Mantener la operatividad de los sistemas informáticos, plataformas tecnológicas, servicios y páginas web críticos identificados por las áreas usuarias, con la finalidad de garantizar el procesamiento, la generación y la publicación de los datos y productos	Unidad de Planeamiento, Modernización y Presupuesto	3	3	3	3	-

7.6. Determinación de la Sede Alterna de Trabajo

La determinación de las instalaciones de continuidad en caso de que no sea posible continuar las operaciones en la sede principal, es una tarea muy importante, debido a que permitirá establecer centros alternativos de trabajo, que si bien, serán de menor tamaño y con menor funcionalidad que la sede central, garantizan la ejecución del Plan de Continuidad Operativa del Programa.

Por otro lado, de contar con un marco normativo para la implementación de la modalidad de teletrabajo durante la emergencia suscitada, dicha modalidad será implementada para los funcionarios y servidores civiles cuyas funciones y naturaleza de sus labores puedan ser ejecutadas desde su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo.

En cuanto a la implementación de una sede alterna, el Programa no dispone de un local propio. Sin embargo, dado que el Programa está adscrito al Ministerio de Trabajo y Promoción del Empleo, se solicitará a dicho Ministerio la facilitación de un espacio adecuado que funcione como sede alterna. Esto permitirá recuperar la operatividad de las

actividades críticas que puedan verse afectadas ante la ocurrencia de un desastre o evento que interrumpa de manera prolongada las operaciones de la entidad.

7.7. Activación del Plan de Continuidad Operativa

La activación del PCO del Programa se origina ante la ocurrencia de un evento adverso con el fin de continuar brindando los servicios y desarrollando las actividades de la institución.

7.7.1. Momento del evento desencadenante y Activación

El Plan de Continuidad Operativa, considera los escenarios en los que puede ocurrir el evento, según el momento en que suceda, ya que ello implica diferentes acciones a tener en cuenta.

Día laborable (en horas de trabajo): En el supuesto que el evento ocurra durante el día y en horas laborables, el personal se encontrará en sus labores habituales, por lo que, una vez ocurrido, deberá reportarse de inmediato a sus respectivos jefes de Unidad para saber la condición en que se encuentran; así mismo es natural que el personal verificará las condiciones de su entorno familiar, y se pondrá a disposición una vez verificado esto.

Feriado / Fin de semana: Es necesario precisar que normalmente en estas circunstancias, el Programa, suele estar con los procesos operativos disminuidos. Si el evento ocurre en este periodo, el personal de la entidad debe saber que tiene que reportarse en los tiempos establecidos en este plan, según su rol y función, a los diversos niveles de organización, para poner en marcha la Continuidad Operativa de la entidad.

De noche / medianoche / madrugada: Si el evento ocurre en la noche o la madrugada de cualquier día, el personal de la entidad debe saber que tiene que reportarse en los tiempos establecidos en este plan, según su rol y función, a los diversos niveles de organización, para poner en marcha la Continuidad Operativa. Salvo que no medie indicación en contrario, deberá presentarse al centro de labores en las horas habituales de ingreso.

Los medios de comunicación a ser considerados, según orden de prioridad, son:

1. Mensajes de Texto por celular.
2. Mensaje al Chat de WhatsApp del Programa.
3. Redes sociales y correos electrónicos.
4. Llamada al teléfono fijo y celular
5. Cualquier otro medio que permita la comunicación

Los primeros dos medios de comunicación han de ser usados de manera simultánea.

7.7.2. Flujo de acciones

El flujo de acciones es determinado por la naturaleza del impacto de cada peligro (Sismo de gran magnitud, incendios, ataque informático, epidemia - pandemia y alteración del orden público).

Sucedido el evento contemplado como peligro de la operatividad del Programa, las acciones que se emprenden se dividen en cuatro fases:

- **Primera Fase:** Alerta.
- **Segunda Fase:** Activación
- **Tercera Fase:** Preparación de la desactivación.

g. Fase de alerta

Esta fase se refiere al acopio y reporte de la información inicial de los daños ocasionados por las amenazas, por lo que, se constituye en una situación de alerta.

Consta de tres (02) momentos:

1. Primer Momento: Evaluación inicial de Recursos Humanos (RRHH) y de la infraestructura del Programa *(utilizar ficha técnica descrita en anexo 07).*

Ocurrido un evento, el personal del Programa aplica los procedimientos de evacuación y planes de contingencia específicos, según corresponda al evento y magnitud. Cada responsable de los diferentes niveles de organización debe verificar que su personal priorizado esté en condiciones de incorporarse al Plan Continuidad Operativa. Tener en cuenta que es importante verificar que se encuentren en condiciones físicas y emocionales de asumir su responsabilidad. El personal capacitado de turno designado por el Grupo de Comando aplicará la Ficha Técnica de Evaluación de la infraestructura Inicial considerada y reportará a este el resultado (condición de habitabilidad o no habitabilidad, así como la capacidad de operatividad o no operatividad).

2. Segundo Momento: Reporte al COES del MTPE, responsable del nivel de organización de la Continuidad Operativa.

El grupo de comando en el marco de sus funciones reporta al COES del MTPE el resultado (condición de habitabilidad o no habitabilidad, así como la capacidad de operatividad o no operatividad) del Programa.

El tiempo máximo de duración de esta fase, entendiendo que es la que brindará los insumos para la decisión de activación del Plan de Continuidad Operativa (fase de ejecución), no debe superar dos (02) horas.

h. Fase de activación

Esta fase se inicia con la activación del Plan de Continuidad Operativa, activándose con la gestión de la crisis. El tiempo máximo de duración de esta fase no debe superar las 12 horas una vez activado el Plan de Continuidad Operativa, salvo que dicho periodo se amplíe por un tiempo adicional dispuesto por el Grupo Comando, para lo cual deberá coordinarse con la Dirección Ejecutivo, la Unidad de Administración y Finanzas, la Unidad de Planeamiento, Modernización y Presupuesto y las Unidades de Línea. Los momentos de esta fase son las siguientes:

1. **Activación del PCO: Cadena de mando y trabajo no presencial o mixto**
   - El presidente del Grupo de Comando de la Gestión de la Continuidad Operativa evalúa la información de los daños causados *(ficha técnica descrita en anexo 07).* Asimismo, comunica de contar con un marco normativo para iniciar la implementación del trabajo no presencial o trabajo mixto (combinación de trabajo presencial o no presencial).
   - El área de Recursos Humanos de la Unidad de Administración y Finanzas, establece los criterios y evalúa a propuesta de las unidades orgánicas de Programa el riesgo de los trabajadores que realizarían el trabajo presencial, en función de la emergencia y su estado de salud.
   - Asimismo, se debe considerar si el servidor civil propuesto está en condiciones de realizar dicha labor, evaluando sus condiciones personales y familiares, por ejemplo, el daño de su domicilio o, deceso de familiares, familiares heridos, entre otros.

2. **Acondicionamiento y puesta en operaciones**
   - Tomada la decisión de trabajar no presencial o en trabajo mixto, cada trabajador deberá comunicar a su jefe inmediato si cuenta con equipo informático, así como con acceso a los servidores informáticos del Programa por información específica para la ejecución de sus funciones, de no contar solicitará al Área de

Informática y al Área de Abastecimiento para la asignación respectiva.

3. Inicio de Operaciones

- El Área de Informática, brindará el apoyo a los servidores para la instalación de los aplicativos que se requiere para el inicio del trabajo no presencial, así como las solicitudes de acceso por parte de los trabajadores del Programa, a fin de contar con la información necesaria para la ejecución de sus funciones.
- El Área de Recursos Humanos, elaborará y brindará las indicaciones necesarias a los servidores de Programa respecto a la condición de trabajo no presencial y mixto, los protocolos de seguridad y salud en el trabajo entre otros.
- Adicionalmente, a las tareas de apoyo en las operaciones de emergencia, el Área de Abastecimiento, deberá asignar el equipamiento necesario al personal dedicado a resolver las demandas de la implementación de los nuevos ambientes dispuestos para la operatividad del Programa para lo cual deberá analizar e identificar una lista base de insumos y recursos que se necesitaría en caso de una contingencia.

4. Evaluación detallada de la sede institucional afectada (de ser necesario)

- Trascurrido hasta un máximo de 12 horas posterior a la emergencia, el Área de Abastecimiento, debe disponer las concurrencias del personal capacitado, así como la convocatoria de un Especialista en Defensa Nacional, Gestión del Riesgo de Desastres, o el que haga sus veces, para realizar una evaluación detallada sobre la situación real de la infraestructura afectada. **Esa actividad se realiza en coordinación con el INDECI.**
- Posteriormente a la evaluación definitiva de habitabilidad y operatividad que realice el Área de Abastecimiento de la sede principal del Programa emitirá un informe señalando las conclusiones y recomendaciones a que hubiera lugar en un plazo no mayor a 24 horas de ocurridos los hechos, el cual será enviado al Grupo de Comando.

i. Fase de desactivación

Al momento que la emergencia haya sido superada, el presidente del Grupo de Comando decide la culminación de la ejecución del Plan de Continuidad Operativa del Programa, emitiendo un informe a la Dirección Ejecutiva sobre las acciones y gestiones realizadas adjuntando los documentos que sean pertinentes.

j. Desarrollo de las Actividades Críticas

Con el fin de asegurar la continuidad de los servicios se deberá desarrollar las tareas que harán posibles el cumplimiento de las actividades críticas identificadas en los diversos procesos que han sido considerados como indispensables para la entidad.

k. Cronograma de ejercicios del Plan de Continuidad Operativa

El Plan de Continuidad Operativa del Programa debe responder a la realidad y a las necesidades de garantizar sus actividades indispensables, es por ello que se hace necesario programar ensayos, simulaciones y simulacros que permitan medir la operatividad de este plan.

El objetivo principal que se persigue al realizar los ejercicios es determinar el nivel de respuesta deseado para la continuidad operativa de las actividades críticas. Por tal motivo, los ejercicios del Plan de Continuidad Operativa del Programa, se deben ejecutar en las fechas y de acuerdo a lo establecidos en la siguiente tabla.

N°	Fecha	Supuesto	Responsable
01	3ra semana del mes de mayo	Atentado terrorista afectó gran parte de la sede principal	Grupo de Comando del Programa
02	3ra semana del mes de julio	Incendio afectó totalmente a la sede principal	Grupo de Comando del Programa
03	3ra semana del mes de setiembre	Sismo de gran magnitud afectó totalmente a la sede central	Grupo de Comando del Programa
04	3ra semana del mes de noviembre	Ataque informático colapso totalmente los sistemas de información de la entidad	Grupo de Comando del Programa

I. Anexos

Anexo N.º 01: Plan de Recuperación de los Servicios Informáticos

Ítems	Servicio TI	Descripción	Crítico para operaciones internas	Crítico para servicios externos
1	Internet Corporativo	El servicio de acceso a Internet con flujo de carga (publicación) y descarga (navegación) en la Sede Central del PNPEJP	Alta	Alta
2	Acceso a dominio	Servicio de autenticación en el dominio de PNPEJP con el uso de credenciales institucionales.	Alta	Baja
3	Telefonía IP	Servicio de comunicación telefónica por Red IP mediante el uso de Teléfono, físico o teléfonos software.	Baja	Media
4	Correo electrónico	Servicio de mensajería de correo electrónico bajo el dominio @jovenesproductivos.gob.pe	Media	Media
5	Internet inalámbrico	Servicio de acceso a internet mediante conectividad WI-Fi.	Baja	Baja
6	Almacenamiento Nube	El servicio de almacenamiento en nube habilita el mecanismo para resguardo de archivos y acceso desde cualquier lugar conectado a internet.	Baja	Baja
7	Videoconferencia	Servicio de videoconferencia, conferencia Web, y llamadas por internet.	Baja	Baja
8	Acceso a Red	El servicio de acceso a Red permite la conexión de una computadora a la red de datos institucional.	Alta	Media
9	Firma Digital	Servicio de firma digital mediante el uso de Certificados digitales de RENIEC	Alta	Media
10	Almacenamiento en Servidores	Servicio de repositorio digital de archivos generados en la las aplicaciones y digitalización de documentos.	Alta	Alta
11	Base de datos	Servicio de repositorio de información indexada en Base de Datos para aplicaciones y servidores del Centro de Datos.	Alta	Alta
12	VPN	Servicio de conectividad remota segura para ejecutar trabajo remoto.	Media	Baja
13	Estaciones de trabajo	Equipamiento de cómputo como recurso para el procesamiento de información.	Media	Baja
14	Personal crítico responsable de los procesos TI	Servicios profesionales críticos encargados de procesos de TI del AEI	Media	Media
15	Sistemas de Información Internos	Aplicaciones disponibles para acceso por personal administrativo de PNPEJP.	Alta	Media
16	Sistemas de Información Externos (publicados)	Aplicaciones disponibles para acceso para público en general.	Media	Alta
17	Centro de datos	Servicio de hosting y housing como infraestructura de soporte para los servicios de TI del PNPEJP.	Alta	Alta

Plan de Recuperación:	Descripción
Escenario:	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos se encuentran no disponibles a causa de la destrucción originada por un sismo, inundación o un incendio.
Estrategia:	1. Implementar un centro de contingencia en las instalaciones de un proveedor de hosting, además que en caso se presente un escenario de contingencia, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos. 2. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware. 3. Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc. 4. Implementar enlaces redundantes con el Centro de Datos alterno 5. Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI.
Servicios TI:	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina que los servicios de TI a recuperar se pueden agrupar y recuperar en el siguiente orden de prioridad: 6. Red de datos (Equipos de comunicaciones) 7. Internet y Seguridad Perimetral 3. Servicio de Autenticación de Red 8. Base de datos. 9. Sistema de almacenamiento (Storage) 8. Servidores Físicos 10. Sistema de Virtualización (Hipervisor) 10. Servidores Virtuales

1. PLAN DE ACCIÓN – Red de Datos (Equipos de comunicación)

Componentes:

- Switches Core, Switches de Servidores, Switches de Distribución.
- Enlace de datos con proveedor de hosting

Etapas

a) Antes de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Contratar servicios de enlace de datos y servicio de enlace de contingencia hacia el Centro de Datos deun proveedor de hosting, donde se recuperarán los servicios críticos.

Experto en Infraestructura y Soporte Técnico	2. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación.
Experto en Infraestructura y Soporte Técnico	3. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos.
Experto en Infraestructura y Soporte Técnico	4. Mantener un switch administrable de contingencia, que mínimo sea de capa3 del modelo OSI.
Jefe del AEI	5. Revisar el cumplimiento de las copias de respaldo yde la operatividad del equipo de contingencia.

b) Durante la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Revisar la operatividad del Switch Core y equipos de comunicación del Centro de Datos.En caso de estar inoperativos realizar el punto2, caso contrario ir al punto 3.
Experto en Infraestructura y Soporte Técnico	2. Realizar las configuraciones de red en el Switch capa 3 de contingencia.
Experto en Infraestructura y Soporte Técnico	3. Verificar la conectividad con el Centro de Datosde contingencia.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Configurar el hardware nuevo o reparado.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

2. PLAN DE ACCIÓN – Internet y Seguridad Perimetral

Componentes:

- UTM (parte del servicio de Internet y Seguridad Perimetral)

Etapas

a) Antes de la contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Supervisar que el proveedor esté realizando respaldos periódicos de la configuración de los equipos UTM
Experto en Infraestructura y Soporte Técnico	2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el Centro de Datos y

	el documento con la relación de políticas implementadas.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Reportar al proveedor de Servicio de Internet y Seguridad Perimetral la falla en el servicio.
Experto en Infraestructura y Soporte Técnico	2. Revisar el correcto funcionamiento de las políticas de navegación en el servicio de Internet de Contingencia
Experto en Infraestructura y Soporte Técnico	3. Verificar la comunicación desde Internet hacia los servicios publicados.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Revisar el correcto funcionamiento del nuevo hardware.
Experto en Infraestructura y Soporte Técnico	3. Verificar la comunicación desde Internet hacia los servicios publicados.

3. PLAN DE ACCIÓN – Servicio de autenticación de red (Directorio Activo)

Componentes:

- Servidor virtual del directorio activo (DC1, DC2).
- Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el procedimiento de Respaldo de la Información
Experto en Infraestructura y Soporte Técnico	2. Guardar una copia de respaldo en un servidor local y enviar una copia al lugar de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Restablecer la copia de respaldo del servidor de directorio activo.
Experto en Infraestructura y Soporte Técnico	2. Configurar parámetros de red y verificar.

Experto en Infraestructura y Soporte Técnico	3. Realizar pruebas sobre el servicio de directorio activo.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Realizar una copia de respaldo del Directorio Activo de Contingencia
Experto en Infraestructura y Soporte Técnico	3. Restaurar el Directorio Activo de Contingencia en el Directorio Activo de producción recuperado
Jefe del AEI	4. Verificar el cumplimiento del procedimiento de recuperación.

4. PLAN DE ACCIÓN – Base de Datos

Componentes:

- Servidor: DB1, DBQA
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el procedimiento de Respaldo de la Información
Administrador de Base de Datos o quien haga sus veces	2. Monitorear el correcto funcionamiento del SQL Server
Experto en Infraestructura y Soporte Técnico	3. Guardar una copia de respaldo en un servidor local y enviar copia al lugar de custodia.
Jefe del AEI	4. Revisar que se ejecute el Respaldo de la Información

b) Durante la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Activar una máquina virtual como parte del hosting y restaurar la base de datos.
Administrador de Base de Datos o quien haga sus veces	2. Validar la información puede ser consultada
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Instalar recursos afectados.

Administrador de Base de Datos o quien haga sus veces	3. Configurar Base de Datos.
Administrador de Base de Datos o quien haga sus veces	4. Validar que la información puede ser consultada en hardware nuevo o reparado.
Jefe del AEI	5. Verificar el cumplimiento del procedimiento de recuperación.

5. PLAN DE ACCIÓN – Sistema de almacenamiento (Storage)

Componentes:

- Sistema de almacenamiento (Storage, Switches de Fibra Canal).

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento
Experto en Infraestructura y Soporte Técnico	2. Mantener copias de respaldo de la configuración de switches de fibra canal.
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	3. Cumplir con el Respaldo de la Información
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	4. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting)
Experto en Infraestructura y Soporte Técnico	5. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento
Jefe del AEI	6. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Revisar la operatividad del sistema almacenamiento de contingencia (Storage) y promoverlo como sistema de almacenamiento principal
Experto en Infraestructura y Soporte Técnico	2. Configurar parámetros de red y verificar.
Experto en Infraestructura y Soporte Técnico	3. Verificar la comunicación desde los servidores
Ejecutante	**Actividad**
Jefe del AEI	4. Realizar pruebas de los Sistemas de Información.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Configurar el hardware y software de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	3. Actualizar las configuraciones del Sistema de almacenamiento (Storage).
Coordinador de Desarrollo de Sistemas	4. Realizar pruebas sobre las aplicaciones involucradas.
Jefe del AEI	5. Verificar el cumplimiento del procedimiento de recuperación.

6. PLAN DE ACCIÓN – Servidores Físicos

Componentes:

- Respaldo de información
- Licencias de sistemas operativos de servidores
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información.
Experto en Infraestructura y Soporte Técnico	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar la restauración del servidor físico en un servidor virtual.
Experto en Infraestructura y Soporte Técnico	2. Configurar parámetros de red y verificación.
Coordinador de Desarrollo de Sistemas	3. Realizar pruebas de los servicios en el servidor virtual.
Jefe del AEI	4. Verificar el cumplimiento del procedimiento de recuperación.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información.

Experto en Infraestructura y Soporte Técnico	3. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Coordinador de Desarrollo de Sistemas	4. Realizar pruebas sobre los servicios del servidor virtual.
Jefe del AEI	5. Verificar el cumplimiento del procedimiento de recuperación.

7. PLAN DE ACCIÓN – Sistema de Virtualización:

Componentes:

- Servidores: SRV-V
- Hipervisor: Hyper-V.
- Conexión al Sistema de almacenamiento (Storage).

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Contratar servicio de hosting bajo demanda, asegurando la disponibilidad de máquinas virtuales para ser activadas en un escenario de contingencia
Experto en Infraestructura y Soporte Técnico	2. Cumplir con el Respaldo de la Información
Experto en Infraestructura y Soporte Técnico	3. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia.
Coordinador de Desarrollo de Sistemas	4. Revisar que se ejecute el Respaldo de la Información
Jefe del AEI	5. Verificar el cumplimiento del procedimiento de recuperación.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Comunicar a proveedor de hosting la activaciónde la contingencia y solicitar el aprovisionamiento de los recursos para las a. máquinas virtuales necesarias.
Experto en Infraestructura y Soporte Técnico	2. Verificar la conectividad con el sistema de almacenamiento(Storage)
Experto en Infraestructura y Soporte Técnico	3. Configurar la plataforma de Virtualización (Hipervisor)
Coordinador de Desarrollo de Sistemas	4. Verificar la comunicación a nivel de red de cada Hipervisor
Jefe del AEI	5. Verificar el cumplimiento del procedimiento de recuperación

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados.
Experto en Infraestructura y Soporte Técnico	2. Configurar la plataforma de Virtualización en el recurso nuevo o reparado.

Experto en Infraestructura y Soporte Técnico	3. Actualizar las configuraciones de red dé cada Hipervisor
Jefe del AEI	4. Verificar el cumplimiento del procedimiento de recuperación

8. PLAN DE ACCIÓN – Servidores Virtualización:

Componentes:

- Máquinas virtuales
- Licencias de sistemas operativos de servidores
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información.
Experto en Infraestructura y Soporte Técnico	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar la restauración del servidor virtual
Experto en Infraestructura y Soporte Técnico	2. Configurar parámetros de red y verificación.
Coordinador de Desarrollo de Sistemas	3. Realizar pruebas de los servicios del servidor virtual.
Jefe del AEI	4. Verificar el cumplimiento del procedimiento de recuperación.

c) Después de la Contingencia

Ejecutante	Actividad
Coordinador de Desarrollo de Sistemas	1. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información.
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	2. En caso lo soliciten, ejecutar el pase a producción para actualización de información
Coordinador de Desarrollo de Sistemas	3. Realizar pruebas sobre los servicios del servidor virtual.
Jefe del AEI	4. Verificar el cumplimiento del procedimiento de recuperación.

Plan de Recuperación:	PR-02
Escenario:	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores.
Estrategia:	1. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware. 2. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos y central telefónica 3. Implementar un procedimiento de respaldos que considere los RTO obtenidos en las reuniones con las áreas de negocio. 4. Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
Servicios TI:	Servicios críticos alojados en Servidores Físicos.

9. PLAN DE ACCIÓN – Base de Datos

Componentes:

- Servidor de Base de datos
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el procedimiento de Respaldo de Información (Bases de Datos).
Administrador de Base de Datos o quien haga sus veces	2. Mantener actualizado los parches de seguridad en los servidores.
Experto en Infraestructura y Soporte Técnico	3. Guardar una copia de respaldo en un servidor local y enviar otra copia al proveedor de custodia.
Jefe del AEI	4. Supervisar el cumplimiento de las actividades 1, 2 y 3 establecidas en esta etapa “Antes de la Contingencia”.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Aislar el servidor de base de datos afectado.
Experto en Infraestructura y Soporte Técnico	2. Comunicar al proveedor del Servicio Antimalware y/o al Proveedor del Servicio de Seguridad Gestionada sobre el suceso para queidentifique la fuente y otros posibles equipos comprometidos.
Administrador de Base de Datos o quien haga sus veces	3. Evaluar el nivel de compromiso en el servidor y posibilidad de restablecerlo.
Administrador de Base de Datos o quien haga sus veces	4. Para el caso donde el servidor no pueda restablecerse, deberá reinstalarse.
Administrador de Base de Datos o	5. Levantar la copia de respaldo en el servidor de

quien haga sus veces	Base de Datos reinstalado.
Administrador de Base de Datos o quien haga sus veces	6. Realizar las configuraciones necesarias para la comunicación entre la base de datos y storage.
Coordinador de Desarrollo de Sistemas	7. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Jefe del AEI	8. Supervisar el cumplimiento de las actividades durante la contingencia.
Oficial de Seguridad de la Información	9. Revisar los controles principales de seguridad para la configuración en contingencia.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Revisar el funcionamiento, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo y solicitar el pase a producción de base de datos en caso corresponda.
Administrador de Base de Datos o quien haga sus veces	2. Ejecutar el pase a producción con los cambios solicitados.
Administrador de Base de Datos o quien haga sus veces	3. Validar que la información puede ser consultada en el servidor configurado
Coordinador de Desarrollo de Sistemas	4. Gestionar las pruebas con los usuarios principales de los sistemas de información
Jefe del AEI	5. Supervisar el cumplimiento de las actividades 2, 3 y 4.
Oficial de Seguridad de la Información	6. Revisar el restablecimiento de los controles de seguridad.

10. PLAN ACCIÓN – Sistema de información

Componentes:

- Código fuente de aplicaciones
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Coordinador de Desarrollo de Sistemas	1. Mantener el registro de cambios y versiones del código fuente de las aplicaciones.
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	2. Cumplir con el Respaldo de Información (servidores de aplicaciones, códigos fuente de las aplicaciones).
Experto en Infraestructura y Soporte Técnico	3. Revisar que el antimalware instalado en los servidores se encuentre actualizado.
Experto en Infraestructura y Soporte Técnico	4. Mantener actualizado los parches de seguridad en servidores.
Jefe del AEI	5. Supervisar el cumplimiento de las actividades 1, 2, 3 y 4 establecidas en esta etapa “Antes de la Contingencia”.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Aislar el servidor afectado.
Experto en Infraestructura y Soporte Técnico	2. Comunicar al proveedor del Servicio Antimalware y/o al Proveedor del Servicio de Seguridad Gestionada sobre el suceso para queidentifique la fuente y otros posibles equipos comprometidos.
Experto en Infraestructura y Soporte Técnico	3. Validar con el proveedor antimalware y/o proveedor de Seguridad Gestionada sobre la factibilidad de recuperación del equipo(s) o servicio(s) comprometido(s).
Experto en Infraestructura y Soporte Técnico	4. Para el caso donde el servicio o equipo comprometido no pueda restablecerse, se deberán levantar las copias de respaldo de los servidores más recientes.
Coordinador de Desarrollo de Sistemas	5. Realizar las configuraciones necesarias para la comunicación con la base de datos y storage.
Coordinador de Desarrollo de Sistemas	6. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Oficial de Seguridad de la Información	7. Revisar los controles principales de seguridad para la configuración de contingencia.

c) Después de la Contingencia

Ejecutante	Actividad
Coordinador de Desarrollo de Sistemas	1. Coordinar con el dueño del proceso soportado por el sistema de información, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo.
Coordinador de Desarrollo de Sistemas Administrador de Base de Datos o quien haga sus veces	2. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Coordinador de Desarrollo de Sistemas	3. Realizar pruebas sobre la aplicación.
Jefe del AEI	4. Supervisar el cumplimiento de la actividad 1, 2 y 3.

Plan de Recuperación:	PR-04
Escenario:	En este escenario se considera que el suministro de energía eléctrica del Centro de Datos no se encuentre disponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
Estrategia:	1. Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías. 2. Implementar un tablero de transferencia automático (Bypass) en el Centro de Datos para asegurar la continuidad eléctrica ante fallas del sistema de UPS.

	3. Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y quipos críticos del Centro de Datos. 4. Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías. 5. Realizar el apagado de los equipos en forma ordenada 6. Implementar un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento. 7. Evaluar el implementar un generador eléctrico para proveer energía al Centro de Datos en casos de falla de la red eléctrica pública.
Servicios TI:	Analizando el escenario de riesgo, mientras se cuenta con energía del UPS, se debe realizar el apagado de los equipos. Una vez que retorne la energía eléctrica se realizara el encendido de los equipos en el siguiente orden: 1. Red de datos (Equipos de comunicaciones) 2. Internet y Seguridad Perimetral 3. Sistema de almacenamiento (Storage) 4. Sistema de Virtualización (Hipervisor) 5. Servicio de Autenticación de Red 6. Base de datos. 7. Servidores Virtuales 8. Servidores Físicos

11. PLAN ACCIÓN – Red de Datos (Equipos de comunicación)

Componentes:

- Switches Core, Switches de Servidores, Switches de Distribución.
- Enlace de datos con proveedor de hosting

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación.
Experto en Infraestructura y Soporte Técnico	2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos.
Experto en Infraestructura y Soporte Técnico	3. Mantener un switch administrable de contingencia, que mínimo sea de capa 3 del modelo OSI.
Jefe del AEI Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia.	4. Revisar el cumplimiento de las copias derespaldo y de la operatividad del equipo de contingencia.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el apagado de los equipos de comunicación

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el encendido de los equipos de comunicaciones.
Jefe del AEI	2. Verificar el cumplimiento del procedimiento de recuperación.

12. PLAN ACCIÓN – Internet y Seguridad Perimetral

Componentes:

- TM (parte del servicio de Internet y Seguridad Perimetral)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Supervisar que el proveedor esté realizando respaldos periódicos de la configuración de los equipos UTM.
Experto en Infraestructura y Soporte Técnico	2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el Centro de Datos y el documento con la relación de políticas implementadas.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Reportar al proveedor de Servicio de Internet y Seguridad Perimetral el corte de energía eléctrica.
Experto en Infraestructura y Soporte Técnico	2. Realizar el apagado de los equipos del proveedor.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el encendido de los equipos
Experto en Infraestructura y Soporte Técnico	2. Revisar el correcto funcionamiento del servicio de internet y políticas de navegación
Experto en Infraestructura y Soporte Técnico	3. Verificar la comunicación desde Internet hacia los servicios publicados.

13. PLAN ACCIÓN – Sistema de almacenamiento (Storage):

Componentes:

- Sistema de almacenamiento (Storage, Switches de Fibra Canal).

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento
Experto en Infraestructura y Soporte Técnico	2. Mantener copias de respaldo de la configuración de switches de fibra canal.
Experto en Infraestructura y Soporte Técnico	3. Cumplir con el Respaldo de la Información
Administrador de Base de Datos o quien haga sus veces	4. Mantener actualizada la copia en el sistema de almacenamiento de contingencia de contar con el Hosting de redundante.
Experto en Infraestructura y Soporte Técnico	5. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento
Jefe del AEI	6. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el apagado del sistema de almacenamiento (Storage)

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el encendido del Storage.
Coordinador de Desarrollo de Sistemas	2. Realizar pruebas sobre las aplicaciones
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

14. PLAN ACCIÓN – Hipervisores de Virtualización:

Componentes:

- Servidores: NODO1, NODO2
- Hipervisor: Hyper-V, VMware
- Conexión al Sistema de almacenamiento (Storage).

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información
Experto en Infraestructura y Soporte Técnico	2. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el apagado de los servidores de virtualización

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar en encendido de los servidores de virtualización
Coordinador de Desarrollo de Sistemas	2. Revisar el correcto funcionamiento del servicio de virtualización.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

15. PLAN ACCIÓN – Servicio de autenticación de red (Directorio Activo):

Componentes:

- Servidor virtual del directorio activo (DC1 y DC2).
- Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el procedimiento de Respaldo de la Información.
Experto en Infraestructura y Soporte Técnico	2. Guardar una copia de respaldo en un servidor local y enviar una copia al lugar de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el apagado de los servidores de Directorio Activo

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el encendido de la máquina virtual de Directorio Activo
Coordinador de Desarrollo de Sistemas	2. Revisar el correcto funcionamiento de las máquinas virtuales.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

16. PLAN ACCIÓN – Base de Datos (SQL Server)

Componentes:

- Servidor: DB-PROD1, DB-QA
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información
Administrador de Base de Datos o quien haga sus veces	2. Monitorear el correcto funcionamiento del SQL Server
Experto en Infraestructura y Soporte Técnico	3. Guardar una copia de respaldo en un servidor local y enviar copia al lugar de custodia.
Jefe del AEI	4. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	1. Realizar el apagado de la base de datos

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico Administrador de Base de Datos o quien haga sus veces	1. Encender la base de datos.
Administrador de Base de Datos o quien haga sus veces	2. Validar que la información puede ser consultada.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

17. PLAN ACCIÓN – Servidores Virtualizados:

Componentes:

- Máquinas virtuales
- Licencias de sistemas operativos de servidores
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información.
Experto en Infraestructura y Soporte Técnico	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	4. Realizar el apagado de la máquina virtual

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Encender la máquina virtual.
Experto en Infraestructura y Soporte Técnico	2. Realizar pruebas sobre los servicios del servidor virtual
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

18. PLAN ACCIÓN – Servidores Físicos:

Componentes:

- Servidor: APPS, SRV-DP
- Respaldo de información
- Conexión al Sistema de almacenamiento (Storage)

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Cumplir con el Respaldo de la Información.
Experto en Infraestructura y Soporte Técnico	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.

Jefe del AEI	3. Revisar que se ejecute el Respaldo de la Información

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar el apagado del servidor físico

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Encender el servidor físico.
Experto en Infraestructura y Soporte Técnico	2. Realizar pruebas sobre los servicios del servidor virtual.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

Plan de Recuperación:	PR-05
Escenario:	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos.
Estrategia:	1. Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol (personal alterno), de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto. 2. Entrenar al personal de la OITEC en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos. 3. Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OITEC, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información. 4. Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

19. PLAN ACCIÓN – Personal crítico de TI:

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Establecer instructivos y/o procedimientos para la administración de los servicios críticos

Experto en Infraestructura y Soporte Técnico	2. Mantener los accesos remotos para que en caso se requiera se puedan administrar los servicios informáticos desde lugares externos
Experto en Infraestructura y Soporte Técnico Coordinador de Desarrollo de Sistemas	3. Capacitar a personal alterno en la gestión y operación de los servicios críticos para garantizar la continuidad de la operación.
Jefe del AEI	4. Revisar el cumplimiento de los puntos 1, 2 y 3.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico Coordinador de Desarrollo de Sistemas	1. Comunicar a la jefatura inmediata superior sobre la ausencia del personal especialista.
Experto en Infraestructura y Soporte Técnico Coordinador de Desarrollo de Sistemas	2. Coordinar la conexión remota a los equipos y sistemas, por parte de personal alterno.

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Comunicar el personal reincorporado sobre las acciones tomadas en su ausencia.
Experto en Infraestructura y Soporte Técnico Coordinador de Desarrollo de Sistemas	2. Complementar los instructivos y/o procedimientos en caso sea necesario.
Jefe del AEI	3. Revisar el cumplimiento de los puntos 1, 2

Plan de Recuperación:	PR-06
Escenario:	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o lógica, lo cual puede traer como consecuencia la caída de servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
Estrategia:	1. Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado del Centro de Datos. 2. Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones. 3. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de Datos.
Servicios TI:	4. Analizando el escenario de riesgo, mientras se cuenta con energía del UPS, se debe realizar el apagado de los equipos. Una vez que retorne la energía eléctrica se realizara el encendido de los Red de Datos (Equipos de comunicaciones)

20. PLAN ACCIÓN – Red de Datos (Equipos de comunicaciones):

Componentes:

- Switches Core, Switches de Servidores, Switches de Distribución.
- Enlace de datos con proveedor de hosting

Etapas

a) Antes de la Contingencia:

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación.
Experto en Infraestructura y Soporte Técnico	2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos.
Experto en Infraestructura y Soporte Técnico	3. Mantener un switch administrable de contingencia, que mínimo sea de capa 3 delmodelo OSI.
Jefe del AEI	4. Revisar el cumplimiento de las copias derespaldo y de la operatividad del equipo de contingencia.

b) Durante de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Revisar la operatividad del Switch Core y equipos de comunicación del Centro de Datos. En caso de estar inoperativos realizar el punto2, caso contrario ir al punto 3.
Experto en Infraestructura y Soporte Técnico	2. Realizar las configuraciones de red en el Switch capa 3 de contingencia.
Experto en Infraestructura y Soporte Técnico	3. Reemplazar equipo dañado y probar conectividad con los servidores

c) Después de la Contingencia

Ejecutante	Actividad
Experto en Infraestructura y Soporte Técnico	1. Gestionar con el proveedor de soporte la reparación o reemplazado del equipo averiado
Experto en Infraestructura y Soporte Técnico	2. Configurar el hardware nuevo o reparado.
Jefe del AEI	3. Verificar el cumplimiento del procedimiento de recuperación.

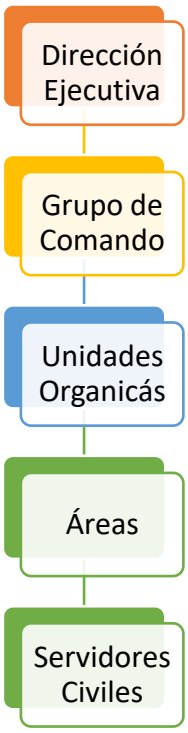
Anexo N.º 02: Procedimientos para la convocatoria del personal involucrado en la ejecución de las actividades críticas

1. Los medios de comunicación a emplear, según orden de prioridad, son:

   a) Mensaje de texto por celular
   b) Mensaje al Chat de WhatsApp del Programa.
   c) Redes sociales y correos electrónicos.
   d) Llamada al teléfono fijo y celular
   e) Cualquier otro medio que permita la comunicación

2. Ejecución de la convocatoria y actividades a desarrollar

   a) El jefe de la UPMP toma la decisión de convocar a los miembros del Grupo de Comando e informa a la Dirección Ejecutiva la situación de la condición de funcionamiento del Programa, recomendando la necesidad de activar el PCO.
   b) En caso de activar el PCO, el jefe de la UPMP coordina, en sesión de Grupo de Comando, con el representante de la UAF la movilización del personal titular que realizará trabajo presencial y mixto.
   c) Los representantes de cada unidad orgánica, que forman parte del Grupo de Comando, solicitarán al personal Titular que realiza Teletrabajo total informar sobre la disponibilidad de su equipo informático y de los aplicativos, a fin de dicho representante informe en la sesión de Grupo de Comando.
   d) En el caso en que el personal titular que realiza teletrabajo total no tenga la disponibilidad de su equipo o de un aplicativo informático, inmediatamente comunica al representante de su órgano o unidad orgánica para que este informe en sesión de Grupo de Comando.
   e) El personal titular que realiza teletrabajo total informará al representante de su unidad orgánica toda situación respecto al desarrollo de las actividades críticas, fotografiando evidencias y que estas serán comunicadas en la sesión de Grupo de Comando
   f) La comunicación se confirma retornando la llamada o mensaje a quien lo hizo, hasta llegar nuevamente al primer emisor o quien inició la llamada.



Anexo 03: Directorio del Grupo de Comando

Grupo de Comando		Unidad Orgánica	Celular / Nombres y Apellidos/ Correo Institucional
01	Jefe de la Unidad de Planeamiento, Modernización y Presupuesto quien lo preside.	UPMP	962648372 / Manuel Palacios Ramos / mpalaciosr@jovenesproductivos.gob.pe
02	Jefe de la Unidad Técnica Operativa de los Servicios para la Empleabilidad	UTO	958142626 / Vanessa Otiniano Rosales/ votiniano@jovenesproductivos.gob.pe
03	Jefe de la Unidad de Acompañamiento e Inserción Laboral	UAIL	975033669 / Jesús Alejandro Aliaga Baldeón / jaliaga@jovenesproductivos.gob.pe
04	Jefe de la Unidad de Administración y Finanzas.	UAF	998997144 / Rusel Emerson Torres Grijalva / torresgrijalva@jovenesproductivos.gob.pe
05	Jefe/a del Área de Informática.	UPMP	949442058 / Hernán Villanueva Zavala / hvillanueva@jovenesproductivos.gob.pe
06	Jefe/a del Área de Recursos Humanos.	UAF	955379017 / Karinna Margarita Esquerre Paz / kesquerre@jovenesproductivos.gob.pe

Anexo 04: Organización para el Desarrollo de las Actividades Críticas

N.°	Actividad crítica	Unidad Responsable	Personal	Escritorios	Sillas personales	Pc /Laptop	Impresoras
1	Planificar, ejecutar y monitorear la capacitación laboral	Unidad Técnico Operativa de los Servicios para la Empleabilidad	3	3	3	3	1
2	Planificar, ejecutar y monitorear la Capacitación y Asistencia Técnica para el Autoempleo Productivo	Unidad Técnico Operativa de los Servicios para la Empleabilidad	2	2	2	2	-
3	Planificar, ejecutar y monitorear la Certificación de Competencias Laborales	Unidad Técnico Operativa de los Servicios para la Empleabilidad	2	2	2	2	-
4	Planificar, ejecutar y monitorear el Acompañamiento e inserción laboral	Unidad de Acompañamiento e Inserción Laboral	3	3	3	3	1
5	Ejecutar el pago de planillas y beneficios	Unidad de Administración y Finanzas	3	3	3	3	1
6	Provisión de Bienes y Servicios a demanda (incluye pago a proveedores)	Unidad de Administración y Finanzas	4	4	4	4	1
7	Mantener la operatividad de los sistemas informáticos, plataformas tecnológicas, servicios y páginas web críticos identificados por las áreas usuarias, con la finalidad de garantizar el procesamiento, la generación y la publicación de los datos y productos	Unidad de Planeamiento, Modernización y Presupuesto	3	3	3	3	-

Anexo 05: Sistema de Comunicaciones de Emergencia

1. Introducción

Ante la ocurrencia de una catástrofe de gran magnitud, los canales normales de comunicaciones serian afectados por la falta de energía eléctrica, por la destrucción física de los elementos que los conforman o por la saturación producto de la desesperación de comunicarse con los familiares haciendo necesario prever otras formas de comunicación, a fin de asegurar el flujo de información entre las diversas unidades del Programa.

2. Objetivo

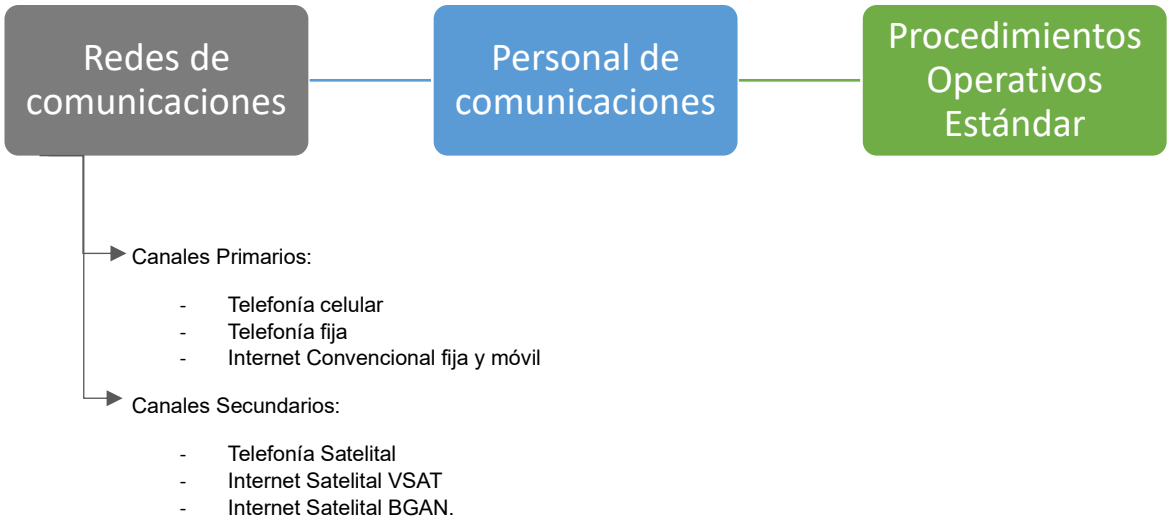
Regular los procedimientos para la implementación y operación de los sistemas de comunicaciones durante los procesos de preparación, respuesta y rehabilitación a las emergencias o desastres; a fin de brindar el flujo rápido y ordenado de las informaciones y comunicaciones de las unidades del Programa.

3. Concepto de Operación

El empleo de los Sistemas de Comunicaciones Convencionales (Canales Primarios) que brindan las empresas proveedoras de servicio de telecomunicaciones en el país deben ser empleadas permanentemente por todas las unidades del Programa.

4. Sistema de comunicaciones

Los sistemas de Comunicaciones están compuestos por 3 elementos básicos:



Anexo 06: Cronograma de Implementación de la Gestión de la Continuidad Operativa

Acciones	Indicador	Meta estimada	2025											
			E	F	M	A	M	JN	JL	A	S	O	N	D
Desarrollar capacidades para la gestión de la continuidad Operativa	Porcentaje de personal capacitado*	100%				X			X			X		
Elaboración, difusión de campañas comunicacionales	Nº de Campañas Comunicaciones	12			X			X			X			X

Anexo 07: Formato de Evaluación de Daños

Ficha Técnica de Evaluación

Sede: …..……..……

Dirección: ……..……..……..…..

Distrito:……Provincia…….……Región: :……

Fecha De Inspección: Día: …….. Mes: …..……..….. Año: ……..……

DATOS DE LA SEDE:

Nombre del responsable: ……..……

Teléfono: ……. Correo Electrónico: ……..

Área del Terreno: …… m² Dimensiones del Terreno:……..……

1. DESCRIPCIÓN Y ESTADO DE LA INFRAESTRUCTURA ACTUAL DE LA SEDE (PISO.....)

Item	Destruido	Parcialmente Dañado	No afectado	Comentarios
AREAS				
Estado de la estructura (Muros, Columnas, Vigas, Techo y Piso)				
Integridad del centro de cómputo				
Salidas de Emergencia				
Escaleras				
Otros				
SERVICIOS				
Agua potable				
Energía eléctrica				
Aire acondicionado				
Comunicación telefónica				
Detectores de Humo				
Extintores				
EQUIPO DE INFORMÁTICA Y COMUNICACIONES				
Switch Core				
Switch de Distribución				
Firewall				
Central telefónica				
Servidores				
UPS				
ARCHIVO				
Documentación				

Conclusiones del análisis de los daños que influyan en la instalación:

……
……
……
…… .

3. SEGURIDAD PARA LA CUSTODIA DE LAS SEDES:

Cuenta con vigilancia: NO ( ) SI ( )
Cuenta con cerco perimétrico: NO ( ) SI ( )

Material: ……..

Firma en señal de Conformidad:

……..…….…… ….. ….……..……..
Nombre del evaluador Nombre del responsable
Sello y Firma Sello y Firma