



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Despacho  
Viceministerial de Justicia

Programa Nacional de  
Centros Juveniles



**PRONACEJ**  
Programa Nacional de  
Centros Juveniles

**PLAN DE CONTINGENCIA INFORMÁTICO DEL PROGRAMA NACIONAL DE CENTROS  
JUVENILES - 2025**

<b>ROL</b>	<b>UNIDAD O SUBUNIDAD/DIRECCIÓN</b>	<b>SELLO Y FIRMA</b>
ELABORADO POR:	SUBUNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	
VALIDADO POR:	UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	
APROBADO POR:	UNIDAD DE ADMINISTRACIÓN	

**PLAN DE CONTINGENCIA INFORMÁTICO DEL PROGRAMA NACIONAL DE  
CENTROS JUVENILES - 2025**

**INDICE**

I. INTRODUCCIÓN .....	3
II. BASE LEGAL .....	3
III. GLOSARIO DE TÉRMINOS .....	4
IV. FINALIDAD .....	5
V. OBJETIVOS .....	5
VI. ÁMBITO DE APLICACIÓN .....	5
VII. ANÁLISIS DE SITUACIÓN ACTUAL .....	6
VIII. ARTICULACIÓN DEL PLAN DE TRABAJO CON EL PEI Y POI .....	11
IX. ACTIVIDADES .....	13
X. PRESUPUESTO .....	23
XI. CRONOGRAMA DE ACTIVIDADES .....	24
XII. RESPONSABILIDAD.....	25
XIII. ANEXOS .....	25

# PLAN DE CONTINGENCIA INFORMÁTICO DEL PROGRAMA NACIONAL DE CENTROS JUVENILES - 2025

## I. INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia a presentarse en el Programa Nacional de Centros Juveniles. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de tecnologías de la información en el menor tiempo e impacto posible.

El Plan de Trabajo de Contingencia permitirá mantener la operatividad frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada.

## II. BASE LEGAL

- 2.1. Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado.
- 2.2. Ley N.º 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)
- 2.3. Ley N.º 29733, Ley de Protección de Datos Personales
- 2.4. Decreto Legislativo N.º 1412, Ley de Gobierno Digital.
- 2.5. Decreto Supremo N.º 115-2022-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres 2022-2030.
- 2.6. Resolución Ministerial N.º 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- 2.7. Resolución Ministerial N.º 046-2013-PCM, Lineamiento que definen el marco de responsabilidad en Gestión de Riesgos de Desastres en las entidades del Estado en los tres niveles de Gobierno.
- 2.8. Resolución Ministerial N.º 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- 2.9. Resolución Ministerial N.º 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- 2.10. Resolución Ministerial N.º 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".
- 2.11. Resolución de Dirección Ejecutiva N.º 086-2023-JUS/PRONACEJ, que aprueba la Directiva N.º 001-2023-JUS/PRONACEJ, "Directiva para la elaboración de Planes de Trabajo del Programa Nacional de Centros Juveniles".

Las referidas normas incluyen sus respectivas modificatorias, de ser el caso.

### III. GLOSARIO DE TÉRMINOS

Para efectos del presente plan se toman en cuenta las siguientes definiciones:

- 3.1. **Antivirus:** programa cuyo objetivo es detectar y/o eliminar virus informáticos.
- 3.2. **Amenaza:** probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.
- 3.3. **Backup:** se refiere a una copia de seguridad o réplica de datos y archivos. Su objetivo es permitir la restauración de la información original en caso de pérdida de datos, fallos del sistema o desastres informáticos.
- 3.4. **Base de datos:** es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
- 3.5. **Hardware:** se refiere a todas las partes tangibles de un sistema informático, sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.
- 3.6. **Incidente:** circunstancia o suceso inesperado que puede afectar el desarrollo normal de una actividad, aun cuando no forme parte de ella. En el contexto del Programa Nacional de Centros Juveniles (PRONACEJ), se entiende como cualquier interrupción o alteración de las condiciones habituales de operación en los procesos informáticos.
- 3.7. **Plan de Contingencia Informático:** es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la institución. Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:
  - 3.7.1. **Antes**, como un plan de prevención para mitigar los incidentes.
  - 3.7.2. **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
  - 3.7.3. **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.
- 3.8. **Plan de Prevención:** es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan.
- 3.9. **Plan de Ejecución:** es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del Plan de Ejecución deben ser completamente claras y definidas.

- 3.10. **Plan de Recuperación:** es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.
- 3.11. **Software:** es el equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.
- 3.12. **Tiempo de recuperación:** es aquel tiempo que demora en desarrollarse un trabajo de recuperación de un servicio determinado.
- 3.13. **Virus informático:** es un malware que tiene por objeto alternar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

#### **IV. FINALIDAD**

Garantizar la continuidad operativa de los servicios de tecnología de la información y de comunicaciones en el PRONACEJ, estableciendo estrategias y procedimientos para su recuperación ante eventos disruptivos, minimizando el impacto en la infraestructura tecnológica y asegurando la rápida restauración de los servicios críticos.

#### **V. OBJETIVOS**

##### **5.1 Objetivo General**

Asegurar la protección, restauración y funcionamiento oportuno de la infraestructura tecnológica, los sistemas de información y la comunicación institucional, contribuyendo a la prestación ininterrumpida y eficiente de los servicios a cargo de la entidad.

##### **5.2 Objetivos Específicos**

- 5.2.1 Identificar, evaluar y gestionar los riesgos informáticos que puedan afectar total o parcialmente la prestación de los servicios institucionales.
- 5.2.2 Definir actividades de prevención, preparación, respuesta y recuperación orientadas a proteger la infraestructura tecnológica y la información institucional frente a incidentes derivados de fallas eléctricas, fenómenos naturales, amenazas cibernéticas, ingeniería social, vandalismo u otras contingencias.
- 5.2.3 Establecer estrategias que aseguren la continuidad de los servicios informáticos y permitan su restablecimiento en el menor tiempo posible tras la interrupción.
- 5.2.4 Determinar los procedimientos, tareas, roles y responsabilidades necesarias para la recuperación de los servicios críticos de tecnología de la información, garantizando su retorno a condiciones normales de operación.

#### **VI. ÁMBITO DE APLICACIÓN**

El presente Plan de Contingencia Informático del PRONACEJ es de aplicación exclusiva para la Subunidad de Tecnologías de la Información y las Comunicaciones (STIC), como responsable de la gestión, administración,

mantenimiento, recuperación y restablecimiento de los servicios informáticos y de comunicaciones institucionales; que comprende los equipos, servidores, software, bases de datos, sistemas de información, equipos de comunicación, redes y demás recursos tecnológicos administrados por la STIC, así como al personal técnico encargado de su operación y soporte.

Las demás unidades de organización del PRONACEJ no intervienen directamente en la ejecución del presente plan; sin embargo, se encuentran involucradas en su aplicación en calidad de usuarias de los servicios informáticos, cuya continuidad, disponibilidad y restablecimiento oportuno resultan esenciales para el desarrollo de sus funciones institucionales.

## **VII. ANÁLISIS DE SITUACIÓN ACTUAL**

El PRONACEJ, a través de la STIC, cuenta con una infraestructura informática que soporta servicios críticos de gestión administrativa, documentaria y operativa de alcance nacional. Dichos servicios incluyen: SGD, SIGAI, SIGA, SIAF, GLPI, correo electrónico institucional, portal web, servidores de archivos y sistemas colaborativos.

Actualmente, esta infraestructura se encuentra alojada principalmente en la sede central, donde operan los servidores físicos y virtualizados, bases de datos, equipos de comunicación (switches, access points, firewalls), servidores de correos, DNS y directorio activo, que son la base para la continuidad de los procesos institucionales.

El estado actual presenta fortalezas como la existencia de infraestructura propia con inventarios actualizados de hardware y software, la implementación de políticas de respaldo de información mediante procedimientos de copias completas, incrementales y diferenciales, controles de seguridad perimetral a través de firewall, uso de antivirus actualizados. Asimismo, se cuenta con personal técnico especializado en servidores, redes, base de datos y soporte.

No obstante, se identifican debilidades y riesgos, principalmente la alta dependencia de la sede central como único centro de datos, la exposición a riesgos endógenos como fallas en cableado estructurado, inoperatividad de servidores, interrupciones de DNS, fallas de correo institucional e inconvenientes eléctricos, así como riesgos exógenos vinculados a sismos, incendios, atentados, pérdida del servicio de internet o ataques externos. La autonomía eléctrica actual está limitada a aproximadamente una hora a través de UPS, lo cual reduce la capacidad de resiliencia frente a apagones prolongados. Aunque existen respaldos, la recuperación total de los servicios puede demorar desde horas hasta días, generando un impacto significativo en la continuidad operativa.

A nivel de oportunidades, la institución cuenta con un centro alternativo en el CJDR – Lima, con virtualización VMware, que constituye una opción viable para la recuperación mínima de operaciones en caso de desastre. También se encuentra alineada con el Sistema Nacional de Gestión del Riesgo de Desastres, así como con los lineamientos de la Ley de Gobierno Digital, lo que abre la posibilidad de modernizar gradualmente la infraestructura tecnológica y fortalecer la transformación digital institucional.

El análisis de riesgos implica mucho más que calcular la probabilidad de que ocurran eventos negativos, por lo que se consideran los siguientes aspectos:

**7.1 Identificación de amenazas;** una amenaza se define como el evento en posible ocurrencia con capacidad de afectar negativamente las instalaciones y actividades del PRONACEJ. Aquellos eventos negativos que puedan afectar el desarrollo normal de las actividades que se afectan en las unidades de organización del PRONACEJ, se conocen como amenazas de tipo **endógenos** y requieren de un plan de contingencia para su prevención y atención (tubería de agua y desagüe, inconvenientes eléctricos, cableados de red dañado, etc.).

Por otra parte, el desarrollo de actividades ajenas al tema informático sumadas a los fenómenos naturales puede llegar a constituirse en elementos perturbadores del medio ambiente y posibles generadores de emergencia, estas amenazas son de tipo **exógenos** y entre ellas se consideran los incendios, sismos, atentados y robo.

Los equipos informáticos y de comunicaciones están expuestos a distintas clases de riesgos, que pueden afectar su normal funcionamiento, los problemas potenciales se clasifican en los siguientes factores.

## **7.2 Factores Endógenos:**

### **7.2.1 Problemas con la tubería y desagüe:**

Este factor no ocurre frecuentemente en las diferentes unidades de organización del PRONACEJ, pero en caso de que se llegara a dar, los daños que causaría serían cuantiosos, a esto se agrega el peligro de que las computadoras no cuentan con fundas impermeables que minimicen estos inconvenientes.

### **7.2.2 Daños de cableado de red:**

Los equipos informáticos del PRONACEJ se encuentran integrados a la red de cómputo institucional y acceden a sus servicios mediante dos tipos de conexión: cableada, a través de cables UTP categoría 6 protegidos por canaletas plásticas (de pared o de piso), e inalámbrica (Wireless). La amenaza identificada está asociada a la interrupción o inaccesibilidad de la red, la cual puede afectar desde un equipo individual hasta un área completa, e incluso, en el escenario más crítico, a toda la sede central del PRONACEJ. Entre las principales causas de esta amenaza se encuentran cortes, quiebres o estiramientos de cables, contacto con cables eléctricos, sulfatación de conectores y, en el caso de las conexiones inalámbricas, ruidos, vibraciones e interferencias.

### **7.2.3 Fallas de equipos de comunicación:**

La red de cómputo llega a todas las unidades de organización del PRONACEJ a través de los equipos de comunicaciones, ya sea por Switches o Access Point, ubicados estratégicamente en los sectores norte, centro, y sur de las instalaciones.

La alteración y/o inoperatividad de algunos de estos componentes se traducirían en que determinadas unidades de organización no tengan acceso a los servicios que brinda la red del PRONACEJ.

#### **7.2.4 Inoperatividad de los servidores de comunicación:**

Es una situación fortuita, ocasionada por fallas de software y/o hardware, que acarrea la imposibilidad de acceder a los servicios de internet como: correo electrónico, portal institucional, sistemas administrativos (Sistema Integrado de Gestión Administrativa (SIGA), Sistema de Gestión Documentaria (SGD), Sistema Integrado de Administración Financiera (SIAF), Sistema Integrado de Gestión de la Administración de Inmuebles (SIGAI), entre otros.), transferencias de archivos, etc.

#### **7.2.5 Inoperatividad en los servicios de la Base de Datos:**

A partir del año 2024, el PRONACEJ cuenta con un sistema SGD, el cual permite optimizar los procesos y tener un mejor flujo de la documentación de la institución optimizando los recursos con cero papel, así como un eficiente uso y gestión administrativa de la información de la institución, usando nuestros servidores.

Todos los aplicativos y sistemas de información que almacenan sus datos en estos servidores estarían impedidos de acceder a su información y a todos los aplicativos.

#### **7.2.6 Inoperatividad del Servidor DNS Interno:**

El PRONACEJ cuenta con un servidor DNS propio encargado de resolver los nombres de dominio internos; una eventual falla en este servicio podría originar interrupciones y problemas en la red.

#### **7.2.7 Inoperatividad del Servidor de Correos:**

Se cuenta con un servidor de correo a través del cual circulan todos los servicios de mensajería; una eventual falla en este sistema ocasionaría la interrupción de los servicios de envío y recepción de correos corporativos.

#### **7.2.8 Inoperatividad del Servidor de Archivos:**

Se cuenta con un servidor de archivos que permite compartir y acceder a la información entre las diferentes unidades organizacionales; una falla en este servicio ocasionaría la imposibilidad de acceder a los archivos almacenados y compartidos.

#### **7.2.9 Inoperatividad del servidor de Directorio Activo:**

El servidor de directorio activo (Active Directory) permite la gestión centralizada de equipos, usuarios y grupos, la cual gestiona entre otras cosas, los inicios de sesión y las políticas de acceso a los usuarios que

laboran en la institución, cuya falla originaría que los usuarios no puedan acceder a la red interna de PRONACEJ.

#### **7.2.10 Inconvenientes eléctricos:**

Por razones de seguridad interna la Unidad de Administración (UA), en coordinación con la STIC, debe disponer la supervisión y mantenimiento periódico de las instalaciones, dispositivos y conexiones de la red eléctrica de cómputo (cables, circuitos, pozo a tierra, grupo electrógeno, entre otros).

#### **7.2.11 Acción de virus informáticos:**

Se consideran a los virus informáticos como amenazas endógenas cuando se filtran desde el interior de la institución a través del uso de USB, discos externos, CD, DVD, mala manipulación y mal uso de descargas a través del internet por parte del usuario y amenazas como exógenas cuando se filtran a través del correo electrónico y la navegación en internet.

Es importante señalar que las computadoras de la Institución cuentan con el servicio de Antivirus, el cual es actualizado periódicamente.

### **7.3 Factores Exógenos**

#### **7.3.1 Corte de fluido eléctrico:**

Todos los equipos informáticos usan la electricidad por lo que su ausencia conduce directamente a una inoperatividad de los mismos.

#### **7.3.2 Corte de Servicio de Circuito Digital:**

El PRONACEJ cuenta con un circuito digital para la transmisión/recepción de datos con un ancho de banda de 500 Mbps. Un corte temporal o definitivo de este tipo de servicio aislaría tecnológicamente a la institución a nivel nacional.

#### **7.3.3 Inoperatividad del Servidor DNS Externo:**

El servidor DNS que resuelve los nombres de dominios de internet está bajo la administración del Proveedor de Internet "Bitel S.A." cuya inoperatividad se traduciría en la imposibilidad de acceder a internet.

#### **7.3.4 Acción de virus informáticos:**

Se consideran los virus informáticos como amenazas exógenas debido a que se pueden alterar el normal desenvolvimiento de las actividades, infiltrándose desde el exterior a través del correo electrónico, archivos adjuntos infectados o con la acción de navegar en internet.

#### 7.3.5 Incendios:

La UA del PRONACEJ, a través de la Subunidad de Abastecimiento (SA), cuenta con personal capacitado que incluye periódicamente a los brigadistas designados en cada unidad y subunidad de la institución, en el uso de extintores destinados a la protección exclusiva de los equipos de cómputo.

#### 7.3.6 Sismos:

Las unidades de organización del PRONACEJ, se encuentran en un inmueble de cinco pisos, por lo que los daños que podrían causar al parque informáticos serían altos.

#### 7.3.7 Atentados:

Son actos criminales efectuados por personas o grupos, el PRONACEJ cuenta con personal de seguridad, quienes se encuentran ubicados estratégicamente en las diversas áreas, para realizar labores de control y vigilancia a efectos de evitar cualquier robo de diversa naturaleza.

#### 7.3.8 Hackers:

Es el individuo que usa sus habilidades y recursos para invadir sistemas informáticos ajenos, la red del PRONACEJ cuenta con un Firewall que controla los accesos desde fuera de la entidad.

### 7.4 Factores de Vulnerabilidad:

La vulnerabilidad es el grado relativo de sensibilidad, que un sistema tiene respecto a una amenaza determinada. Los factores de vulnerabilidad dentro de un análisis de riesgo, permite determinar cuáles son los efectos negativos; para efectos del análisis de riesgos se consideran los siguientes factores de vulnerabilidad:

7.4.1 **Víctimas:** se refiere al número y clase de afectados (trabajadores, personas de emergencia, etc.).

7.4.2 **Daño Ambiental:** incluye los impactos sobre el aire y la comunidad a consecuencia de la emergencia.

7.4.3 **Pérdida de Materiales o Económicos:** representados en instalaciones, equipos, multas, indemnizaciones, entre otros.

### 7.5 Aceptabilidad

En cuanto a la aceptabilidad a los riesgos, los escenarios son:

Aceptabilidad del Riesgo		
Acceptable	Tolerable	Inaceptable
Un escenario situado en esta región de la matriz significa que la combinación de probabilidad - gravedad no representa una amenaza.	Significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, estas tienen una probabilidad de segundo nivel.	Se requiere siempre desarrollar acciones prioritarias e inmediatas para su gestión, debido al alto impacto que tendrían sobre el sistema.

## 7.6 Niveles de Planeación

La aceptabilidad de riesgos está directamente relacionada con los niveles de Planeación de contingencias, de la siguiente manera:

Niveles de Planeación		
No Plan	Plan General	Plan Detallado
Significa que la combinación de probabilidad-gravedad no representa una amenaza.	Un escenario situado en esta región de la matriz significa que, aunque debe diseñarse una respuesta para dichos casos, ésta debe ser solo de carácter general.	Un escenario situado en esta región de la matriz significa que se requiere siempre diseñar una respuesta detallada a las contingencias y que es preciso realizar inversiones particulares para cada uno de estos escenarios.

## VIII. ARTICULACIÓN DEL PLAN DE TRABAJO CON EL PEI Y POI

### 8.1 ARTICULACIÓN CON EL PEI

El Plan de Contingencia Informático del PRONACEJ 2025 tiene como propósito garantizar la continuidad de los servicios críticos de tecnología de la información, en alineación con el Plan Estratégico Institucional (PEI) 2025-2030 del Ministerio de Justicia y Derechos Humanos (MINJUSDH), aprobado mediante Resolución Ministerial N.º 262-2025-JUS, el cual define siete (07) Objetivos Estratégicos Institucionales (OEI) y diecinueve (19) Acciones Estratégicas Institucionales (AEI).

En particular, la relación más directa es con el siguiente objetivo:

- **OEI 05: DESARROLLAR LA POLITICA CRIMINOLÓGICA COHERENTE E INTEGRAL EN LA SOCIEDAD**

El Plan de Contingencia se articula con este objetivo al establecer procedimientos específicos de prevención, respuesta y recuperación tecnológica frente a incidentes que puedan afectar la operatividad institucional, tales como fallas en servidores, redes, correo, bases de datos, ataques informáticos, sismos o incendios. Su implementación garantiza la continuidad y disponibilidad de los sistemas críticos utilizados en la gestión institucional, asegurando la ejecución oportuna de los procesos vinculados a la atención socioeducativa, la gestión administrativa y el cumplimiento de las funciones estratégicas del programa.

## 8.2 ARTICULACIÓN CON EL POI

El Plan Operativo Institucional (POI) 2025 – Versión 1 del Ministerio de Justicia y Derechos Humanos, aprobado mediante Resolución Ministerial N.º 262-2025-JUS, se articula con el Plan Estratégico Institucional (PEI) y establece las Actividades Operativas e Inversiones (AOI) necesarias para el cumplimiento de los objetivos estratégicos institucionales, a los cuales se encuentra alineado el PRONACEJ.

En ese marco, el POI 2025 contempla, para el Programa Nacional de Centros Juveniles (PRONACEJ), inversiones y actividades operativas alineadas al OEI 05, orientadas a “Desarrollar la política criminológica coherente e integral en la sociedad”.

Como parte de este enfoque, el Plan de Contingencia Informático constituye un instrumento operativo complementario al POI, dado que:

- Contribuye directamente al cumplimiento del OEI 05 y a la ejecución de las AOI relacionadas con la gestión de riesgos, la continuidad de los servicios tecnológicos y la sostenibilidad operativa del programa.
- Asegura la disponibilidad y recuperación de los sistemas informáticos y plataformas institucionales necesarios para la ejecución de las actividades operativas, administrativas y socioeducativas programadas en el POI 2025.

Objetivo Estratégico Institucional		Acción Estratégica Institucional		Vinculación con el Plan Operativo Institucional		Unidad Responsable
Código	Enunciado	Código	Enunciado	Nombre de la Actividad Operativa del POI	Nombre de la Actividad articulada del PT	
OEI.05	Desarrollar la política criminológica coherente e integral en la sociedad.	AEI 05.01	Atención diferenciada efectiva a adolescentes en riesgo infractor y en conflicto con la ley penal.	Desarrollo e implementación de sistemas informáticos para la mejora de los procesos	Actividades previas al desastres: <ul style="list-style-type: none"> <li>• Sistemas de Información</li> <li>• Obtención y Almacenamiento de los Respaldos de Información</li> <li>• Políticas (Procedimientos de backups)</li> </ul> Actividades durante el desastre: <ul style="list-style-type: none"> <li>• Plan de emergencia</li> <li>• Formación de equipos</li> </ul> Actividades después del desastre: <ul style="list-style-type: none"> <li>• Evaluación de daños.</li> <li>• Priorización de Actividades del</li> </ul>	STIC

Objetivo Estratégico Institucional		Acción Estratégica Institucional		Vinculación con el Plan Operativo Institucional		Unidad Responsable
Código	Enunciado	Código	Enunciado	Nombre de la Actividad Operativa del POI	Nombre de la Actividad articulada del PT	
					Plan de Contingencia. <ul style="list-style-type: none"> <li>• Escenarios considerados para el Plan de Contingencia.</li> <li>• Accesos remotos.</li> </ul>	

## IX. ACTIVIDADES

El plan de contingencia informático se clasifica en tres (3) fases:

### 9.1 Actividades previas del desastre

Son todas las actividades de planeamiento, preparación, entretenimiento, mantenimiento preventivo y correctivo del parque informático y ejecución de las actividades de resguardo de la información.

Para poder efectuar en forma óptica y en el menor tiempo posible las actividades, se debe conocer lo siguiente:

- Reconocer el ambiente donde se encuentra los servidores críticos del PRONACEJ y el saber identificar a cada uno de ellos.
- Conocer los procedimientos a analizar para ofrecer los servicios críticos del PRONACEJ.
- Gestionar adecuadamente los activos del software para contar con un inventario de cada computadora de los usuarios, que faciliten una rápida identificación y restauración del software instalado.

Mantenimiento Preventivo por Equipo Informático			Responsable
Computadoras	Revisión, limpieza interna y externa de todos los componentes, revisión de virus.	1 vez al año	Soporte Técnico
Laptops	Acciones Preventivas/Correctivas		
Impresoras	Limpieza Interna y configuración de software	1 vez al año	
Servidores	Se realiza un monitoreo a través de acciones manuales en la consola del servidor y limpieza interna y actualizaciones.	1 vez por año	Administrador de Infraestructura de Servidores
Comunicaciones	Mantenimientos de equipos de red, swicht, cableado, actualizaciones	1 vez por año	Administrador de redes

### 9.1.1 Sistemas de Información:

Se detallan la relación de los niveles de prioridad con su puntaje que se aplicaran a los sistemas desarrollados por la STIC.

Niveles de Prioridad de Sistemas de Información	
Prioridad	Puntaje
Baja	1
Media	2
Alta	3

A continuación, se muestra la lista de Sistemas de Información ordenados por prioridad de restauración, que son necesarios para garantizar una continuidad de la operatividad y servicios que ofrece el PRONACEJ.

SISTEMAS DE INFORMACIÓN/SERVICIOS IMPLEMENTADOS						
SISTEMA DE INFORMACIÓN	PROVEEDOR	PLATAFORMA	LENGUAJE DE PROGRAMACIÓN	USUARIOS	PRIORIDAD	RESPONSABLE
DIRECTORIO ACTIVO DNS LOCAL	DESARROLLO PROPIO	WINDOWS SERVER		TODAS LAS UNIDADES	3	Administrador de servidores
DIRECTORIO ACTIVO SECUNDARIO	DESARROLLO PROPIO	WINDOWS		TODAS LAS UNIDADES	1	Administrador de servidores
CORREO	DESARROLLO PROPIO	ZIMBRA - LINUX	PHP, JAVA	TODAS LAS UNIDADES	3	Administrador de servidores
SIAF	MEF	WINDOWS SERVER	VISUAL FOXPRO	STIC, SCF, SA, UA Y UPPM	3	Administrador de servidores
FILE SERVER	DESARROLLO PROPIO	WINDOWS SERVER		TODAS LAS UNIDADES	2	Administrador de servidores
SIGA	MEF	WINDOWS SERVER	POWERBUILDER Y BASE DE DATOS SQL SERVER	TODAS LAS UNIDADES	3	Administrador de servidores
SIGAI – PRODUCCION	TERCERO	LINUX	JAVA	TODAS LAS UNIDADES	3	Administrador de servidores
SIGAI – QA	TERCERO	LINUX	JAVA	TODAS LAS UNIDADES	1	Administrador de servidores
SGD	TERCERO	WINDOWS SERVER	SQL SERVER	TODAS LAS UNIDADES	3	Administrador de servidores
SGD	TERCERO	LINUX	JAVA	TODAS LAS UNIDADES	3	Administrador de servidores
MESA DE PARTES VIRTUAL	DESARROLLO PROPIO	LINUX	PHP POSTGRES	USUARIOS EXTERNOS	2	Desarrollador
CONTRATACIONES MENORES	DESARROLLO PROPIO	LINUX	POSTGRES	TODAS LAS UNIDADES Y USUARIOS EXTERNOS	2	Desarrollador
RENDICION DE CAJA CHICA	DESARROLLO PROPIO	LINUX	POSTGRES	TODAS LAS UNIDADES	2	Desarrollador
GLPI	DESARROLLO PROPIO	LINUX	PHP MYSQL	STIC	1	Administrador de servidores
NETXCLOUD	DESARROLLO PROPIO	LINUX	PHP MYSQL	STIC	1	Administrador de servidores
STD	DESARROLLO PROPIO	LINUX	PHP	TODAS LAS UNIDADES	1	Administrador de servidores
STD	DESARROLLO PROPIO	WINDOWS SERVER	SQL SERVER	TODAS LAS UNIDADES	1	Administrador de servidores

### 9.1.2 Obtención y Almacenamiento de los Respaldos de Información

La STIC realiza copias de respaldo o backups, de:

- Base de Datos (SGD, SIGAI, SIAF, SIGA, GLPI, MODULOS)
- Sistemas de Gestión (SIGAI, SIAF, SIGA, CAJA CHICA, ETC)
- Aplicativo (SGD, SIGAI, MESA DE PARTES VIRTUAL)
- Correo Corporativos, dependiendo de la disponibilidad del servidor.
- Archivos de Trabajo cuando se solicitan y dependiendo la disponibilidad de los servidores.

Las copias de respaldo se presentan en el Anexo N.º 1.

Se efectuarán de tres (3) formas:

- **Respaldo Completo:** copia completa de información.
- **Respaldo Incremental:** copia de todos los cambios o adicionales que se realizan a determinada información.
- **Respaldo Diferencial:** copia de cambios o adicionales que se realizan a determinada información respecto al respaldo completo, después de cierto periodo de tiempo.

### 9.1.3 Políticas (Procedimientos de backups)

La STIC, tiene establecido procedimientos para obtener copias de seguridad de Base de Datos, Sistemas de gestión, aplicativos y correo electrónico.

El procedimiento se presenta en el Anexo N.º 2.

## 9.2 Actividades durante el desastre

### 9.2.1 Plan de Emergencia

La STIC, proporciona una relación de su personal, la misma que será utilizada en caso de producirse algún incidente informático.

#### **Pasos a seguir en caso de emergencia**

Se deberán seguir los siguientes pasos:

- Determinar la ubicación del incidente, estimar el tamaño y el tipo de incidente.
- Llevar a cabo acciones específicas para controlar la armonía informática.
- Notificar la ocurrencia a los responsables de la STIC.
- Modificar las operaciones para evitar la ocurrencia potencial del incidente.
- Documentar el incidente.

A continuación, se muestra un cuadro de resumen de procedimientos durante la emergencia:

Procedimientos durante la Emergencia			
Horario	Ocurrencia	Acción a Seguir	Responsable en atender el incidente
Laboral	Problemas en el funcionamiento de computador personal y red de comunicaciones.	Avisar a la STIC, vía teléfono y/o personalmente.	Equipo de la Subunidad de Tecnologías de la Información y las Comunicaciones
Laboral	Problemas con el portal institucional, correo corporativo e internet.	Avisar a la STIC, vía teléfono y/o personalmente.	Equipo de la Subunidad de Tecnologías de la Información y las Comunicaciones

### 9.2.2 Formación de Equipos

La UA, a través de la SA, cuenta con brigadistas designados por los responsables de cada Unidad, quienes actúan de manera inmediata en la lucha contra incendios, evacuación y primeros auxilios. Asimismo, hacen uso de los extintores contra incendios, mientras que la STIC se encarga de la protección de los recursos informáticos de acuerdo con la clasificación de prioridades.

Equipos Mínimos de Respuestas	Responsable
Equipos de cómputo	Equipo de Soporte Técnico
Impresoras multifuncionales	Equipo de Soporte Técnico
Servidores	Administrador de Servidor
Base de Datos	Desarrollador web
Aplicativos	Desarrollador web
Swiches Administrables	Administrador de redes
Access Point	Administrador de redes
Cables de Red, Access Point	Administrador de redes

## 9.3 Actividades después del desastre

### 9.3.1 Evaluación de Daños

Inmediatamente después que el siniestro haya concluido, los brigadistas y el personal de la STIC, realizarán la evacuación de los bienes materiales, equipos, y sistemas de información que se hayan visto afectados, indicando cuales pueden ser recuperados y en cuanto tiempo.

### 9.3.2 Priorización de Actividades del Plan de Contingencia

A fin de habilitar los ambientes y poner en funcionamiento en el término perentorio los equipos, sistemas operativos y sistemas de aplicación de la institución. En materia de informática se dará prioridad a las actividades estratégicas y urgentes, las cuales son:

- Habilitación de servidores si fuera el caso que estén dañados.
- Restauración del último Backups de datos de los sistemas en producción.
- Reinstalación de los sistemas de información de acuerdo al cuadro de prioridades en los equipos de cómputo.
- Reinstalación de Sistemas Operativos y Software Base en los términos que se encuentren operativos en ese momento, si es que presentan problemas.
- Puesta en marcha del Centro de Datos de Respaldo alternativo (Bakups).

Acciones Correctivas a tomar Después del Desastre				
Equipo Informático Afectado	Acción Correctiva	Responsable	Tiempo Estimado	Dependencia
Equipos de Red: Hub, Switch genérico	Se reemplazarán con Switch, Router inalámbrico (Si hubiera)	Administrador de redes	60 min	STIC
Impresoras: de tinta o laser	Se reemplazan con impresoras del mismo tipo, si hay disponibilidad (si hubiera), caso contrario se utilizará impresoras de red de la misma área o de otras áreas	Equipo de Soporte Técnico	30 min	STIC
Equipos de Comunicaciones: Switches layer 2	Se reemplazará con switches de contingencia que se tiene actualmente dentro de la entidad, con la finalidad de tenerlo como contingencia para un reemplazo de algún equipo inoperativo.	Administrador de redes	120 min	STIC
Computadoras	Se reemplazarán con equipos disponibles en el stock de equipos informáticos (si hubiera), los equipos de garantía que presentan fallas de coordinará con el proveedor.	Equipo de Soporte Técnico	40 min	STIC
Servidores	Se reemplazarán con equipos virtualizados que se tiene como contingencia.	Administrador de Servidores	8 h	STIC

### 9.3.3 Escenarios considerados para el Plan de Contingencia

- Falla de comunicación entre la máquina del usuario y los servidores del PRONACEJ.
- Falla de un servidor.
- Interrupción del fluido eléctrico durante la ejecución de los procesos.

- Pérdida de comunicación (interconectividad) entre las sedes del PRONACEJ.
- Pérdida del servicio de internet.

La evaluación y administración de estos riesgos van a permitir al PRONACEJ:

- Desarrollar estrategias de recuperación y respaldo de decisiones operacionales, tecnológicas y humanas.
- Identificar los controles existentes y los nuevos controles a implementar para minimizar los riesgos, evaluando el costo/beneficio de dichos controles.
- Planificar la Seguridad de la Información.

**ESCENARIO I: NO HAY COMUNICACIÓN ENTRE EQUIPO DE USUARIO Y EL SERVIDOR DE LA INSTITUCIÓN PRONACEJ.**

✓ **Responsables de resolver la incidencia:**

- a) Equipo de Soporte Técnico.
- b) Administrador de redes.
- c) Administrador de servidores.

✓ **Impacto**

Impacto	Área afectada
No se puede trabajar con los recursos de la red del PRONACEJ.	Área en que labora el usuario
Interrupción de sus actividades	Área en que labora el usuario

Tiempos aceptables de caída de los sistemas informáticos

Tiempo Aceptable de Caída	
Recurso (Sistemas)	Prioridad de recupero
Sistema SGD, SIAF, SIGA, SIGAI	ALTO
Mesa de Partes Virtual, Contrataciones Menores y Caja Chica	MEDIO
Servidor de archivos	MEDIO
Servidor de Directorio Activo Principal	ALTO
Servidor de Directorio Activo Secundario	BAJO
Servidor de Correos	ALTO
GLPI	BAJO
Nextcloud	BAJO
STD	BAJO
Internet	ALTO

✓ **Recursos de Contingencia**

Componentes de reemplazo:

- a) Tarjeta de red
- b) Conector RJ-45
- c) Jack RJ-45
- d) Testeador
- e) Herramientas de cableado estructurado.

✓ **Procedimiento**

- a) El usuario hace su requerimiento de incidencia de red.
- b) El equipo de Soporte Técnico identifica el problema y ve los posibles factores:
  - Problema de Patch cord.
  - Problema de la tarjeta de red.
  - Problema del cable UTP.
  - Problema del equipo de comunicaciones (Switch) ubicado en el gabinete.
- c) Identifica el factor del problema, y realiza los cambios necesarios.
- d) Hace el testeo nuevamente para la verificación de la red, con la finalidad que el usuario continúe con sus labores correspondientes.

**ESCENARIO II: FALLA DE UN SERVIDOR CRÍTICO**

✓ **Responsables de resolver la incidencia:**

- a) Administrador de redes.
- b) Administrador de Servidores.

✓ **Impacto**

Impacto	Área afectada
Paralización de los Sistemas o aplicaciones que se encuentran en los servidores que presentan fallas	Todas las áreas
Posible pérdida de Software y Hardware	STIC
Pérdida del proceso automático de backup y restore.	STIC
Interrupción de las operaciones	STIC

Tiempos aceptables de caída de las bases de datos de los sistemas informáticos.

Tiempo Aceptable de Caída	
Recurso	Prioridad de recuperacion
Servidor de BASE DE DATOS	ALTO

Tiempo Aceptable de Caída	
Recurso	Prioridad de recupero
Servidor WEB	ALTO
Servidor de aplicaciones – SISTEMAS	ALTO
Servidor de Controlador de dominio Primario	ALTO
Servidor de Correo	ALTO
Servidor SIAF	ALTO
Servidor FILE SERVER	ALTO
Servidor de BACKUP	ALTO

✓ **Factores:**

- a) Error físico de disco del Servidor (RAID)
- b) Error de Memoria RAM.
- c) Error de tarjeta controladora de discos.

✓ **Recursos de Contingencia**

- a) Componente de reemplazo (Memoria, disco duro, servidor virtualizado de contingencia)
- b) Backup diario de información del Servidor.

✓ **Procedimiento**

**a) Error físico de disco del servidor (RAID)**

1. Ubicar el disco malogrado
2. Avisar a los usuarios que deben salir del sistema.
3. Deshabilitar la entrada al sistema para que el usuario no reintente el ingreso.
4. Bajar el sistema y apagar el equipo
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle la partición correspondiente.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema a los usuarios.

**b) Error de Memoria RAM**

1. Avisar a los usuarios que deben salir de los sistemas.
2. Se realizará el apagado del Servidor.
3. Ubicar las memorias RAM malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, con la finalidad de evitar que los usuarios ingresen al prender el servidor.
6. Realizar las pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar las entradas para estaciones en las cuales se realizarán las pruebas.

7. Probar los sistemas que están en red en las diferentes estaciones.
8. Finalmente, una vez realizado todas las pruebas, habilitar las entradas al sistema para los usuarios.

**c) Error de tarjeta controladora de disco**

1. Avisar a los usuarios que deben salir de los sistemas.
2. Se realizará el apagado del Servidor.
3. Ubicar las memorias RAM malogradas.
4. Ubicar la posición de la tarjeta controladora.
5. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra similar o igual.
5. Retirar la conexión del servidor con el concentrador, con la finalidad de evitar que los usuarios ingresen al prender el servidor.
6. Realizar las pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar las entradas para estaciones en las cuales se realizarán las pruebas.
7. Finalmente, una vez realizado todas las pruebas, habilitar las entradas al sistema para los usuarios.

**d) Error total del servidor**

1. Ubicar el servidor de contingencia que contiene los servicios y sistemas informáticos.
2. Restaurar el último backup del aplicativo y base de datos
3. Realizar pruebas locales
4. Poner en producción dentro de la red de PRONACEJ
5. Configurar las nuevas rutas (en caso haya) en los equipos de cómputo de los usuarios.

**ESCENARIO III: INTERRUPCIÓN DE FLUIDO ELÉCTRICO**

✓ **Responsables de resolver la incidencia:**

- a) Administrador de redes.
- b) Administrador de Servidores.

✓ **Impacto**

Impacto	Área afectada
Cierre inapropiado de la base de datos	Todas las áreas
Finalización incompleta de los backups	Todas las áreas
Falla de un componente de equipo servidor	Todas las áreas
Pérdida total o parcial de la operatividad de los sistemas	Todas las áreas

✓ **Recursos de Contingencia**

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores con motores de base de datos.

Por tal motivo, es necesario revisar continuamente el estado de las baterías UPS. Dichas baterías deben garantizar una autonomía de aproximadamente una (1) hora.

✓ **Procedimiento**

1. Se tiene un UPS de 6KVA, el cual está configurado cuando se produce una interrupción de fluido eléctrico, para el apagado de los servidores de una manera automática y correcta.
2. Posteriormente una vez restablecido el fluido eléctrico, se realiza el encendido manual del UPS y de los servidores.
3. Se verifica el funcionamiento de los servidores.

**ESCENARIO IV: PÉRDIDA DE SERVICIO DE INTERNET**

✓ **Responsables de resolver la incidencia:**

- a) Administrador de Servidores.
- b) Administrador de redes.

✓ **Impacto**

Impacto	Área afectada
Interrupción de la recepción y envío de información, mensajes y data a nivel nacional e internacional	Todas las áreas

**Se puede presentar por tres (3) factores:**

- a) Falla de hardware o software del equipo Router del ISP ubicado en el centro de datos.
- b) Falla del equipo Switch Core de comunicaciones de la Institución PRONACEJ.
- c) Problemas con el ISP.

✓ **Recursos de Contingencia**

Utilización del segundo enlace de fibra óptica que brinda el proveedor.

✓ **Procedimiento**

1. El procedimiento comienza con el inicio de un problema de conexión. El primer paso es un corte del servicio de internet.
2. A continuación, se realiza un diagnóstico para determinar si la falla es del Switch Core.
3. Si no es un problema interno, el siguiente paso es comunicarse con el ISP (Proveedor de Servicios de Internet) para que resuelvan el problema.
4. Si es un problema interno, se deben realizar diagnósticos de software y hardware para identificar la causa exacta del fallo. Una vez encontrada, se procede a un cambio de componente o configuración para restablecer el servicio.

#### **9.3.4 Acceso Remoto**

- Los accesos remotos serán habilitados a solicitud de las unidades de organización del PRONACEJ.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le habilitará un nuevo equipo, dependiendo de la disponibilidad que tenga la STIC.
- El usuario del acceso remoto deberá observar de manera estricta las disposiciones descritas en el presente plan.
- Las unidades de organización supervisan el buen uso del acceso remoto habilitado.
- El usuario debe comunicar cualquier ocurrencia en el desarrollo de su trabajo remoto.
- El usuario debe cumplir con la regularización sobre la seguridad, protección y confiabilidad de la información.

#### **9.3.5 Retroalimentación del Plan de Contingencia**

El plan de contingencia es un documento de gestión, que posee contenidos que cambian en el tiempo, vale decir que van acorde con las emergencias que se podrían suscitar y con los cambios tecnológicos de los equipos informáticos.

### **X. PRESUPUESTO**

Las actividades contempladas en el presente plan se ejecutarán con cargo a los recursos presupuestales asignados en la Actividad Operativa vinculada a la Gestión de los Sistemas de Información, sin generar demanda adicional de financiamiento. Dichos recursos han sido programados en el marco del Plan Operativo Institucional (POI) 2025, asegurando su consistencia con el Presupuesto Institucional de Apertura (PIA).

De este modo, las acciones orientadas a la continuidad de los servicios informáticos, la administración de los sistemas de información y la atención de posibles contingencias tecnológicas, se financiarán mediante la optimización de los recursos disponibles, garantizando la sostenibilidad y eficiencia en la ejecución de las medidas previstas.

Asimismo, se precisa que toda implementación, mantenimiento y mejora vinculada a la gestión del riesgo informático se desarrollará respetando los lineamientos técnicos y presupuestales aprobados por la Unidad Ejecutora correspondiente, en concordancia con los objetivos estratégicos institucionales y sectoriales.

## XI. CRONOGRAMA DE ACTIVIDADES

N°	OBJETIVO ESPECIFICO	ACTIVIDADES	UNIDAD DE MEDIDA	META PROGRAMADA	PRESUPUESTO (S/.)	RESPONSABLE	CRONOGRAMA		
							TRIMESTRE IV		
							OC	NOV	DIC
1	Identificar, evaluar y gestionar los riesgos informáticos	Levantamiento y actualización del inventario de activos (hardware, software, servidores, redes) y clasificación de sistemas por prioridad de restauración (Alta/Media/Baja) y tiempos aceptables de caída (RTO)	Informe	1	S/ 10,000.00	Equipo de soporte técnico			1
		Identificación de amenazas y factores endógenos/exógenos (fallas eléctricas, cableado, servidores, DNS, correo, BD; incendios, sismos, pérdida de Internet, malware externo)	Informe	1	S/ 23,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores			1
		Evaluación de vulnerabilidades y aceptabilidad del riesgo (aceptable, tolerable, inaceptable) y definición del nivel de planeación (sin plan, plan general, plan detallado).	Informe	1	S/ 23,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores			1
		Monitoreo continuo de servidores y servicios críticos; registro en bitácoras y retroalimentación del plan (mejora continua).	Informe	3	S/ 7,000.00	Administrador de servidores	1	1	1
		Control preventivo de seguridad: antivirus actualizado, políticas de uso de dispositivos/USB, verificación de infraestructura eléctrica (UPS/pozo a tierra)	Informe	1	S/ 13,500.00	Administrador de servidores y administrador de redes			1
2	Definir actividades de prevención, preparación, respuesta y recuperación orientadas a proteger la infraestructura tecnológica y la información institucional frente a incidentes derivados de fallas eléctricas, fenómenos naturales, amenazas cibernéticas, ingeniería social, vandalismo u otras contingencias	Mantenimiento preventivo anual de computadoras, laptops, impresoras, servidores y comunicaciones (switch, AP, cableado).	Jornada de Mantenimiento	1	S/ 30,000.00	Proveedor de servicios	1		
		Gestión de respaldos: ejecución de backups completo, incremental y diferencial; resguardo de BD (SGD, SIGAI, SIAF, SIGA), aplicativos, correo y archivos; política/procedimiento de copias (Anexo).	Informe	3	S/ 7,000.00	Administrador de Servidores	1	1	1
		Reconocimiento del entorno (servidores críticos, dependencias), gestión de licencias/activos de software y preparación de equipos mínimos de respuesta (stock/repuestos).	Informe	1	S/ 7,000.00	Administrador de Servidores			1
		Activación del Plan de Emergencia: ubicar y dimensionar el incidente, ejecutar acciones de contención, notificar a responsables STIC, modificar operaciones si aplica y documentar.	Informe	1	S/ 23,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores			1
		Procedimientos específicos por tipo de evento: caída de red/puesto, fallas de portal/correo/Internet, problemas de switch/AP, con canales de escalamiento (Correo/mesa de ayuda)	Informe	1	S/ 23,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores			1
		Acciones correctivas por equipo (red, impresoras, comunicaciones, servidores, PCs) con tiempos estimados y responsables; puesta en producción y verificación funcional.	Informe	3	S/ 23,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores	1	1	1
3	Establecer estrategias que aseguren la continuidad de los servicios informáticos y permitan su restablecimiento en el menor tiempo posible tras la interrupción.	Priorización de servicios críticos y RTO por sistema (SGD, SIAF, SIGA, SIGAI, AD, correo, file server, Internet)	Informe	1	S/ 18,500.00	Administrador de servidores, administrador de redes y desarrollador web			1
		Centro de datos alterno / virtualización para servidores de contingencia y posibilidad de puesta en marcha del centro alterno; stock de repuestos críticos (memoria, discos, controladoras)	Informe	1	S/ 7,000.00	Administrador de servidores			1
		Doble enlace / contingencia de Internet y procedimiento para diagnóstico y conmutación (ISP / switch core).	Informe	1	S/ 6,500.00	Administrador de redes			1
		Automatización de apagado seguro por UPS y secuencia de encendido/validación post-restablecimiento.	Informe	1	S/ 7,000.00	Administrador de servidores y administrador de redes		1	
		Acceso remoto regulado (habilitación bajo solicitud, supervisión de uso, cumplimiento de seguridad) para continuidad operativa	Correo	3	S/ 10,000.00	Equipo de soporte técnico	1	1	1
		Bitácoras, evidencias, correos y tickets para trazabilidad y auditoría de cada restablecimiento.	Informe	3	S/ 23,500.00	Equipo de soporte técnico	1	1	1
4	Determinar los procedimientos, tareas, roles y responsabilidades necesarias para la recuperación de los servicios críticos de tecnología de la información, garantizando su	Roles definidos por escenario: equipo de soporte técnico, administrador de redes, administrador de servidores, desarrollador/BD; tablas de responsables por incidencia.	Informe	1	S/ 28,500.00	Equipo de soporte técnico, administrador de redes y administrador de servidores			1
		Matrices de equipos mínimos de respuesta y tiempos estimados de corrección por componente	Informe	3	S/ 13,500.00	Equipo de soporte técnico	1	1	1
		Validación funcional con usuarios	Correo	3	S/ 10,000.00	Equipo de soporte técnico	1	1	1

## XII. RESPONSABILIDAD

La STIC es la unidad de organización encargada de:

- Desarrollar, implementar y gestionar los sistemas de información, la infraestructura tecnológica y las telecomunicaciones que brindan soporte a las unidades de organización del PRONACEJ según el siguiente cuadro:

Responsabilidades	Responsable (s)
Soporte Técnico de equipos de cómputo	Equipo de Soporte Técnico
Monitoreo de servidores y sistemas de información	Administrador de Servidores
Administración de Base de Datos y Aplicativos	Desarrollador web
Mantenimiento correctivo de equipos informáticos (equipos de cómputo e impresoras)	Equipo de Soporte Técnico
Administración de respaldos de Información	Administrador de Servidores
Soporte técnico de equipos de comunicaciones (Switches)	Administrador de redes


- Proponer, formular, organizar, dirigir e implementar las políticas y planes de aplicación y de uso de tecnologías de la información y de telecomunicaciones, de manera que estos provean soporte a las operaciones de la entidad.

## XIII. ANEXOS

- 13.1 Anexo N.º 1: Formato de bitácora de respaldo de datos de los sistemas informáticos
- 13.2 Anexo N.º 2: Procedimiento de las copias de respaldo de la información

**ANEXO N.º 1**

**FORMATO DE BITÁCORA DE RESPALDO DE DATOS DE LOS SISTEMAS INFORMÁTICOS**

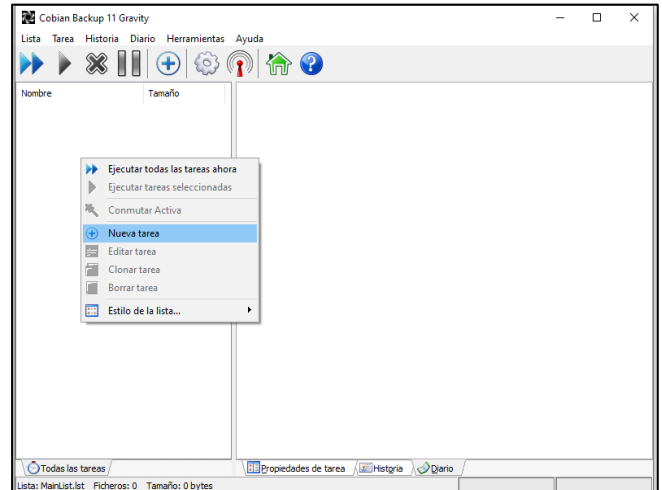
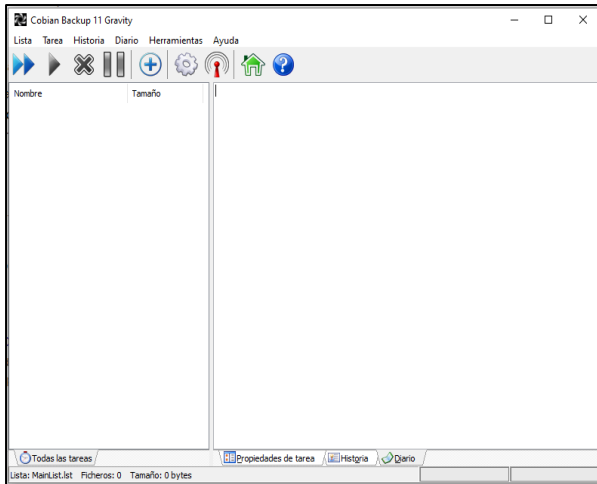
 <b>PRONACEJ</b> <small>Programa Nacional de Centros Juveniles</small>		<b>BITACORA DE RESPALDO DE DATOS DE LOS SISTEMAS INFORMÁTICOS</b>								FORM - 02		
Ubicación	SEDE CENTRAL - PRONACEJ											
Realizado Por	Johan Dario Rojas Banda			Area	Subunidad de Tecnologías de la Información y las Comunicaciones							
Cargo	Administrador de Servidores			Nombre / Ubicación	Servidor Local (snr-backup)			Software de Copias	Cobian Backup 11 Gravity (OpenSource)			
FECHA DE GENERACION DE BACKUP	BD A RESPALDAR					TAMAÑO DE BACKUP(GB)	FRECUENCIA DE BACKUP	TIEMPO DE RESPALDO (Minutos)			GUARDADO EN (Servidor, PC, Disco, D. Externo)	OBSERVACIONES
	SIAF	SGD	STD	SIGA	Otro _____			H. INICIO	H. FIN	TOTAL (min)		
01/01/2025												
02/01/2025												
03/01/2025												
04/01/2025												
05/01/2025												
06/01/2025												
07/01/2025												
08/01/2025												
09/01/2025												
10/01/2025												
11/01/2025												
12/01/2025												
13/01/2025												
14/01/2025												
15/01/2025												
16/01/2025												
17/01/2025												
18/01/2025												
19/01/2025												
20/01/2025												
21/01/2025												

## ANEXO N.º 2 PROCEDIMIENTO DE LAS COPIAS DE RESPALDO DE LA INFORMACIÓN

El presente procedimiento muestra una guía de los pasos a seguir, para poder hacer uso del servicio de backup que ofrece el Software Cobian Backup 11 Gravity, el cual es una herramienta para la gestión de backup que permite realizar recuperaciones de ficheros en función del backup generado según la programación de las copias.

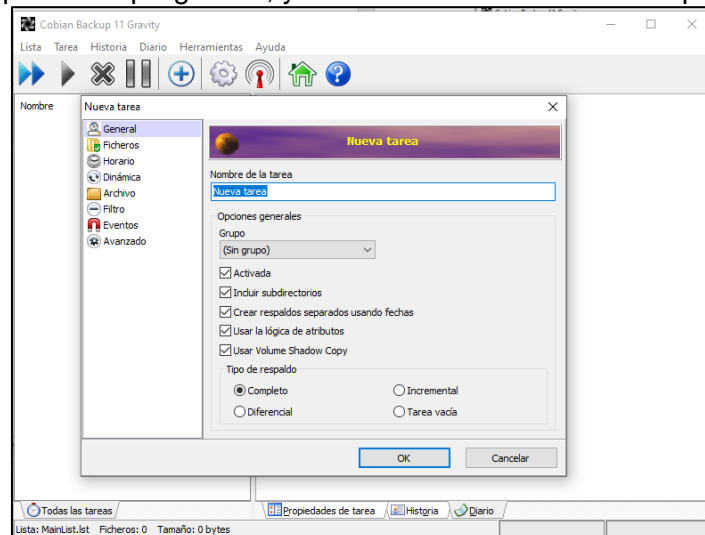
### **PASO 01**

Creamos una nueva tarea para la realización de una copia de respaldo.

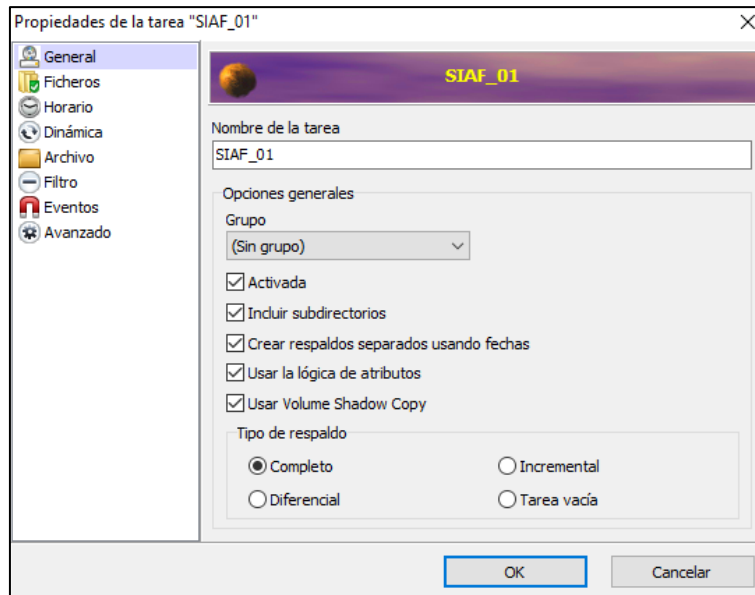


### **PASO 2**

En la pestaña General ponemos el nombre que le vamos a dar a la tarea de copia de seguridad que queremos programar, y marcamos las casillas correspondientes.



Se selecciona el tipo de respaldo "Completo" porque es la primera copia de seguridad que se va a realizar. Una vez que se haya hecho esta primera copia de seguridad, se cambiará la opción para que la siguiente copia que se haga de los mismos archivos sea "Incremental".

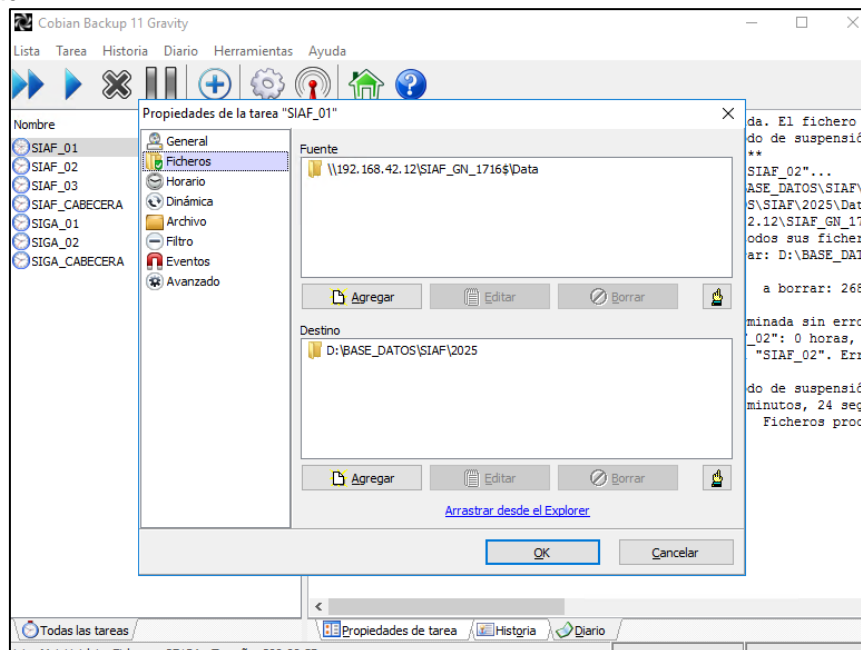


Para hacer todas estas tareas es importante tener conectado como unidad de red los discos donde contengan las carpetas que se requieren hacer copias, y así poder configurarlos dentro del aplicativo de Backup. En nuestro caso, estamos tomando de referencia la unidad "M" que viene desde la IP 192.168.42.12, en donde están alojados los archivos a copiar.

### **PASO 03**

En ficheros, elegimos:

- Los ficheros y carpetas de los que queremos hacer copia de seguridad.
- El destino donde lo guardaremos. En este caso, se ha elegido guardar las copias de seguridad en una unidad de red que tiene nuestro servidor. Es importante que el destino sea un disco diferente del que estamos haciendo las copias. De este modo, si tenemos algún problema en el disco del servidor no perderemos nuestras copias de seguridad.



## PASO 04

Elegimos la hora que queremos que se ejecute o inicie la copia, y si queremos que sea de un periodo semanal, diaria y en qué días debe hacerse. Todo depende de nuestros requerimientos.

Como el servidor está todo el día encendido será mejor programar las copias de seguridad para que se realicen cuando el horario de trabajo se haya terminado.

En este caso se ha colocado el horario de 00:00 horas, por ser un horario en donde hay muy pocos usuarios que utilizan los diversos sistemas informáticos de la institución, teniendo en cuenta que el tamaño es grande (específicamente para este sistema).

