



# Resolución Directoral

Lima, 10 de diciembre de 2025

## VISTO:

El expediente N° 25-3602-1, conteniendo el Memorando N° 1786-2025-OEPE/INMP de fecha 19 de noviembre de 2025, de la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico; Informe N° 107-2025-CMAV-UFO-OEPE-INMP de fecha 18 de noviembre de 2025, del Especialista en Modernización de la Oficina Ejecutiva de Planeamiento Estratégico; Memorando N° 0899-2025-OEI/INMP de fecha 13 de noviembre de 2025, del Jefe de la Oficina de Estadística e Informática; Informe N° 125-2025-EFI-OEI/INMP de fecha 12 de noviembre de 2025, del Equipo Funcional de Informática.

## CONSIDERANDO:

Que, el numeral XIV del Título Preliminar de la Ley N° 26842, Ley General de Salud, establece que la información en salud es de interés público y que toda persona está obligada a presentar a la Autoridad de Salud la información que le sea exigible de acuerdo a ley. La información que el Estado tiene en su poder es de dominio público, con las excepciones que establece la ley;

Que, el numeral 1.1 del artículo 1 de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, el artículo 2 de la Ley N° 29733, Ley de Protección de Datos Personales, define los datos personales como toda información sobre una persona natural que la identifica o hace identificable a través de medios que puedan ser utilizados razonablemente, y datos sensibles, aquellos datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información referida a la salud o a la vida sexual;

Que, el artículo 16 de la Ley N° 29733, Ley de Protección de Datos Personales, establece que, para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado;

Que, con Resolución Ministerial N° 246-2007-PCM, se 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;

Que, con Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de Seguridad.



Sistemas de Seguridad de la Información. Requisitos. 2° Edición”, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el numeral 72.1 del artículo 72 del TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General establece que, la competencia de las entidades tiene su fuente en la Constitución y en la ley, y es reglamentada por las normas administrativas que de aquéllas se derivan; y el numeral 72.1 establece que, toda entidad es competente para realizar las tareas materiales internas necesarias para el eficiente cumplimiento de su misión y objetivos, así como para la distribución de las atribuciones que se encuentren comprendidas dentro de su competencia;

Que, mediante Resolución Directoral N° 202-2021-DG/MINSA de fecha 24 de setiembre de 2021, se aprueba la Directiva N° 004-2021-DG-INMP/MINSA, “Directiva para la Elaboración de Documentos Normativos en el Instituto Nacional Materno Perinatal”, cuyo objeto es establecer los principios, normas y procedimientos que se aplican al proceso de modernización y ecoeficiencia en la gestión pública, en concordancia con la Resolución Ministerial N° 826-2021-MINSA, que aprueba “Normas para la Elaboración de documentos normativos del Ministerio de Salud”;

Que, con el documento de Visto, el Jefe de la Oficina de Estadística e Informática adjunta el documento denominado proyecto “Directiva para que la Información Digital Crítica del INMP posean Copia de Respaldo Obligatorio” y la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico emite informe recomendando su aprobación;

Que, en consecuencia, por convenir a los intereses funcionales institucionales que permitan un mejor cumplimiento de los fines y objetivos del Instituto Nacional Materno Perinatal, resulta necesario formalizar la aprobación de la “Directiva para que la Información Digital Crítica del INMP posean Copia de Respaldo Obligatorio”, mediante la emisión del acto resolutivo correspondiente;

Que, con la visación del Director Ejecutivo de la Oficina Ejecutiva de Administración, de la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico, del Jefe de la Oficina de Estadística e Informática y de la Jefa de la Oficina de Asesoría Jurídica del Instituto Nacional Materno Perinatal; en armonía con las facultades conferidas en la Resolución Ministerial N° 504-2010/MINSA y la Resolución Ministerial N° 006-2022/MINSA;

**SE RESUELVE:**

**ARTÍCULO PRIMERO:** APROBAR la DIRECTIVA N° 010 -2025-DG-INMP "DIRECTIVA PARA QUE LA INFORMACIÓN DIGITAL CRÍTICA DEL INSTITUTO NACIONAL MATERNO PERINATAL POSEAN COPIA DE RESPALDO OBLIGATORIO", la misma que forma parte integrante de la presente resolución y por las razones expuestas en la parte considerativa.

**ARTÍCULO SEGUNDO:** DISPONER que la Oficina de Estadística e Informática sea responsable de su implementación.

**ARTÍCULO TERCERO:** El responsable de elaborar y actualizar el Portal de Transparencia, publicará la presente Resolución en el Portal Institucional.

Regístrese y Comuníquese,

MINISTERIO DE SALUD  
INSTITUTO NACIONAL MATERNO PERINATAL

Mg. FÉLIX DASIO AYALA PERALTA  
C.M.P. N° 19726 - R.N.E. N° 9170  
DIRECTOR DE INSTITUTO

FDAP/JLCHR/ea

cc.

- DEEMSC
- DEOG
- DEN
- Oficina Ejecutiva de Administración

- Oficina Ejecutiva de Planeamiento
- OEI (Portal Transparencia)
- Oficina de Asesoría Jurídica
- Archivo.
- Oficina de Logística
- Oficina de Economía



M. UGARTE



A. CHARCON



J. CHAPA



J. TORRES




**MATERNAL PERINATAL**  
MATERNIDAD DE LIMA

**Instituto Nacional Materno Perinatal  
(INMP)**

**“DIRECTIVA PARA ESTABLECER LA OBLIGATORIEDAD DE COPIAS DE  
RESPALDO DE LA INFORMACIÓN DIGITAL CRÍTICA DEL INMP”**

Resolución de Dirección General N° 363-2025-DG-INMP, de fecha 10/12/2025

UNIDAD ORGANICA	RESPONSABLE	
Propuesto por	M.C.O. Juan Macedonio Torres Osorio	
Cargo	Jefe de Oficina de Estadística e Informática	
Fecha	__/__/2025	
Revisado por	Eco. Roxana Jacqueline Alarcón Guizado	
Cargo	Jefa de Oficina Ejecutiva de Planeamiento y Presupuesto	
Fecha	__/__/2025	
Aprobado por:	Dr. Félix Dasio Ayala Peralta	
Cargo	Director General del Instituto Nacional Materno Perinatal	
Fecha	__/__/2025	

	<b>Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP</b>	<b>Oficina de Estadística e Informática</b>
		<b>Página 2 de 11</b>

<b>Versión</b>	<b>Fecha</b>	<b>Justificación</b>	<b>Responsable</b>
1.0	__/__/2025	Elaboración inicial del documento	Oficina de Estadística e Informática

**HOJA DE CONTROL DE CAMBIOS  
(Versionamiento)**





## Índice

I. FINALIDAD .....	4
II. OBJETIVO .....	4
III. ÁMBITO DE APLICACIÓN .....	4
IV. BASE LEGAL .....	4
V. DEFINICIONES Y ABREVIATURAS .....	5
VI. DISPOSICIONES ESPECIFICAS .....	6
VII. RESPONSABILIDADES .....	10
VIII. DISPOSICIONES FINALES .....	10
IX. BIBLIOGRAFIA .....	10



## I. FINALIDAD

Establecer medidas para proteger y asegurar la disponibilidad e integridad de los datos y sistemas informáticos críticos del INMP mediante copias de respaldo periódicas y seguras. Con ello se busca garantizar la continuidad operativa, reducir el riesgo de pérdida de información, facilitar la recuperación ante incidentes, cumplir con normas de seguridad y fortalecer la gestión de riesgos tecnológicos.

## II. OBJETIVO

Establecer un proceso estandarizado y obligatorio para la realización y gestión de copias de respaldo periódicas de los equipos de cómputo críticos, a fin de garantizar la disponibilidad e integridad de la información institucional y asegurar su recuperación oportuna ante incidentes o contingencia.

### 2.1 Objetivos específicos


- 2.1.1 Asegurar la protección y disponibilidad de los datos esenciales para el funcionamiento institucional, garantizando su recuperación en caso de fallos o pérdidas imprevistas.
- 2.1.2 Minimizar el impacto de incidentes o desastres que puedan afectar a los equipos críticos, permitiendo una restauración rápida y efectiva de los sistemas y datos afectados.
- 2.1.3 Cumplir con las normativas de seguridad informática y las mejores prácticas de gestión de riesgos, contribuyendo a la prevención de pérdidas de información y al cumplimiento de los estándares de calidad tales como ISO 9001 (Sistemas de Gestión de Calidad), ISO 14001 (gestión ambiental), ISO 45001 (seguridad y salud en el trabajo) y ISO 27001 (seguridad de la información).
- 2.1.4 Facilitar la continuidad operativa de la institución, reduciendo al mínimo el tiempo de inactividad y asegurando que los servicios y procesos esenciales puedan reanudarse sin interrupciones significativas.

## III. ÁMBITO DE APLICACIÓN

- La directiva se aplica a todo el manejo de información digital y a los equipos críticos del INMP, siendo de cumplimiento obligatorio para todas sus oficinas, colaboradores, proveedores y terceros involucrados en la gestión de sistemas informáticos.

## IV. BASE LEGAL



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 5 de 11


- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Ley N° 30096 - Delitos Informáticos y la Modificación de la Ley N° 30071
- Ley N° 29733, Ley de protección de datos personales.
- Resolución Ministerial N° 004-2016-PCM "Aprueban 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.
- Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno.
- Ley N° 32069, Ley General de Contrataciones Públicas y su reglamento aprobado mediante Decreto Supremo N° 009-2025--EF.

## V. DEFINICIONES Y ABREVIATURAS

### 5.1 Definiciones y abreviaturas

- **Backup de Información** (copia de seguridad): Es el proceso de realizar una copia de los datos importantes y almacenarlos en un lugar seguro, con el fin de protegerlos contra pérdidas, daños o corrupciones.
- **Colaborador del INMP**: Para efectos de la presente política se entenderá como colaborador, a la persona que en el INMP cuentan con vínculo laboral bajo el régimen laboral que establece el D.L. 728 (Decreto Supremo 003-97-TR), D.L. 1057 – CAS (Decreto (Supremo N° 075-2008-PCM), o que presta servicios por intermediación laboral, o que realiza practicas preprofesionales o profesionales.
- **INMP**: Instituto Nacional Materno Perinatal.
- **Jefe de EFI**: Persona designada como jefe funcional de informática.
- **Proveedor**: Persona natural o jurídica que brinda un servicio o producto al INMP. En el marco de la norma de contrataciones recibe la denominación de contratista.
- **Ransomware**: Software malicioso que los ciberdelincuentes utilizan para bloquear el acceso a los datos o sistemas de una víctima.
- **Tercero**: Toda persona que no cuentan con vínculo laboral con el INMP, pero requiere hacer uso de sus activos de información ya sea para la prestación de un servicio (proveedores), en calidad de visitante o



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 6 de 11

administrado (empresa operadora o usuario de servicio de telecomunicaciones).

- **Vulnerabilidad de información:** La vulnerabilidad de la información se refiere a los puntos débiles dentro de los sistemas de gestión de información que pueden ser explotados para acceder, alterar o destruir datos. Esto puede ocurrir por varias razones, como errores humanos, fallos en el software, configuraciones incorrectas, o falta de protección adecuada. Las vulnerabilidades de la información pueden ser muy perjudiciales para las organizaciones, ya que comprometen la confidencialidad, integridad y disponibilidad de los datos.

## VI. DISPOSICIONES ESPECIFICAS

### 6.1 Definición de equipos críticos:

Se considerarán equipos críticos aquellos cuya interrupción afecte de manera significativa las operaciones del INMP, la disponibilidad de servicios clave o la integridad de los datos.

### 6.2 Requisitos de copia de respaldo:


Todos los equipos críticos deberán contar con una copia de respaldo completa y periódica que incluya:

- **Datos clave:** Archivos, bases de datos y configuraciones esenciales para la operación del equipo.
- **Configuraciones del sistema operativo y software:** Para garantizar la restauración rápida en caso de falla.
- **Frecuencia de respaldo:** La copia de respaldo debe realizarse al menos una vez al día. En el caso de sistemas que operen con datos de alta rotación, como bases de datos, se recomienda realizar respaldos incrementales cada hora o de acuerdo a las necesidades del negocio.
- **Almacenamiento seguro:** Las copias de seguridad deberán almacenarse en ubicaciones seguras y separadas físicamente del equipo original, ya sea en almacenamiento en la nube, unidades externas, o sistemas de respaldo en servidores dedicados.

### 6.3 Tipos de respaldo:

- **Copia completa:** Se realizará al menos una vez por semana.



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 7 de 11

- **Copia incremental o diferencial:** Se realizará según la frecuencia indicada para cada tipo de sistema, permitiendo minimizar el espacio de almacenamiento utilizado sin comprometer la recuperación de datos.

#### 6.4 Proceso de copia en el servidor de archivos del INMP

##### 6.4.1 Copia en servidor de datos (INMP-263):

El INMP posee un servidor de datos destinado para almacenar información crítica y/o importante, dicho equipo se encuentra alojado en el Centro de Datos del INMP.

Se precisa que;

- La disponibilidad y confidencialidad de la información estará a cargo del personal de EFI.
- La integridad de dicha información estará a cargo del personal asignado por el área usuaria.

Procedimiento para almacenar datos en el servidor es:

- El Jefe de la oficina solicitante envía un correo electrónico al Jefe de EFI comunicando que requiere que se almacene información en el servidor de archivos.


El correo electrónico debe poseer como mínimo la siguiente información:

- ✓ Nombre de la carpeta donde se guardará la información.
- ✓ De ser necesario indicar el nombre de las sub carpetas.
- ✓ Nombre completo del personal responsable que manipulara la información (a nivel de lectura y/o escritura).
- El personal asignado por la oficina solicitante es responsable del copiado, actualización y supervisión de la información almacenada.
- La información almacenada en el servidor de datos no debe ser eliminada de los equipos computo locales u otros.

##### 6.4.2 Contrato de backup con empresa tercera

La Oficina de Estadística e Informática, posee un servicio de Backup de Información, por la cual una empresa tercera copia en medios externos la



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 8 de 11

información crítica y/o importante contenida en los servidores de datos alojados en el Centro de Datos.

Ante un evento que requiera obtener información de los servidores de datos, el personal de redes de EFI lo solicita a la empresa contratista.

#### 6.4.3 Copiado en medios externos

El copiado de archivos críticos institucionales no se recomienda en medios externos (USB, disco duro), por los siguientes motivos:

No se tiene seguridad de la información, los medios de almacenamiento externos pueden sufrir los siguientes casos de fallos:

- Daño físico y/o lógico, se daña o pierde la información.
- Extraviar, personas no autorizadas podrían tener acceso a la información crítica institucional.
- Poseer virus informático, la información puede ser dañada y/o eliminada, además los equipos de cómputo donde se coloquen los medios externos también pueden ser contagiados con virus informático.


#### 6.5 Verificación y pruebas de restauración:

- Las copias de respaldo deberán ser verificadas periódicamente para garantizar que los datos sean consistentes y completos.
- Se deben realizar pruebas de restauración de las copias de respaldo de forma trimestral, con el objetivo de verificar la efectividad de los respaldos y reducir el tiempo de inactividad en caso de un evento adverso.
- El personal asignado de cada oficina debe confirmar la integridad de la información almacenada de manera periódica, mínimo con una frecuencia de una semana.

#### 6.6 Accesibilidad y seguridad de las copias de respaldo:

- Las copias de respaldo deben ser accesibles solo para personal autorizado mediante un sistema adecuado de control de accesos.
- La integridad de las copias debe ser protegida mediante mecanismos de cifrado para evitar la alteración no autorizada de los datos respaldados. La responsabilidad de la integridad de la información es del área usuaria.



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 9 de 11

### 6.7 Documentación y registros:

El personal de EFI deberá mantener un registro detallado de las siguientes actividades:

- Resultado de las pruebas de restauración y verificación.
- Detalles de cualquier fallo o problema identificado durante el proceso de respaldo.

### 6.8 Cumplimiento y auditoría:

El cumplimiento de esta directiva será auditado de forma periódica (semestral). En caso de incumplimiento, se podrán tomar medidas correctivas que incluyen la mejora de los procesos, la implementación de nuevas soluciones tecnológicas o sanciones internas si fuera necesario.

### 6.9 Indicador de la directiva

Para medir la efectividad de la implementación de la directiva, se deben establecer indicadores claros que permitan monitorear el cumplimiento de los procesos de respaldo en los equipos de cómputo críticos. Algunos de los indicadores clave son:

#### 6.9.1 Porcentaje de copias de respaldo activas y actualizadas:

Fórmula:  $(\text{Número de equipos críticos con respaldo completo y actualizado} / \text{Número total de equipos críticos}) * 100$

Objetivo: Asegurar que el 100% de los equipos críticos cuenten con copias de respaldo regulares y actualizadas.

#### 6.9.2 Frecuencia de respaldo cumplida:


Fórmula:  $(\text{Número de respaldos realizados dentro del intervalo definido} / \text{Número total de respaldos programados}) * 100$

Objetivo: Verificar que los respaldos se realicen según la frecuencia definida (diaria, semanal, etc.), alcanzando al menos el 95% de cumplimiento.

### 6.10 Acciones ante desviaciones de las políticas

El incumplimiento de las disposiciones establecidas en la DIRECTIVA PARA ESTABLECER LA OBLIGATORIEDAD DE COPIAS DE RESPALDO DE LA INFORMACION DIGITAL CRITICA DEL INMP, tales como procedimientos,



	Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP	Oficina de Estadística e Informática
		Página 10 de 11

manuales o cualquier otro documento derivado de estas, tiene como resultado la aplicación de medidas correctivas y de mejora necesarias. En caso se encontrar responsabilidad en un colaborador y/o tercero, se da inicio al procedimiento administrativo disciplinario correspondiente y/o a las acciones legales que la ley faculte.

## VII. RESPONSABILIDADES

**7.1 Jefe de la Oficina de Estadística e Informática:** Realiza gestiones administrativas con la Alta Dirección con el objetivo que en el INMP se cumplan los lineamientos para preservar la información del INMP.

**7.2 Jefe del Equipo Funcional de Informática (EFI):** Es el responsable de autorizar la atención de requerimiento de backup de información institucional, teniendo en cuenta los alcances del presente documento, así como las limitaciones de los recursos institucionales.

Es responsable de implementar, gestionar y monitorear el estado del servidor de archivos (INMP-263).

**7.3 Personal de EFI (TI):** Responsables de realizar la configuración y acceso a las carpetas solicitadas por los usuarios solicitantes. Capacitar al personal usuario sobre el uso de los recursos asignados.

Realizar coordinaciones con la empresa contratista del backup de información, en el caso se requiera alguna información almacenada.

**7.4 Jefatura del área solicitante:** O a quien delegue debe velar por el buen uso e integridad de la información institucional asignada a su oficina y que encuentra almacenada en el servidor de archivos (INMP.263). Como mínimo debe realizar una supervisión semanal.

## VIII. DISPOSICIONES FINALES

Este documento es válido desde la fecha de su aprobación.

## IX. BIBLIOGRAFIA

- <https://cdn.www.gob.pe/uploads/document/file/5696231/5057789-directiva-n-002-2024-agn-recursos-informaticos-y-servicios-digitales.pdf?v=1705518193>  
[https://www.grupoacs.com/ficheros\\_editor/File/05\\_Compliance/Pol%C3%ADticas/31\\_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf](https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf).
- <https://cdn.www.gob.pe/uploads/document/file/7163226/6143817-directiva-n-009-2024-agn-recursos-informaticos.pdf?v=1730725291>





Directiva para establecer la obligatoriedad de copias de respaldo de la información digital crítica del INMP

Oficina de Estadística e Informática

Página 11 de 11

- [https://www.mef.gob.pe/contenidos/acerc\\_mins/doc\\_gestion/RM029\\_2015EF44.pdf](https://www.mef.gob.pe/contenidos/acerc_mins/doc_gestion/RM029_2015EF44.pdf)

