



RESOLUCIÓN DIRECTORAL

El Agustino, 28 de octubre de 2024

VISTO;

El Expediente N° 24-043692-001, que contiene la Nota Informativa N° 352-2024-OEI/HNHU a través de la cual la Oficina de Estadística e Informática solicita aprobación sobre Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue, y;

CONSIDERANDO:

Que, en principio, el TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, establece en su numeral 73.3 del artículo 73° que, *"Cada entidad es competente para realizar tareas materiales internas necesarias para el eficiente cumplimiento de su misión y objetivos"*;

Que, por su parte, el numeral 1.1 del artículo 1° de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado establece: *"Declárase 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, por otro lado, según la Ley N° 29733, Ley de Protección de Datos Personales, modificada por Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses tiene por objeto crear la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalecer el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses;

Que, también, con Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática señala en su numeral 5.2 y 5.3 de artículo 5° que la alta dirección debe establecer una política de seguridad de la información que:

- Es apropiada al propósito de la organización.*
- Incluye objetivos de seguridad de la información (...) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información.*
- Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e*
- Incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información (...)"*

Asimismo, sobre los roles, autoridad y responsabilidades organizacionales; la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

La alta dirección debe asignar la responsabilidad y la autoridad para:

- a) Asegurar que el sistema de gestión de seguridad de la información este conforme a los requisitos de este Proyecto de Norma Técnica Peruana y;
- b) Reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

Que, vale decir también que, según el numeral 7.3 del artículo 7° sobre concientización señala que las personas que trabajan bajo el control de la organización deben ser conscientes de:

- a) La política de seguridad de información.
- b) Su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y
- c) Las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.

Que, a razón de ello, mediante Nota Informativa N° 352-2024-OEI/HNHU de fecha 24 de setiembre de 2024, la Oficina de Estadística e Informática remite la Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue que actualiza la Directiva Administrativa N° 023-HNHU/2017/OEI, "Generación y Restauración de Copias de Respaldo de Información (Backup) del Hospital Nacional Hipólito Unánue", a fin de ser aprobado, adjuntando a la misma, su respectivo Informe Técnico Sustentatorio que pretende establecer los procedimientos adecuados de respaldo y restauración de la información crítica del hospital; a su vez, busca garantizar la disponibilidad, confidencialidad e integridad de los datos. Además, la presente directiva se ajusta con los estándares internacionales como NTP ISO/IEC 27001:2014, lo que asegura la protección de datos hospitalarios frente a riesgos operativos y de seguridad;

Que, es así que, mediante Nota Informativa N° 039-2024-UO-OPE/HNHU de fecha 26 de setiembre de 2024, la Unidad de Organización de la Oficina de Planeamiento Estratégico remite a la Dirección Ejecutiva de la Oficina de Planeamiento Estratégico la **Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue**; y a su vez, en cumplimiento de lo dispuesto en la Resolución Directoral N° 075-2022-HNHU-DG de fecha 29 de marzo de 2022, se aprobó la Directiva Administrativa N° 045-HNHU/2022/OPE, Directiva Administrativa para la elaboración de documentos normativos en el Hospital Nacional Hipólito Unánue, en el cual pone a conocimiento su opinión favorable respecto del Documento Normativo, a fin de ser aprobado para su difusión, implementación y evaluación;

Que, Por otra parte, a través de la Nota Informativa N° 071-2024-OPE-HNHU de fecha 27 de setiembre de 2024, la Dirección Ejecutiva de la Oficina de Planeamiento Estratégico remite a la Oficina de Asesoría Jurídica la **Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue**, a fin de emitir opinión legal correspondiente;

Que, estando a lo informado por la Oficina de Asesoría Jurídica, con el Informe N° 477-2024-OAJ-HNHU;

Con el visado de la Oficina de Estadística e Informática, Jefe de la Oficina de Asesoría Jurídica y de la Dirección Ejecutiva de la Oficina de Planeamiento Estratégico; y,

De acuerdo a las facultades establecidas en el Reglamento de Organización y Funciones del Hospital Nacional Hipólito Unánue, aprobado mediante Resolución Ministerial N° 099-2012/MINSA;



RESOLUCIÓN DIRECTORAL

El Agustino, 28 de octubre de 2024

SE RESUELVE:

ARTÍCULO 1.- APROBAR la Directiva Administrativa N° 08 -HNHU/OEI-UI-2024 – “Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue”, la misma que forma parte íntegramente de la presente resolución, y por las razones expuestas en la parte considerativa.

ARTICULO 2.- DISPONER que la Oficina de Estadística e Informática, realice las acciones administrativas que resulten pertinentes, a fin de implementar la Directiva Administrativa N° 08 -HNHU/OEI-UI-2024 – “Directiva Administrativa que Regula el Respaldo y Restauración de la Información en el Hospital Nacional Hipólito Unánue”.

ARTÍCULO 3.- DAR TÉRMINO a la Resolución Directoral N° 278-2017-HNHU-DG de fecha 29 de diciembre de 2017 que aprobó la Directiva Administrativa N° 023-HNHU/2017/OEI, “Generación y Restauración de Copias de Respaldo de Información (Backup) del Hospital Nacional Hipólito Unánue”

ARTÍCULO 4.- DISPONER que la Oficina de Comunicaciones proceda con la publicación de la presente Resolución en la Página Web del Hospital <https://www.gob.pe/hnhu>.

Regístrese y comuníquese.

MINISTERIO DE SALUD
Hospital Nacional “Hipólito Unánue”

DR. MOISÉS ENRIQUE TAMBINI ACOSTA
Director General (e)
CMP: 16412

META/VMIF/vcrc

DISTRIBUCIÓN

- () Oficina de Estadística e Informática
- () OAJ
- (...) Dirección Ejecutiva de la Oficina de Planeamiento Estratégico
- () O. Comunicaciones
- (...) OCI
- () ARCHIVO

DIRECTIVA ADMINISTRATIVA QUE REGULA EL RESPALDO Y RESTAURACION DE LA INFORMACION EN EL HOSPITAL NACIONAL HIPOLITO UNANUE

I. FINALIDAD

Garantizar la continuidad de los servicios informáticos y de comunicaciones en el Hospital Nacional Hipólito Unanue (HNHU) ante eventos que puedan afectar el normal funcionamiento de los sistemas de información y comunicaciones.

II. OBJETIVO

Establecer las normas y procedimientos para realizar el respaldo y la restauración de la información que permita asegurar la disponibilidad, integridad y confidencialidad de los datos críticos del Hospital Nacional Hipólito Unanue.

III. BASE LEGAL

- ✓ Ley N° 27658 Ley Marco de Modernización de la Gestión de Estado, y sus modificatorias
- Ley N° 27806 - Ley de Transparencia y Acceso a la Información Pública:
- Directiva de Seguridad de la Información para Entidades del Estado: Emitida por la Autoridad Nacional de Protección de Datos Personales (APDP), establece lineamientos específicos para la implementación de medidas de seguridad de la información en las entidades del Estado, que incluyen la realización de backups como parte de la estrategia de protección de datos.
- Decreto Supremo N° 030-2020-PCM Reglamento de la Ley N° 27658 Ley Marco de Modernización de la Gestión del Estado.
- Resolución Ministerial N° 1143-2019/MINSA que aprueba la Directiva Administrativa N° 280- MINSA/2019/OGPPN Directiva Administrativa "Para la Formulación, Seguimiento y Evaluación de los Planes Específicos de los Órganos, Unidades Orgánicas de la Administración Central, los Órganos Desconcentrados, Programas y Organismos Públicos Adscritos del MINSA.
- Ley N° 29733, Ley de Protección de Datos Personales, modificada por Decreto Legislativo N° 1353.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2° Edición", en todas las entidades integrantes del Sistema Nacional de Informática modificada por Resolución Ministerial N° 166-2017-PCM y Resolución Ministerial N° 087-2019-PCM.



- Resolución Ministerial N° 028-2015-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.

IV. DISPOSICIONES GENERALES

5.1. Definiciones

- **Archivos:** Conjunto de datos o información almacenada en un formato digital y gestionada como una unidad.
- **Base de Datos:** Conjunto estructurado de datos organizados que se almacenan y gestionan electrónicamente.
- **Copia de Respaldo:** Réplica de los datos originales almacenada en un medio de almacenamiento secundario para protección contra pérdidas.
- **Incidente de Seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información o sistemas.
- **Operador de Backup:** Persona responsable de ejecutar y gestionar las operaciones de copia de respaldo de datos.
- **Responsable de Servicios de Backup:** Individuo o equipo encargado de supervisar y garantizar la efectividad de los servicios de copia de respaldo.
- **Respaldo:** Acción de realizar copias de los datos y sistemas críticos para asegurar su disponibilidad en caso de pérdida o daño.
- **Restauración:** Proceso de recuperación de datos desde las copias de respaldo hacia los sistemas originales.
- **Servidores:** Computadoras o sistemas dedicados a proporcionar servicios, almacenar datos y gestionar recursos en una red.
- **Software de Backup:** Aplicación o herramienta utilizada para automatizar y gestionar procesos de copia de respaldo de datos.
- **Tipo de Backup:** Método específico utilizado para realizar copias de seguridad de datos y sistemas.
- **NAS:** Sistema de almacenamiento conectado a red.
- **Usuario:** Persona autorizada que accede y utiliza sistemas informáticos y recursos tecnológicos.

SIGLAS

- HHU: Hospital Nacional Hipólito Unanue
- OEI: Oficina de Estadística e Informática

V. RESPONSABILIDADES

6.1. Del Jefe (área usuaria)

- Solicitar la restauración de información.

6.2. Del Jefe de la Oficina de Estadística e Informática (OEI)

- Autorizar las solicitudes de restauración de información.



6.3. Del Operador de Backup

- Preparar el espacio y la estructura de carpetas para el almacenamiento.
- Ejecutar la copia de seguridad
- Informar al jefe de informática de los nuevos backups ingresados a la NAS.
- Realizar la restauración de la información autorizada por el Jefe de OEI.
- Verificar si la información restaurada es la información solicitada.
- Ejecutar la prueba de restauración de la información.
- Elaborar Informe Técnico de las pruebas de restauración de copias.

6.4. De los usuarios

- Almacenar la información digital importante para la institución en las unidades de red que le sean asignadas. El resguardo de la información digital que no sea almacenada en dichas unidades de red; será de total responsabilidad del usuario.

VI. DISPOSICIONES ESPECIFICAS

- El HNHU a través de la Oficina de Estadística e Informática, es responsable de los datos que están almacenados en los servidores.
- El Jefe de la Unidad de Informática: Asigna al personal responsable de realizar las Copias de Seguridad (operador de backup).
- El jefe de la Unidad de Informática debe brindar el listado de activos de información a respaldar.
- El Responsable del Servicio de Backup, debe realizar el análisis para determinar la planificación de copias de respaldo (Anexo N°2).
- Toda generación y restauración de copia de seguridad debe estar documentada en algún medio físico o a través de herramientas de software aplicadas a la generación y restauración de copias de respaldo.
- Las copias de respaldo deben tener una frecuencia según el tipo de información y su criticidad.



7.1. Del Proceso de Respaldo de la Información

- a) Toda información a respaldarse debe estar relacionada a las funciones de HNHU basados en su nivel de importancia y criticidad.

Esta información será calificada como:

- **Critica:** información vital para la continuidad del funcionamiento de los procesos misionales institucionales y que debe ser recuperada con máxima prioridad.
- **Necesaria:** Información importante que puede ser recuperada dentro de un periodo de tiempo razonable.
- **Corriente:** Información que no afecta las operaciones normales del HNHU.



- b) Todo Sistema o aplicativo informático que pase a producción deberá contener especificaciones técnicas de respaldo de información (ubicación lógica, periodicidad y criticidad), a fin que la UI elabore el proceso y programe las tareas para realizar el respaldo de la información correspondiente.
- c) El proceso de respaldo de información, se realiza sobre la información contenida en los servidores y medios de almacenamiento administrados por la oficina de Estadística e Informática, dentro de dicha información se encuentran:
 - Bases de Datos de los sistemas informáticos, que se encuentran en los servidores.
 - Los aplicativos y sistemas informáticos, que se encuentran en los servidores del HNHU.
 - Correos electrónicos
 - Servidores Virtuales
- d) La información respaldada es sometida a un proceso de compresión, con el fin de optimar recursos de almacenamiento.
- e) El periodo de retención del respaldo de la información debe estar en función de lo indicado en el "Directorio de Información a Respalidar" (Anexo N°1)
- f) En caso en el proceso de verificación se detecta que es conforme el respaldo de información, el operador de backup, procede a registrar el incidente y envía un mensaje de alerta al correo electrónico del responsable de la unidad de informática.
- g) Todo proceso de respaldo de información debe estar registrado para el monitoreo y control, Registro de Respaldo de Información (Anexo N°3)

7.2. De la Programación:

- a) El operador de Backup, debe configurar en el software y/o herramienta, el respaldo de la información indicada en el "Directorio de Información a Respalidar" (Anexo N°1), a fin de garantizar la disponibilidad en el momento que se requiera.
- b) El respaldo de información se realiza bajo un esquema cíclico, utilizando los siguientes tipos de respaldo:

Completa: Un backup completo copia todos los datos de la base de datos en el momento en que se realiza el backup. Incluye todos los archivos de datos y de log necesarios para restaurar la información

Incremental: el backup incremental no existe como un tipo separado; en cambio, el concepto de backup incremental se maneja a través de los backups de registros de transacciones. Un backup de registros de transacciones copia solo los registros de transacciones que han ocurrido desde el último backup de registros de transacciones, ya sea completo o incremental.

Diferencial: Un backup diferencial copia solo los datos que han cambiado desde el último backup completo. Esto significa que cada backup diferencial depende del último backup completo realizado.

7.3. Del Rotulado de las Copias de Seguridad:

- El formato de los nombres de la copia contener obligatoriamente los siguientes datos:

Ejemplo:

- Nombre del servidor = LEONIDAS
- Nombre de la base datos de la información = FARMACIA
- Fecha y hora de creación = dd_mm_yyyy_hhmmss
- Identificador de Tipo de backup (BK), seguido de tipo copia de respaldo (BKFULL: COMPLETO, BKDIF: Diferencial, BKLOG: Log)

LEONIDAS_FARMACIA_10_08_2024_230000_BKFULL.bak

7.4. De las Pruebas de la Información Respaldata

- El responsable de la unidad de informática elabora anualmente el Plan de pruebas de restauración de información, el cual es una lista de actividades que se realiza a fin de validar que el proceso de respaldo, la periodicidad mínima de las pruebas debe ser trimestral.
- El operador de backup se encarga de realizar las pruebas programadas y no programadas; registra el resultado en el "Registro de Pruebas de la Información" (ver Anexo N°5)
- El oficial de Seguridad de la información supervisa las pruebas, evalúa el cumplimiento y elabora un informe con los resultados al Jefe de la OEI.

7.5. De la Solicitud Restauración de la Información.

- El funcionario responsable de la unidad orgánica, podrá solicitar formalmente (documento o correo electrónico) a la oficina de Estadística e Informática, la recuperación de la información perteneciente a su unidad orgánica adjuntando el formato de Solicitud de Restauración de Información (Anexo N°4).
- El operador de Respaldo de la información, deberá verificar el tipo de información solicitada, conforme señalado en la presente directiva, atenderá el requerimiento siempre y cuando la información solicitada se encuentre dentro de la política de retención asociada al proceso.
- Para la recuperación de la información, el operador del Respaldo de la información, realiza la búsqueda de lo solicitado, verificando su funcionalidad a través de los sistemas de información.
- En caso que no se pueda recuperar la información respaldada, el operador del respaldo de la información, informara al usuario solicitante, el motivo y causas presentadas.
- El operador de respaldo de la información, para la recuperación de la información, debe registrar en el documento "Registro de información recuperada" (Anexo N°6).

En el caso que no se pueda recuperar la información respaldada, se debe registrar de igual manera lo acontecido en el mismo formato.

7.6. De las condiciones de Almacenamiento y Seguridad Física

- a) El medio de respaldo de la información histórica, serán almacenadas debidamente identificados.
- b) El acceso a los ambientes donde se procesa y resguarda las copias de respaldo de información será restringida, será autorizada por la jefatura de la oficina de Estadística e Informática.
- c) El ambiente donde se custodia los medios de almacenamiento de información, deberá contar con las adecuadas condiciones de temperatura y no presentar humedad, deberá tener un sistema contra incendio, además presentar con sistemas de seguridad que garantice su protección contra robos.



VII. ANEXOS

Forman parte de la presente Directiva los anexos siguientes:

Anexo N°1: Directorio de Información a Respaldar.

Anexo N°2: Planificación de Copias de Respaldo.

Anexo N°3: Registro de Respaldo de Información

Anexo N°4: Solicitud de Restauración de Información.

Anexo N°5: Registro de Pruebas de la Información

Anexo N°6: Registro de Información Recuperada



MINISTERIO DE SALUD
HOSPITAL NACIONAL HIPOLITO UNANUE

ING. MÓNICA MICHÉ ROSAS SÁNCHEZ
C.I.F. N° 143558
Jefe de Oficina de Estadística e Informática

Ministerio
de SaludHOSPITAL NACIONAL
POLITO UNALVE

OFICINA DE ESTADISTICA E INFORMATICA - UNIDAD DE INFORMATICA

DIRECTORIO DE INFORMACIÓN A RESPALDAR

Fecha de Actualización: __/__/__

[illegible]

(a) Grupo de Backup (Servidor de Archivos, Máquinas Virtuales, Base de Datos, otros)

Criticidad: Crítica / Necesaria / Corriente

Periodicidad: Diario / Semanal / Quincenal / Mensual

(d) Tipo de Cópia de Respaldo: Completo / Incremental / Diferencial



Anexo N° 3

[illegible]

ANEXO N° 4

 PERÚ Ministerio de Salud	HOSPITAL NACIONAL HIPOLITO UHANE	SOLICITUD DE RESTAURACIÓN DE INFORMACION	N°

Fecha de la solicitud (Día/Mes/Año):							
Nombre del solicitante:							
Oficina o Unidad:							
Para ser llenada por el solicitante						Para uso del encargado de copias de respaldo (UNIDAD DE INFORMATICA)	
Nombre del activo Informático para backup de base de datos de respaldo	Base de datos	Servidor	Rutas del backup de respaldo.	Fecha de corte del activo a restaurar (DD/MM/YYYY)	Observación	Fecha de la restauración (DD/MM/YYYY)	Ubicación o descripción de la restauración
Observaciones:							
Firma y Sello Jefe de Unidad Orgánica							

REGISTRO DE PRUEBAS DE LAS COPIAS DE SEGURIDAD

[illegible]

Anexo N° 6

[illegible]