MINISTERIO DE SALUD
HOSPITAL NACIONAL
HIPÓLITO UNANUE

N° 280-2024-DG-HNHU

RESOLUCIÓN DIRECTORAL

El Agustino, 28 de octubre de 2024

VISTO;

El Expediente N° **24-040470-001**, que contiene la Nota Informativa N° 313-2024-OEI/HNHU a través de la cual la Oficina de Estadística e Informática solicita aprobación sobre Directiva Administrativa: Disposiciones para el Acceso al Centro de Datos del Hospital Nacional Hipólito Unánue, y;

CONSIDERANDO:

Que, de conformidad con el numeral VI del Título Preliminar la Ley N° 26842, Ley General de Salud, establece que "Es de interés público la provisión de servicios de salud, cualquiera sea la persona o institución que los provea. Es responsabilidad del Estado promover las condiciones que garanticen una adecuada cobertura de prestaciones de salud a la población, en términos socialmente aceptables de seguridad, oportunidad y calidad";

Que, es así que, según el artículo II del Título Preliminar de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, señala sobre ***Principio de servicio al ciudadano*** *que, "Las entidades del Poder Ejecutivo están al servicio de las personas y de la sociedad; actúan en función de sus necesidades, así como del interés general de la nación, asegurando que su actividad se realice con arreglo a:*

1. *Eficacia: la gestión se organiza para el cumplimiento oportuno de los objetivos y las metas gubernamentales.*
2. *Eficiencia: la gestión se realiza optimizando la utilización de los recursos disponibles, procurando innovación y mejoramiento continuo.*
3. *Simplicidad: la gestión elimina todo requisito y procedimiento innecesario. Los procesos deben ser racionales y proporcionales a los fines que se persigue cumplir.*
4. *Sostenibilidad ambiental: la gestión se orienta al uso racional y sostenible de los recursos naturales.*
5. *Predictibilidad: la gestión brinda información veraz, completa, confiable y oportuna, que permita conciencia bastante certera acerca del resultado de cada procedimiento.*
6. *Continuidad: la gestión adopta como referentes de actuación las políticas de Estado acordadas, así como los objetivos y metas de planeamiento y programación multianual establecidos.*
7. *Rendición de cuentas: los responsables de la gestión dan cuenta periódicamente, a la población, acerca de los avances, logros, dificultades y perspectivas.*
8. *Prevención: gestión para enfrentar los riesgos que afecten la vida de las personas, y para asegurar la prestación de los servicios fundamentales.*
9. *Celeridad: la gestión debe asegurar que todo procedimiento cumpla su trámite regular dentro de los plazos establecidos, evitando actuaciones que dificulten su desenvolvimiento, bajo responsabilidad";*

Que, por otro lado, 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, asimismo, el artículo 4° de la referida Ley, se establece sobre la finalidad del proceso de modernización de la gestión del Estado, que: *"El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos. El objetivo es alcanzar un Estado:*

a) Al servicio de la ciudadanía.
b) Con canales efectivos de participación ciudadana.
c) Descentralizado y desconcentrado.
d) Transparente en su gestión.
e) Con servidores públicos calificados y adecuadamente remunerados.
f) Fiscalmente equilibrado;

Que, por su parte, el Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud y sus modificatorias, establece en el artículo 1° sobre la finalidad que: *"El presente Decreto Legislativo determina y regula el ámbito de competencia, las funciones, la estructura orgánica básica del Ministerio de Salud y su función rectora como único ente que establece políticas en materia de salud a nivel nacional, con la finalidad de disponer la estandarización de los procesos, a fin de brindar atenciones oportunas y de calidad. Determina también sus relaciones de articulación y coordinación con otras entidades"*;

Que, a su vez, del referido Decreto, se señala en su artículo 7° sobre las funciones específicas; en el marco de sus competencias, el Ministerio de Salud cumple las siguientes funciones:

a) Regular la organización y prestación de servicios de salud (...)"
c) Establecer la política de aseguramiento en salud, regular a las entidades y los procesos vinculados a ésta (...)"

Que, por otro lado, la Resolución Ministerial N° 450-2017, que aprueba los Lineamientos para la elaboración y aprobación de los Manuales de Operaciones de los órganos desconcentrados del Ministerio de Salud: Direcciones de Redes Integradas en Salud, tiene por finalidad; establecer disposiciones para la elaboración y aprobación de los manuales de Operaciones de los Órganos Desconcentrados del Ministerio de Salud: Direcciones de Redes Integradas de Salud de Lima Metropolitana;

Que, también, con Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio Norma Técnica Peruana "NTP-ISO/IEC27001:2014 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:

a) *Es apropiada al propósito de la organización.*
b) *Incluye objetivos de seguridad de la información (...) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información.*
c) *Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e*
d) *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.

MINISTERIO DE SALUD
HOSPITAL NACIONAL
HIPÓLITO UNANUE

N° 280 -2024-DG-HNHU

RESOLUCIÓN DIRECTORAL

El Agustino, 28 de octubre de 2024

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, ahora bien, con Informe Técnico Sustentatorio la Unidad de Informática de la Oficina de Estadística e Informática remite la propuesta de la Directiva Administrativa: "Disposiciones para el acceso al Centro de Datos del Hospital Nacional Hipólito Unánue", la cual tiene como finalidad brindar los conocimientos técnicos, administrativos, lineamientos y responsabilidades en el ámbito de actuación para la administración y acceso al centro de datos; asegurando el correcto funcionamiento, seguridad y disponibilidad de la infraestructura de redes y servidores; a su vez, señala que, el Centro de Datos del HNHU alberga la infraestructura crítica que soporta los servicios de tecnología de la información del hospital, es así que la presente directiva pretende alinearse con estándares internacionales y nacionales, tales como ISO/IEC 27001:2013, ANSI/TIA-942-B y las normativas locales vigentes, garantizando que las mejores prácticas en la gestión de centros de datos se apliquen en el HNHU;

Que, también con Nota Informativa N° 033-2024-UO-OPE/HNHU de fecha 09 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 su opinión favorable al citado documento, al haberse realizado el levantamiento de las observaciones y verificado que: se establecen aspectos técnicos en materia específica, se han considerado criterios básicos en su redacción, cuenta con la estructura adecuada, se establecen responsabilidades y roles conforme a lo señalado en el Reglamento de Organización y Funciones del HNHU;

Que, a razón de ello, con Nota Informativa N° 333-2024-OEI/HNHU de fecha 11 de setiembre de 2024, la Oficina de Estadística e Informática remite a la Dirección Ejecutiva de la Oficina de Planeamiento Estratégico el levantamiento de las observaciones, a fin de obtener la aprobación de la Directiva Administrativa: "Disposiciones para el Acceso al Centro de Datos del Hospital Nacional Hipólito Unánue";

Que, finalmente, mediante Nota Informativa N° 066-2024-OPE-HNHU de fecha 13 de setiembre de 2024, la Dirección Ejecutiva de la Oficina de Planeamiento Estratégico remite a

la Dirección General los actuados, con la finalidad de ser trasladado dicho documento a la Oficina de Asesoría Jurídica para emitir opinión legal correspondiente

Que, estando a lo informado por la Oficina de Asesoría Jurídica, con el Informe N° 453-2024-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 conformidad con la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, Resolución Ministerial N° 450-2017, que aprueba los Lineamientos para la elaboración y aprobación de los Manuales de Operaciones de los órganos desconcentrados del Ministerio de Salud: Direcciones de Redes Integradas en Salud y Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio Norma Técnica Peruana "NTP-ISO/IEC27001:2014 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 y el literal c) del artículo 6° de la Resolución Ministerial N° 099-2012/MINSA que aprobó el Reglamento de Organización y Funciones del Hospital Nacional Hipólito Unánue;

SE RESUELVE:

ARTÍCULO 1.- APROBAR la Directiva Administrativa N° 07 -HNHU/OEI-UI-2024 – Directiva Administrativa: "Disposiciones para el acceso al Centro de Datos del 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° 07 -HNHU/OEI-UI-2024 – Directiva Administrativa: "Disposiciones para el acceso al Centro de Datos del Hospital Nacional Hipólito Unánue".

ARTÍCULO 3.- DAR TÉRMINO a la Resolución Directoral N° 277-2017-HNHU-DG de fecha 29 de diciembre de 2017 que aprobó la Directiva Administrativa N° 022-HNHU/2017/OEI, "Administración de Redes y Servidores 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 Unanue"
DR. MOISES ENRIQUE TAMBINI ACOSTA
Director General (e)
CMP: 16412

META/VMIF/vcrc
DISTRIBUCION
( ) *Oficina de Estadística e Informática*
( ) OAJ
(...) *Dirección Ejecutiva de la Oficina de Planeamiento Estratégico*
( ) O. Comunicaciones
(...) OCI
( ) ARCHIVO

DIRECTIVA ADMINISTRATIVA: "DISPOSICIONES PARA EL ACCESO AL CENTRO DE DATOS DEL HOSPITAL NACIONAL HIPOLITO UNANUE"

I. FINALIDAD

Establecer los lineamientos, responsabilidades y el ámbito de actuación para la administración y acceso al centro de datos del Hospital Nacional Hipólito Unanue (HNHU), asegurando el correcto funcionamiento, seguridad y disponibilidad de la infraestructura de redes y servidores. Este documento busca además garantizar la confidencialidad, integridad y disponibilidad de la información crítica, contribuyendo al buen desempeño de los servicios de salud y a la continuidad operativa del hospital.

II. OBJETIVO

Definir un marco normativo y procedimental para la gestión, administración, y acceso seguro al centro de datos del HNHU, en concordancia con estándares internacionales y normativas nacionales aplicables.

III. AMBITO DE APLICACIÓN

Esta directiva es aplicable a todo el personal técnico, administrativo y de soporte que interactúe directa o indirectamente con el Centro de Datos del HNHU, incluyendo la infraestructura física, gestión de la información, conectividad de red y sistemas de soporte asociados. También incluye a terceros que realicen actividades en las instalaciones del centro de datos bajo autorización.

IV. BASE LEGAL

- Ley N° 26842, Ley General de Salud.
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud y sus modificatorias.
- Resolución Ministerial N° 450-2017, que aprueba los Lineamientos para la elaboración y aprobación de los Manuales de Operaciones de los órganos desconcentrados del Ministerio de Salud: Direcciones de Redes Integradas en Salud.
- Resolución Ministerial N° 004-2016-PCM4 - Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnica de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2a Edición en todas las entidades integrantes del Sistema Nacional de Informática".
- ANSI/TIA-942-B: Estándar de Infraestructura de Telecomunicaciones para Centros de Datos.

- ISO/IEC 22237-1: Edificios e Infraestructura Civil - Define los requisitos para el diseño y construcción de edificios de centros de datos, incluidas las estructuras, el acceso, la seguridad física, la protección contra incendios y las consideraciones ambientales.
- ISO/IEC 22237-3: Control Ambiental-Trata sobre las instalaciones de climatización, control de temperatura, humedad, y otras condiciones ambientales críticas para el buen funcionamiento del equipo de TI.
- ISO/IEC 22237-4: Infraestructura de Telecomunicaciones-Especifica los requisitos para la infraestructura de cableado y las telecomunicaciones dentro del centro de datos, asegurando una conectividad eficiente y confiable.
- ISO/IEC 22237-5: Protección Física-Define las medidas para proteger el centro de datos contra amenazas físicas, como intrusiones, incendios, inundaciones, y otros riesgos.
- ISO/IEC 22237-6: Seguridad-Se enfoca en la seguridad del centro de datos, tanto en términos de protección física como lógica (ciberseguridad), para garantizar la integridad y disponibilidad de los datos y sistemas.
- ISO/IEC 22237-7: Gestión y Operación-Proporciona directrices para la operación y el mantenimiento del centro de datos, asegurando que las prácticas operativas cumplan con los requisitos de eficiencia, seguridad, y disponibilidad.
- ISO/IEC 27001:2013: Sistema de Gestión de Seguridad de la Información
- TIA/EIA-942: Norma que especifica los requisitos para la infraestructura de telecomunicaciones dentro de los centros de datos, cubriendo aspectos como la disposición física, energía, refrigeración, y cableado.
- NTA N°119-MINSA/DGIEM-V.01 Norma Técnica de Salud "Infraestructura y Equipamiento de los establecimientos de salud de tercer nivel de atención.

V. DISPOSICIONES GENEREALES

- **Obligatoriedad:** Todos los empleados, contratistas y personal autorizado que interactúen con el centro de datos deben cumplir con esta directiva, asegurando la protección, confidencialidad y operación eficiente del centro de datos (Data Center).
- **Divulgación:** La directiva será difundida entre todo el personal pertinente, y se realizarán sesiones de capacitación periódicas para asegurar que todos comprendan y sigan las disposiciones establecidas.
- **Monitoreo y Control:** El cumplimiento de esta directiva será supervisado regularmente mediante auditorías internas y externas. Cualquier desviación o incumplimiento será registrado y abordado de inmediato.
- **Revisión Periódica:** Esta directiva será revisada anualmente o cuando las circunstancias tecnológicas, normativas o de operación lo requieran, para asegurar que permanezca actualizada y eficaz.
- **Confidencialidad:** Toda la información relacionada con la infraestructura, configuraciones, políticas de seguridad y operaciones del centro de datos es confidencial y no debe ser divulgada sin autorización previa.

5.1. Definiciones Operativas

- **Administrador de Redes y Servidores:** Es el profesional calificado de la Unidad de Informática del Hospital Nacional Hipólito Unanue y con experiencia profesional en su campo de acción.
- **Centro de Datos (DATA CENTER)**: Instalación física donde se alojan servidores, sistemas de almacenamiento, equipos de red y otros componentes críticos de TI.
- **Contraseña**: Seña secreta que permite el acceso a información reservada en un sistema, servicio, sitio web, computador o a un dispositivo móvil.
- **Control de Acceso**: Medidas y procedimientos implementados para asegurar que sólo personal control de autorizado pueda acceder al centro de datos.
- **Cuenta de Usuario**: Es un objeto que se crea para que una entidad le permita acceder a los recursos. Una entidad de este tipo puede representar un ser humano, un servicio de software o una computadora. Las cuentas de usuario permiten a estas entidades iniciar sesión, establecer preferencias y acceder a recursos según los permisos de su cuenta.
- **IDS/IPS:** Los Sistema de Detección de Intrusos (IDS) como los Sistemas de Prevención de Intrusos (IPS) se encargan de vigilar el tráfico con el fin de detectar actividades sospechosas o no autorizadas.
- **Incidente**: Es cualquier evento que no forma parte de la operación estándar de un servicio y que causa o puede causar una interrupción o una reducción de calidad de este.
- **Infraestructura Tecnológica**: Conjunto de recursos, componentes y sistemas que forman la base para la operación y gestión de tecnologías de la información. Incluye hardware, software, redes de comunicaciones, políticas y servicios.
- **Requerimiento**: Es cualquier petición que requiera una modificación de la infraestructura tecnológica.
- **Redes:** Conjunto de dispositivos interconectados para la transmisión de datos.
- **Servidores**: Equipos informáticos que proporcionan servicios y recursos a otros dispositivos en la red.

5.2. SIGLAS

- HNHU: Hospital Nacional Hipólito Unanue
- OEI: Oficina de Estadística e Informática.
- UI: Unidad de Informática.
- TI: Tecnología de Información

VI. DISPOSICIONES ESPECIFICAS

6.1 Respecto a la Seguridad física

- El Data Center deberá contar con un sistema de autentificación biométrica y/o sistema de autentificación para el ingreso de personal autorizado.

- La puerta de acceso al Data Center debe permanecer cerrada, aun con personas en su interior.
- Se deberá registrar el ingreso de todas las personas que ingresen al Data Center en el formato de Registro de Visitas, Anexo N°2
- El jefe responsable debe delegar el monitoreo de la bitácora de control de acceso físico y/o remoto al Data Center, el encargado del monitoreo deberá informar de forma mensual los ingresos efectuados al Data Center.
- La puerta del Data center debe tener rótulos informativos de acceso restringido.
- El Data Center debe contar con un mecanismo de control de aire acondicionado que garantice un entorno operativo adecuado al equipo instalado en el Data Center, con un nivel de temperatura interior de 18°C y 27°C.
- Todos los Racks o gabinetes deben permanecer con las puertas completamente cerradas y aseguradas.
- El Data Center deberá contar con un sistema de monitoreo CCTV y sistemas de alarmas que permitan la supervisión constante.

6.2 Respecto a la Seguridad de la Red

- El personal de la unidad de informática debe administrar y monitorear a través del cortafuego (Firewalls) los accesos no autorizados, intentos de intrusión, peticiones no legítimas y conexiones a servidores remotos en lista negra.
- El personal de la unidad de informática debe segmentar la red de tal manera que se minimice los puntos de colisión.
- El personal de la unidad de informática de hacer pruebas regulares de penetración para asegurarse se estar actualizados en los parches de seguridad correspondientes.
- El personal de la unidad de informática debe aplicar correctamente sistemas de IDS/IPS para detectar y prevenir ataques a la infraestructura tecnológica del HNHU.
- El personal de informática debe configurar correctamente la seguridad de los accesos a los puertos de los switch y routers.

6.3 Respecto al Personal autorizado

a) El acceso al Data Center del personal autorizado solo está permitido para aquellos que pertenecen a la unidad de informática y cuenten con la función de administradores de red y/o servidores.

b) El personal que requiera el acceso al Data Center debe tener la autorización expresa del responsable de la unidad de informática.

c) El personal autorizado debe encontrarse registro en la lista de usuarios autorizados al Data Center y/o en el lector biométrico de ingreso.

6.4 Respeto al Nivel de Accesos

a) El acceso al Data Center del HNHU deben efectuarse previa coordinación con la jefatura de la OEI, considerando un mínimo de 24 horas antes y de forma

documentada, en caso de una urgencia deberán coordinar con la jefatura de la OEI, quien autorizara el acceso.

b) El personal externo que tenga programado desarrollar trabajos en el Data Center y se encuentre autorizado, deberá ingresar con todas sus herramientas para el desarrollo de sus actividades, sus artículos personales y/o artículos de otra índole deberán quedar en custodia de la Unidad de Informática.

c) Toda persona que ingrese al Data center deberá firmar y aceptar el acuerdo de confidencialidad de no divulgación de información, la cual constituye NO divulgar información asociada a la infraestructura, diseño y datos al interior de equipos hardware, sensores, puertas, rack y demás elementos del entorno del Data Center

d) Se encuentra prohibido extraer, copiar, manipular, comunicar, fotografiar, respaldar y/o duplicar en cualquiera de las formas la disposición del Data Center del HNHU.

e) Todas las personas que ingresan y todas las actividades realizadas en el Data Center son monitoreadas por las cámaras que se encuentran ubicadas en diferentes puntos de las instalaciones del Data Center. Las grabaciones realizadas pueden ser revisadas y tomadas como pruebas en caso que sean necesarias para investigaciones de cualquier tipo.

6.5 Respecto al Personal no autorizado

a) Para aquellas personas de otras áreas y externos a la entidad que NO están autorizadas, solo estará permitido el acceso de manera temporal y por cuestiones estrictamente justificadas.

b) Cualquier persona NO autorizada que requiera acceso al centro de Datos, para desarrollar actividades de mantenimiento, implementación o visita, deberá solicitarlo mediante documento y/o formato de Formato de Solicitud de acceso a centro de Datos anexo N°1.

c) Aprobada la solicitud, el responsable de informática designará a un personal autorizado para acompañar e indicar los ambientes a intervenir por parte del personal externo, en caso de denegar la solicitud el responsable de UI deberá informar los motivos por el cual fueron denegados los accesos.

d) El personal autorizado con acceso temporal deberá ingresar en un personal autorizado por la UI.

6.6 Bitácora de Control de Visitas

a) Toda persona que ingrese al Data Center sin excepción sea trabajador interno, visitas, servicio de limpieza, proveedores y otros, deben registrarse en la bitácora de control de acceso físico al centro de datos. Asimismo, se debe llevar un registro de los servicios que se realizará en el centro de datos.

b) El responsable de la UI debe gestionar con el personal bajo su cargo, que toda persona que ingrese al Data Center complete el formulario con los siguientes datos: Fecha, hora de entrada y salida, nombre completo, código único identificación (DNI), nombre de la empresa, actividad a realizar el cual deber estar

codificado, numero de formulario de solicitud de acceso en caso de ser personal con acceso temporal.

6.7 Respecto a la Limpieza de área restringidas

a) El Data Center debe tener un calendario con fechas y horarios de limpieza dentro del mismo, el cual deberá ser coordinado con el responsable de la UI.

b) El responsable de la UI asignará a un personal responsable de velar que la persona delegada, cumpla con los procedimientos de limpieza, utilizando equipo y limpiadores que no dañen o perjudiquen la infraestructura del lugar, el personal asignado permanecerá mientras que el personal de limpieza ejecuta sus labores.

c) Los usuarios del Data Center deberán desechar los desperdicios generados por los desembalajes de equipos, tales como: cajas de cartón, protectores de cartón y/o tecnopor, plásticos, bolsas de papel, etc., coordinando esta actividad con el personal de aseo. Cualquier elemento considerado como basura o desecho, se tratará como una violación a la presente política y será retirado sin perjuicio a reclamaciones posteriores por parte del usuario.

6.8 Respecto a los trabajos a Desarrollar en el Data Center

a) Personal externo que tenga programado desarrollar trabajos físicos o lógicos en el Data Center debe ingresar portando sus Equipos de Protección Personal(EPP), implementos de seguridad obligatorios de acuerdo con las actividades a realizar, además de contar con el seguro complementario de trabajo con riesgo, este debe ser presentado junto al "Formulario de Acceso del Personal NO autorizado".

b) Personal que realice algún servicio en el Data Center, debe mantener la limpieza en el interior del Centro de Datos durante y después de culminada las labores ejecutadas.

c) El uso de elementos que genere fuentes de calor y materiales inflamables, estos deben ser controlados y monitoreados por personal de la Unidad de Informática.

d) Cualquier equipo que genere campos magnéticos deben ser monitoreados por personal de la UI y el personal externo del servicio.

e) El horario de las actividades de mantenimiento para el desarrollo de actividades programadas por personal externo, se hará previa coordinación con el responsable de la Unidad de Informática o quien haga sus veces.

f) Todos los usuarios y proveedores de servicios una vez culminada el trabajo realizado en los Servidores del Data Center deben de proteger el terminal con un bloqueador de teclado o una medida similar a fin de evitar acceso no autorizado.

6.9 Respecto a las Restricciones

a) Manipular o acceder sin autorización a los equipos y gabinetes

b) No está permitido retirar equipo o accesorios sin autorización expresa por escrito del responsable de la Unidad de Informática.

c) No debe utilizarse el Data Center para almacenar cajas, documentos y equipos no instalados.

d) Bloquear, abrir y manipular puertas de acceso, cámaras de seguridad, sensores de humo, controles de climatización o enfriamiento y las alarmas contra incendios.

e) Ingresar al Data Center llevando consigo armas de fuego o punzo cortantes.

f) Ingresar Al Data Center en estado de ebriedad.

g) Ingresar al Data Center llevando consigo celulares, cámaras fotográficas y/o filmadoras no autorizadas.

h) Ingresar al Data Center con cigarrillos o cualquier elemento que genere humo.

i) Ingresar al Data Center con alimentos y bebidas de cualquier tipo.

j) Ingresar al Data Center con productos clasificados como inflamables.

k) Ingresar al Data Center con equipos que generen campos magnéticos que interfieran con las señales de comunicación.

l) Interferir en sensores, cableados, accesos, equipos, cámaras u otros que no estén asociados a los trabajos que están programados y/o autorizados.

m) Modificar, adulterar, conectar, desconectar elementos tales como equipo de redes, de acceso, entre otras actividades que pudieran entorpecer el normal funcionamiento del Data Center.

n) Si se requiere energizar equipos eléctricos y/o electrónicos, se debe usar los enchufes de servicio ubicado en paredes, de ninguna manera en las unidades de distribución (PDU) de uso exclusivo de los equipos en los gabinetes del Centro de Datos.

o) Adulterar las etiquetas de identificación y de inventario de equipos que pertenecen a la infraestructura del Data Center.

VII. RESPONSABILIDADES

- Es responsabilidad de todo el personal de la Unidad de Informática prevenir el ingreso de personal no autorizado a las instalaciones del Data Center.
- Los Jefes de Departamentos, Oficinas y Personal del Hospital Nacional Hipólito Unanue son responsables del cumplimiento de la presente directiva, en lo que les corresponda de acuerdo con su competencia.
- Oficina de Estadística e Informática, es la encargada asegurar que los recursos necesarios estén disponibles para el cumplimiento de las presentes directivas
- Administrador de Redes y Servidores:
  - Asegurar el correcto funcionamiento de la red y servidores.
  - Garantizar la seguridad y disponibilidad de la información.
  - Coordinar con otros departamentos para satisfacer sus necesidades tecnológicas.
  - Mantenerse actualizado con las mejores prácticas y normativas del sector.

VIII. DISPOSICIÓN FINAL:

Cualquier modificación o actualización de este procedimiento deberá ser aprobada por la Jefatura de la oficina de Estadística e Informática del HNHU.

IX. ANEXOS:

Forman parte de la presente Directiva los anexos siguientes:

- Anexo N°1 Formulario de solicitud de acceso.
- Anexo N°2 Formato de Registro de Visitas a la Infraestructura de TI

DIRECTIVA ADMINISTRATIVA: "DISPOSICIONES PARA EL ACCESO AL CENTRO DE DATOS DEL HOSPITAL NACIONAL HIPOLITO UNANUE"

ANEXO N°1 SOLICITUD DE ACCESO A CENTRO DE DATOS (DATA CENTER)

FORMATO DE SOLICITUD DE ACCESO A CENTRO DE DATOS (Data Center)
Directiva Administrativa N° - HNHU/2024

DATOS DE LA SOLICITUD

Tipo de Solicitud: ☐ Personal Interno ☐ Personal Externo Empresa/ Entidad: _____

Fecha de Solicitud : __/__/____ Tipo de Ingreso (Presencial/ Manos Remotas) : _____

Dirección/Oficina/Departamento:		Servicio/Unidad :
Datos del Personal que solicita el acceso al Data Center	Nombres y Apellidos :	
	DNI: Celular :	Correo Electrónico :
	Cargo :	
Fecha de Solicitud a Ingreso al Data Center	Del __/__/____ al __/__/____ Hora de Inicio : __:__	Hora Finalización : __:__
Describa la actividad a Realizar:		

Observaciones:	Firma del Solicitante

FIRMAS PARA AUTORIZAR REQUERIMIENTO (LLENADO SOLO POR LA UNIDAD DE INFORMÁTICA – OEI)

V°.b.° Jefe(a) OEI	V°.b.° Responsable de UI

COMPROMISO DE CONFIDENCIALIDAD

En virtud del cumplimiento de la Constitución Política del Perú, la Ley N° 29733 - Ley de Protección de Datos Personales y de lo señalado en la Ley N° 26842, Ley General de Salud, acepto y reconozco que tengo acceso al Centro de Datos para el cumplimiento de las actividades detalladas lineas arriba.

En ese sentido, por este medio me obligo a no divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir, sin la autorización expresa y por escrito del titular del HNHU, la información y documentación a la que tengo acceso, bajo responsabilidad.
En caso de incumplimiento, me someto a las responsabilidades de índole administrativa, penal y civil conforme a Ley.

Las obligaciones y derechos inmersos en el presente compromiso de confidencialidad estarán vigentes a partir de la fecha de de la solictud, durante el tiempo que dure esta relación y después de la fecha en que se haya dado por terminada la relación contractual o laboral, sin importar la razón de la misma.

Por tanto, expreso mi compromiso de respetar el derecho fundamental a la protección de los datos personales, la intimidad personal y familiar de los usuarios y a guardar la reserva debida sobre la información a la que tuviera acceso por razón de mi actividad, prolongándose esta reserva incluso después que finalice el ejercicio de mi relación contractual o laboral con mi Institución.

Firma:

DNI N°:

HOSPITAL NACIONAL HIPOLITO UNANUE OFICINA DE ESTADISTICA E INFORMATICA V° B°

ANEXO N°2 REGISTRO DE VISITAS

UNIDAD DE INFORMATICA- OEI

BITACORA DE INGRESO AL CENTRO DE DATOS (DATA CENTER) DEL HNHU

MES:

AÑO :

ID	Nombres y Apellidos	DNI	N° Solicitud Aprobada	Actividad a Realizar (*)	Fecha y Hora de Ingreso	Ingreso de Elementos	Servidor /Aplicativo al que accedió	Nombre de Acompañante de TI	Fecha y Hora de Salida	Firma

(*) Actividades

1: Instalación y/o Configuración de Equipos
2: Mantenimiento de Equipos
3: Instalación de Equipos
4: Monitoreo de Equipos
5. Otros