



Resolución Directoral

Lima, 17 de Julio de 2025

VISTO: El Expediente Administrativo Registro N° 22330-2025, que contienen, entre otros, el Informe N° 099-2025-OEI-HNDM, de fecha 3 de julio de 2025, a través del cual el Jefe de la Oficina de Estadística e Informática, solicita la conformación del Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo";

CONSIDERANDO:

Que, el artículo VI del Título Preliminar, de 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, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, en adelante Ley de Gobierno Digital, tiene como objeto establecer el marco de gobernanza del gobierno digital para una adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el artículo 6° de la Ley de Gobierno Digital, precisa que, el gobierno digital consiste en el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público; asimismo, se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital; dicho gobierno digital comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos;

Que, a través del Decreto de Urgencia N° 007-2020, se aprueba el Marco de Confianza Digital, en adelante Marco de Confianza Digital, con el objeto de establecer las medidas que resulten necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional;

Que, el artículo 5° del Marco de Confianza Digital, dispone medidas para su fortalecimiento, así como que, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos;

Que, el artículo 7° y el numeral 9.3 del artículo 9°, del Marco de Confianza Digital, disponen medidas para su fortalecimiento, crea el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital; asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos; y, que, las entidades de la administración pública deben implementar un Equipo de Respuesta ante Incidentes de Seguridad Digital - CSIRP;

Que, mediante Decreto Supremo N° 029-2021-PCM, se aprobó Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; y, en los numerales 104.1, 104.2 y 104.3, del





artículo 104°, se define al Equipo de Respuestas ante Incidentes de Seguridad Digital como aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros. Asimismo, se ha dispuesto que, las entidades de la Administración pública conforman un Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional. Dichos Equipos forman parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad o de la unidad de organización especializada en seguridad de la información o similar prevista en su estructura orgánica o funcional. Su conformación es comunicada a la Secretaría de Gobierno Digital mediante los mecanismos dispuestos para tal fin. La Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital en el país, emite opinión técnica especializada a pedido de una entidad a fin de revisar o validar aspectos técnicos sobre la conformación de un Equipo de Respuesta ante incidentes de Seguridad Digital, conforme a lo establecido en el presente Reglamento y normas complementarias, respectivamente;



Que, a través del link: <https://www.gob.pe/institucion/pcm/informes-publicaciones/5057847-guia-para-la-conformacion-e-implementacion-del-equipo-de-respuestas-ante-incidentes-de-seguridad-digital>, el 17 de enero de 2024, se ha publicado la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital, elaborada por la Secretaría de Gobierno y Transformación Digital, de la Presidencia del Consejo de Ministros, en adelante la Guía, la misma que tiene el propósito de orientar a las entidades públicas en la conformación e implementación de Equipos de Respuesta ante Incidentes de Seguridad y se constituye como un documento de trabajo referencial para dicha conformación;



Que, en el numeral 4.1.3 de la Guía, se precisan las funciones del Equipo de Respuesta ante Incidentes de Seguridad Digital, las cuales son las siguientes: a) Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, b) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad, c) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad, d) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital, e) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital, f) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos, g) Coordinar y colaborar a través del Centro Nacional de Seguridad Digital con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en el ámbito de las redes de confianza, h) Otras que determine la alta dirección de la institución;



Que, en el numeral 4.1.4 de la Guía, señala que, un equipo de respuestas ante incidentes de seguridad digital es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática, en tal sentido es responsabilidad de esta área o la que haga sus veces, la determinación de las responsabilidades del CSIRT mediante la designación de los roles relevantes. La responsabilidad se define en función del perfil del equipo y su autoridad, de esta manera puede cooperar incluso con equipos reguladores y/o fuerzas del orden. Los roles básicos son: a) Coordinador del CSIRT: Es el rol mínimo que debe existir dentro de una organización, es el encargo de realizar todas las actividades de gestión del CSIRT, así mismo es el punto de contacto con el CSIRT Nacional del Centro Nacional de Seguridad Digital. b) Gestor de Incidentes: Es el responsable de la gestión de los incidentes de seguridad digital, así como también de la comunicación del incidente al Centro Nacional de Seguridad Digital. c) Gestor de Redes y Comunicaciones: Es responsable de la seguridad redes de comunicación de la entidad, implementa medidas de cifrado para la protección de la confidencialidad de las comunicaciones y determina el modelo de monitorización de las mismas. d) Gestor de Infraestructuras Digitales: Es el responsable de la seguridad de los servidores e infraestructuras de nube, determina las reglas de seguridad a nivel del sistema operativo y aplicaciones. e) Oficial de Seguridad y Confianza Digital: Participa como miembro del CSIRT para realizar las funciones de apoyo en la gestión de incidentes y articulador de los ámbitos de seguridad y confianza digital que sean relevantes al incidente. f) Otros roles que determine la institución;



Que, asimismo, en el numeral 4.1.4 de la Guía, a manera de ejemplo, se señala que, el Equipo de Respuestas ante Incidentes de Seguridad Digital, estará conformado por: a) El/la Jefe/a de la Oficina de Tecnologías de la Información, quién será el coordinador del CSIRT; b) El/la Especialista en Seguridad Informática de la Oficina de Tecnologías de la Información quien se desempeñará en el rol de Gestor de incidentes; c) El/la Jefe/a de la Unidad de Redes e Infraestructura de la Oficina de Tecnologías de la Información quien se desempeñara en el rol de Gestor de Redes y comunicaciones y Gestor de Infraestructuras Digitales; d) El/la Oficial de Seguridad y Confianza Digital, quien tendrá el rol miembro del CSIRT;



Resolución Directoral

Lima, 17 de Julio de 2025

Que, el artículo 19°, del Reglamento de Organización y Funciones del Hospital Nacional "Dos de Mayo" aprobado mediante Resolución Ministerial N° 696-2008/MINSA, señala que la Oficina de Estadística e Informática es el órgano encargado de lograr que el Hospital provea la información estadística de salud y soporte informático, mecanización e integración de los sistemas de información requeridos para los procesos organizacionales;

Que, a través del Informe N° 074-2025-OEI-HNDM, de fecha 28 de mayo de 2025, el Jefe de la Oficina de Estadística e Informática, solicitó la conformación del Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital; solicitud que no se adecuaba a las disposiciones establecidas en la Guía, por lo que mediante Dictamen Legal N° 108-2025-OAJ-HNDM, de fecha 9 de junio de 2025, el Jefe de la Oficina de Asesoría Jurídica, ante la necesidad de la creación de dicho Equipo, recomendó que la Oficina Ejecutiva de Planeamiento Estratégico, emita opinión favorable sobre su creación como unidad funcional o recomendaciones para su implementación;

Que, mediante Nota Informativa N° 027-2025-ETO-OEPE-HNDM y Proveído N° 073-2025-OEPE-HNDM, de fecha 20 de junio de 2025, la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico Presupuesto, recomienda la conformación del Equipo de Respuesta ante Incidentes de Seguridad Digital del Hospital Nacional "Dos de Mayo"; señalando que, no corresponde crear una unidad funcional de seguridad digital independiente, debido a que ya existe el Equipo de Trabajo de Informática, a quien se le debe asignar dichas funciones; por lo que, mediante Informe N° 099-025-OEI-HNDM, de fecha 3 de julio de 2025, el Jefe de la Oficina de Estadística e Informática, propone que el Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo", esté conformado de la siguiente manera:

Nombre y Apellido	Rol en el CSIRT
Ing. Javier Gustavo JORDAN VELA	Coordinador del CSIRT
Ing. Jessica LAZARO RENGIFO	Gestor de Incidencias
Ing. Carlos Humberto VIERA GUTIERREZ	Oficial de Seguridad y Confianza Digital

Estando a lo informado por la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico y por el el Jefe de la Oficina de Estadística e Informática;

Con las visaciones del Director Adjunto de la Dirección General, 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, del Jefe de la Oficina de Asesoría Jurídica;

De conformidad con lo establecido en la Resolución Ministerial N° 696-2008/MINSA, que aprueba el Reglamento de Organización y Funciones del Hospital Nacional "Dos de Mayo" y la Resolución Ministerial N° 886-2023/MINSA, de fecha 15 de setiembre de 2023, que designa temporalmente al Director de Hospital III (CAP- P N° 001), de la Dirección General del Hospital Nacional "Dos de Mayo";

SE RESUELVE:

Artículo 1°.- Conformar el Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo", adscrito a la Oficina de Estadística e Informática, integrado por los siguientes servidores civiles:



Nombre y Apellido	Rol en el CSIRT
Ing. Javier Gustavo JORDAN VELA	Coordinador del CSIRT
Ing. Jessica LAZARO RENGIFO	Gestor de Incidencias
Ing. Carlos Humberto VIERA GUTIERREZ	Oficial de Seguridad y Confianza Digital

Artículo 2°.- El Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo", tiene, entre otras, las siguientes funciones:

- Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
- Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad,
- Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
- Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
- Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.
- Coordinar y colaborar a través del Centro Nacional de Seguridad Digital con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en el ámbito de las redes de confianza.

Artículo 3°.- Disponer que, las Jefaturas de los Departamentos, Oficinas, y demás Órganos del Hospital, bajo responsabilidad, brinden las facilidades y el apoyo necesario que requiera Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo", para el cumplimiento de sus funciones.

Artículo 4°.- Disponer que, la Jefatura de la Oficina de Estadística e Informática, gestione la aprobación y/o modificación de los documentos normativos que correspondan para el cabal funcionamiento del Equipo de Respuesta ante Incidentes de Seguridad Digital, del Hospital Nacional "Dos de Mayo", creado mediante el artículo primero de la presente resolución.

Artículo 5°.- Disponer que, la Jefatura de la Oficina de Estadística e Informática, haga de conocimiento de la presente resolución a la Secretaría de Gobierno y Transformación Digital, de la Presidencia del Consejo de Ministros.

Artículo 6°.- Disponer que, la Jefatura de la Oficina de Estadística e Informática de la Institución, publique la presente resolución directoral en el portal institucional del Hospital <http://www.hdosdemayo.gob.pe>.

Regístrese, comuníquese y publíquese;



MINISTERIO DE SALUD
HOSPITAL NACIONAL "DOS DE MAYO"
M.C. VICTOR RAFAEL CONZALES PÉREZ
DIRECTOR GENERAL DIRECCIÓN GENERAL
C.M. 27.111. R.N.E. 1977

VRGP/JEVT/amcyd.

- C.c.:
- Dirección General.
 - Órgano de Control Institucional.
 - Dirección Adjunta.
 - Of. Ejecutiva de Planeamiento Estratégico.
 - O. de Estadística e Informática.
 - O. Asesoría Jurídica.
 - Archivo.

