UNIVERSIDAD NACIONAL DE PIURA
SECRETARÍA GENERAL

RESOLUCIÓN RECTORAL N° 367-R-2025
Piura, 12 de mayo de 2025

VISTO

Los Expedientes N° 000081-6201-25-5, del 19.Mar.2025, que presenta la **Dra. Ing. JASSAYRA ARALIZ CHULLE CHAPILLIQUEN,** Jefa de la Oficina de Tecnologías de la Información de la Universidad Nacional de Piura, que contiene el Informe N° 135-OTI-UNP-2025, del 19.Mar.2025, Informe N° 512-2025-OCAJ-UNP, del 09.Abr.2025, Oficio N° 1667-R-2025/UNP, del 10.Abr.2025; y

CONSIDERANDO:

Que, de conformidad con el artículo 18° de la Constitución Política del Perú, prescribe: *"(…) Cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes (…)";*

Que, mediante Ley N° 13531 del 03.Mar.1961, fue creada la Universidad Nacional de Piura, cuya sede está ubicada en el Distrito de Castilla, Departamento de Piura, cuyos fines se encuentran estipulados en el Artículo 8° del Estatuto de la Universidad Nacional de Piura, Aprobado en Sesión Plenaria de Asamblea Estatutaria del 13.Oct.2014 (Ley N° 30220 – Ley Universitaria);

Que, el Artículo 8° de la Ley N° 30220 - Ley Universitaria, prescribe: *"(…) La autonomía inherente a las universidades se ejerce de conformidad con lo establecido en la Constitución, la presente Ley y demás normativa aplicable (…)*"; asimismo, los numerales 8.4 Administrativo, implica la potestad autodeterminativa para establecer los principios, técnicas y prácticas de sistemas de gestión, tendientes a facilitar la consecución de los fines de la institución universitaria, incluyendo la organización y administración del escalafón de su personal docente y administrativo y 8.5 Económico, implica la potestad autodeterminativa para administrar y disponer del patrimonio institucional, así como para fijar el destino de sus recursos propios directamente recaudados, manifiesta los regímenes de su autonomía;

Que, mediante Informe N°135-OTI-UNP-2025, de 19.Mar.2025, la Jefa de la Oficina de Tecnologías de la Información informa, sobre la necesidad de la conformación de un Equipo de Respuesta ante Incidentes de Seguridad Digital de la Universidad Nacional de Piura, en consideración que el CSIRT de la UNP, permitirá la gestión y coordinación ante incidentes de Seguridad Digital en esta Casa Superior de Estudios; recomienda su conformación. de la siguiente manera, cumpliendo los siguientes roles dentro del CSIRT:

N°	CARGO	ROL EN EL CSIRT
1	Jefe de la Oficina de Tecnologías de la Información	Coordinación del CSIRT
2	Oficial de Seguridad de la Información	Gestor de Incidentes

Que, según Informe N° 512-2025-OCAJ-UNP, del 09.Abr.2025, la Abg. Evelyn Maybeline Adrianzén Palacios, Jefa (e) de la Oficina de Asesoría Jurídica, emite opinión legal en los siguientes términos:

"(…)

2.5 Asimismo, dicha Guía establece 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.

5.6 Que, teniendo en consideración los dispositivos legales antes indicados y atendiendo a lo informado por la Jefa de la Oficina de Tecnologías de la Información, quien mediante Informe N°135-OTI-UNP-2025, propone que el Equipo de Respuestas ante Incidentes de Seguridad Digital sea conformado por el Jefe de la Oficina de Tecnologías de la Información como Coordinación del CSIRT y al Oficial de Seguridad de la Información quien asumiría el rol de Gestor de Incidentes; al respecto, este despacho opina por la procedencia de dicha conformación, exhortándose que la disponibilidad de los servicios del CSIRT de la UNP se alinee a las necesidades de la institución.

RECOMENDANDO TEXTUALMENTE:

a) Se declare **PROCEDENTE** que el Equipo de Respuestas ante Incidentes de Seguridad Digital-CSIRT, sea conformado por el/la Jefe(a) de la Oficina de Tecnologías de la Información quien tendría el rol de Coordinación del CSIRT y al Oficial de Seguridad de la Información quien asumiría el rol de Gestor de Incidentes; todo ello, por los argumentos antes expuestos.

b) Se **EMITA** la Resolución correspondiente.

Que, conforme al Oficio N° 1667-R-2025/UNP, del 10.Abr.2025, el Dr. Enrique Ramiro Cáceres Florián, Rector (e) de la Universidad Nacional de Piura, dispone y autoriza a la Secretaria General de la UNP, la emisión de la Resolución Rectoral, que indica; procedente en el Equipo de Respuestas ante Incidentes de Seguridad Digital CSIRT, sea conformado por el/la Jefe (a) de la Oficina de tecnología de la información quien tendría el rol de coordinación del CSIRT y al Oficial de Seguridad de la información quien asumirá el rol de Gestor de incidentes.

Que, el TUO de la Ley del Procedimiento Administrativo General-Ley N° 27444, (aprobado mediante D.S. N°004-2019-JUS), señala en el considerando 1.1 del Artículo IV del título Preliminar; "Principio de Legalidad. - Las autoridades administrativas deben actuar con respecto a la Constitución, la ley y el derecho, dentro de las facultades que le están atribuidas y de acuerdo con los fines para los que le fueron conferidas".

Que, el Decreto de Urgencia Nº 007-2020- Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, establece:

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:
(...)

b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.

(...)

9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

Que, asimismo el Decreto Supremo Nº 029-2021-PCM- Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, establece:

- Artículo 104. Equipo de Respuestas ante Incidentes de Seguridad Digital
  104.1 Un Equipo de Respuestas ante Incidentes de Seguridad Digital es 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.
(...)

- Artículo 105. Obligaciones de las entidades en Seguridad Digital

  Las entidades públicas tienen, como mínimo, las siguientes obligaciones:
  a) Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
  b) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital atendiendo lo establecido en el artículo 107 del presente Reglamento.
  c) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
  d) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad y red de confianza.
  e) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
  f) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
  g) Requerir a sus proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

- Artículo 109. Sistema de Gestión de Seguridad de la Información

  109.1 El Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.
  (...)

Que, la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital, prevé que CSIRT es: "conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación", y dentro de sus beneficios se tendría:

- Disponer de un equipo dedicado a la seguridad digital y ayudar a las organizaciones a mitigar, evitar los incidentes graves y proteger su patrimonio.
- Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad digital dentro de la organización (punto de contacto).
- Reaccionar a los incidentes y tratarlos de un modo centralizado y especializado.
- Garantizar los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad digital.
- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad digital y la mejora continua.

Que, la presente Resolución se suscribe en virtud al Principio de Legalidad, por el cual las autoridades administrativas deben actuar con respeto a la Constitución, la ley y al derecho, dentro de las facultades que le estén atribuidas y de acuerdo con los fines para los que les fueron conferidas; así como al Principio de Buena Fe Procedimental, por el cual la autoridad administrativa, los administrados, sus representantes o abogados y, en general, todos los partícipes del procedimiento, realizan sus respectivos actos procedimentales guiados por el respeto mutuo, la colaboración y la buena fe (...), previstos en el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General aprobado por Decreto Supremo N° 004-2019-JUS;

Que, de conformidad con el artículo 175º inciso 3) del Estatuto de la Universidad Nacional de Piura, que prescribe: *"El Rector es el representante legal de la Universidad y ejerce el gobierno de la misma (...)."* Señalando dentro de sus funciones, *"inciso 3) Dirigir la actividad académica de la Universidad y su gestión administrativa, económica y financiera."*

RESOLUCIÓN RECTORAL N° 367-R-2025
Piura, 12 de mayo de 2025

Que, estando a lo dispuesto por el señor Rector, en uso de sus atribuciones legales conferidas, con visto de la Oficina Central de Asesoría Jurídica y Secretaría General;

SE RESUELVE:

ARTÍCULO 1°.- CONFORMAR, el Equipo de Respuestas ante Incidentes de Seguridad Digital - CSIRT de la Universidad Nacional de Piura, según Informe N° 135-OTI-UNP-2025, del 19.Mar.2025, integrado por:

N°	CARGO	ROL EN EL CSIRT
1	Jefe de la Oficina de Tecnologías de la Información	Coordinación del CSIRT
2	Oficial de Seguridad de la Información	Gestor de Incidentes

ARTÍCULO 2°.- DISPONER, la notificación la presente Resolución a la parte interesada y los órganos competentes de la Universidad Nacional de Piura, para su conocimiento, cumplimiento y demás fines pertinentes.

ARTÍCULO 3°.- DISPONER, la publicación de la presente Resolución en la Plataforma Digital única del Estado Peruano (www.gob.pe) y en "Portal Institucional" (www.unp.edu.pe).

REGÍSTRESE, COMUNÍQUESE Y EJECÚTESE.

c.c. RECTOR (e), VRA, VRI, DGA, OTI,INT (Manuel Requena Saavedra - OTI), ARCHIVO.
07 copias/
VAGV/

Universidad Nacional de Piura
Secretaría General
Abg. Vanessa Arline Girón Viera
SECRETARIA GENERAL

UNIVERSIDAD NACIONAL DE PIURA
DR. ENRIQUE RAMIRO CÁCERES FLOR
RECTOR (e)