RESOLUCION RECTORAL N° 0503-2026

Arequipa, 25 de marzo de 2026.

VISTO el Oficio N° 149-2026-OTI-UNSA de la Oficina de Tecnologías de la Información.

CONSIDERANDO:

Que, la Universidad Nacional de San Agustín de Arequipa está constituida conforme a la Ley Universitaria N° 30220, y se rige por sus respectivos estatutos y reglamentos, siendo una comunidad académica orientada a la investigación y a la docencia, que brinda una formación humanista, ética, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural.

Que, el artículo 8° de la Ley Nº 30220, Ley Universitaria, concordante con el artículo 8° del Estatuto Universitario, referente a la autonomía universitaria establece lo siguiente: *"(...) Esta autonomía se manifiesta en los siguientes regímenes: 8.2. De gobierno, implica lá potestad autodeterminativa para estructurar, organizar y conducir la institución universitaria, con atención a su naturaleza, características y necesidades. Es formalmente dependiente del régimen normativo y 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".*

Que, mediante el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; se estableció en su **artículo 7°** que: *"7.1* ***Créase 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 en su **artículo 9°** que: "***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, de igual forma, mediante el Decreto Supremo N° 029-2021-PCM, se aprobó el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; y se estableció en su **artículo 104°** que: ***"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.* ***104.2 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****. (...)".*

Que, asimismo, mediante Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, se estableció la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas; y en su **artículo 4°,** referido a los responsables en la gestión de la seguridad digital institucional, establece que: ***"4.3 El Comité de Gobierno y Transformación Digital institucional es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI.*** *Asimismo, a solicitud del Titular de la entidad o la máxima autoridad administrativa emite opinión y recomendaciones sobre la gestión estratégica del SGSI. Sin perjuicio de lo indicado la entidad puede solicitar opinión a un órgano consultivo vinculado a la gestión de riesgos de la entidad.*

***4.4 El Oficial de Seguridad y Confianza Digital cumple con lo establecido en la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/ SGTD**, que aprueba la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, así como el marco normativo en materia de seguridad y confianza digital. **4.5 El Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional es responsable de la gestión de incidentes de seguridad digital que afectan los activos de la entidad pública.** Dicho Equipo forma 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. (…)".*

Que, la **Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital** (Enero 2024)[1], publicada por el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, señala en su **punto 4.1.4** 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 (...) b. Gestor de Incidentes (...) c. Gestor de Redes y Comunicaciones (...) d. Gestor de Infraestructuras Digitales (...) e. Oficial de Seguridad y Confianza Digital (...) f. Otros roles que determine la institución**".*

Que, al respecto, se verifica que el Reglamento de Organización y Funciones (ROF) de la UNSA, señala en su **artículo 97°**, que la **Unidad de Sistemas de Información, Redes y Telecomunicaciones:** *"Es la unidad orgánica de apoyo dependiente de la Oficina de Tecnologías de la Información, responsable de proponer, desarrollar, producir y uniformizar sistemas de informática en el ámbito de la gestión administrativa y académica para la UNSA" y en su **artículo 98°,** señala que, entre sus funciones tiene: "98.1 Automatizar y digitalizar procesos que faciliten el uso de servicios universitarios a los estudiantes, docentes y administrativos de la UNSA. **98.2 Desarrollar actividades de control de acceso y seguridad a la información de la UNSA, garantizando su incorruptibilidad y disponibilidad en forma permanente** (…)".*

Que, asimismo, mediante Resolución Rectoral N° 1244-2025 del 06 de noviembre de 2025, se resolvió: *"**1. DESIGNAR al MAG. LUIS RENAN FELIPE PICCONE DIAZ, en su condición de Jefe de la Unidad de Sistemas de Información, Redes y Telecomunicaciones de la Oficina de Tecnologías de la Información, como OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL (OSCD) de la Universidad Nacional de San Agustín**; de conformidad con lo establecido en la Directiva N° 001-2023-PCM/ SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, y en adición a sus funciones. (…)".*

Que, en ese contexto, mediante **Informe N° 001-2026-CGTD-UNSA-C/JBZS, el Coordinador del Comité de Gobierno y Transformación Digital**, previo análisis de la normativa vigente, concluyó entre otros, que: *"**2. Corresponde conformar con urgencia, un Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT)**, de acuerdo con la normativa vigente. Para dichos efectos, la Oficina de Tecnologías de la Información deberá identificar los servidores aptos para integrar dicho equipo y los roles a cubrir, tomando en cuenta la "Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital", **3. De acuerdo con el ROF de la UNSA, corresponde que la Unidad de Sistemas de Información, Redes y Telecomunicaciones, emita el informe técnico respectivo**, señalando los servidores y roles a considerar en la conformación del CSIRT; y brindado el sustento técnico necesario para solicitar la autorización del Rectorado y que formalice la conformación del CSIRT, a través de la resolución respectiva. **4. Corresponde que la Oficina de Tecnologías de la Información, previa validación de lo informado por la Unidad de Sistemas de Información,***

[1] https://www.gob.pe/institucion/pcm/informes-publicaciones/5057847-guia-para-la-conformacion-e-implementacion-del-equipo-de-respuestas-ante-incidentes-de-seguridad-digital

R.R. Nº 0503-2026 *25/03/2026*

Redes y Telecomunicaciones, solicite al Rectorado, la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) de la UNSA, a través de la resolución respectiva".

Que, asimismo, conforme al **artículo 104.3** del Decreto Supremo N° 029-2021-PCM, que aprobó el Reglamento del Decreto Legislativo Nº 1412, Ley de Gobierno Digital: *"(…)* ***104.3 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";* conviene precisar, que según los actuados obrantes en el expediente; se cuenta con los registros y actas de dos (02) reuniones de coordinación realizadas con el Analista en Gestión de Incidentes de Seguridad Digital, Julio C. Soto Sairitupac, en las cuales **se recibió la asistencia técnica por parte de la Subsecretaría de Tecnologías y Seguridad Digital del Centro Nacional de Seguridad Digital de la Presidencia del Consejo de Ministros, para la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA – CSIRT UNSA.**

Que, bajo ese contexto, es que mediante Informe N° 018-2026-USIRT/OTI-UNSA, el Jefe de la Unidad de Sistemas de Información, Redes y Telecomunicaciones de la Oficina de Tecnologías de la Información y Oficial de Seguridad y Confianza Digital (OSCD) de la Universidad Nacional de San Agustín de Arequipa, remitió su propuesta de conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA - CSIRT UNSA.

Que, en consecuencia, mediante el documento del visto, dicha propuesta fue validada por parte de la Oficina de Tecnologías de la Información, y elevada al Rectorado, solicitando que se emita la resolución respectiva, formalizando la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA - CSIRT UNAS; a fin de dar cumplimiento a la normativa vigente.

Que, de conformidad con los dispositivos legales mencionados y en uso de las atribuciones que la Ley Universitaria y el Estatuto conceden al Rectorado,

SE RESUELVE:

1. **CONFORMAR** el **Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA - CSIRT UNSA** conforme al siguiente detalle:

N°	Cargo	Rol en el CSIRT
1	Jefatura de la Oficina de Tecnologías de la Información	Coordinador del CSIRT
2	Jefatura de la Unidad de Sistemas de Información, Redes y Telecomunicaciones	Oficial de Seguridad y Confianza Digital
3	Responsable de la Unidad de Infraestructura Tecnológica y Soporte Técnico	Gestor de Infraestructuras Digitales
4	Personal de la Oficina de Tecnologías de la Información	Gestor de incidentes
5	Personal de la Unidad de Sistemas de Información, Redes y Telecomunicaciones	Gestor de Redes y Comunicaciones
6	Coordinador de Gobierno y Transformación Digital	Miembro de Apoyo Estratégico

2. **PRECISAR** que el **Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA - CSIRT UNSA** tiene las siguientes funciones:

   a. Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital detectados.
   b. Adoptar las medidas necesarias para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la Universidad.

c. Difundir alertas tempranas, avisos e información preventiva sobre riesgos, incidentes y amenazas de seguridad digital en la Universidad.
d. Coordinar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
e. Supervisar el cumplimiento de normas, estándares y mejores prácticas de seguridad digital por parte de los proveedores de software y servicios.
f. 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.
g. Revisar y actualizar las medidas de seguridad de redes y sistemas para identificar y corregir vulnerabilidades.
h. Otras que determine la Alta Dirección o el ente rector de la Secretaría de Gobierno y Transformación Digital.

3. **AUTORIZAR** al **Jefe de la Oficina de Tecnologías de la Información,** para que en su condición de Coordinador del Equipo de Respuestas ante Incidentes de Seguridad Digital de la UNSA - CSIRT UNSA; cumpla con **informar** en el plazo máximo de 05 días hábiles de notificado, sobre el personal que haya designado para que integre el CSIRT-UNSA, en adición a sus funciones.

4. **REMITIR** la presente resolución a la **SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL** de la Presidencia del Consejo de Ministros, para su conocimiento y fines pertinentes.

5. **ENCARGAR** al **Jefe de la Oficina de Tecnologías de la Información**, Funcionario Responsable de la Elaboración y Actualización del Portal de Transparencia, la **publicación** de la presente Resolución y el Reglamento, en el Portal Institucional; **EN COORDINACIÓN** con la **Jefa de la Oficina de Comunicaciones e Imagen Institucional**, para la **difusión** de una pieza gráfica que sintetice la presente resolución, y la ponga en conocimiento de la comunidad universitaria, a través los canales digitales de la Universidad.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

DRA. RUTH MARITZA CHIRINOS LAZO
SECRETARIA GENERAL

DR. HUGO JOSE ROJAS FLORES
RECTOR

C.C. CGTD, OTI, OTI-USIRT, OPPM y ARCHIVO.
Exp. 1011715-2026
/jbzs