UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

SECRETARÍA GENERAL

RESOLUCION Nº R- 245 -2025-UNSAAC

Cusco, 27 FEB 2025

EL RECTOR DE LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO,

VISTO, el Oficio Nº 003-2025-OTI-UNSAAC, registrado con Expediente N°. 811495, presentado por el **Dr. DARIO FRANCISCO DUEÑAS BUSTINZA**, Jefe de la Oficina de Tecnología de la Información, solicitando conformación del Equipo de Respuestas ante incidentes de Seguridad Digital (COMPUTER SECURITY RESPONSE TEAM – CSIRT-UNSAAC, y;

CONSIDERANDO:

Que, el artículo 8 de la Ley N°. 30220, Ley Universitaria y el artículo 7 del Estatuto Universitario de la UNSAAC, señalan que el Estado reconoce la autonomía universitaria, la misma que es inherente a las Universidades y se ejerce de conformidad con los establecido en la Constitución Política del Perú, Ley Universitaria y las demás normas aplicables;

Que, mediante Decreto Supremo N°. 085-2023-PCM, se aprueba la Política Nacional de Transformación Digital, como ente rector del Sistema Nacional de Transformación Digital al 2030, el cual se debe aplicar a todas las entidades de la administración pública señaladas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N°. 27444, Ley del Procedimiento General aprobado por Decreto Supremo N°. 004-2019-JUS;

Que, la Presidencia del Consejo de Ministros, a través de la Secretaria de Gobierno y Transformación Digital, como ente rector del Sistema Nacional de Transformación Digital, conduce la Política Nacional de Transformación Digital al 2030, solicita a las entidades determinar los lineamientos, objetivos, estándares, acciones, servicios, indicadores, actividades, metas y responsables para poder alcanzar la transformación digital tanto de la entidad y se llegue a la transformación digital del país;

Que, el Decreto de Urgencia N.° 007-2020 aprobó el Marco de Confianza Digital y dispuso medidas para su fortalecimiento, que tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por las entidades públicas y organizaciones del sector privado en el territorio nacional;

El literal e) del artículo 3.° del Decreto de Urgencia N.° 007-2020 define al incidente de seguridad digital como el evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales; asimismo, el literal f) del referido artículo, establece que la gestión de incidentes de seguridad digital es el proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como, la recuperación y determinación de acciones correctivas para prevenir incidentes similares;

Que, el numeral 9.3 del artículo 9.° del Decreto de Urgencia N.° 007-2020, dispone que las entidades de la administración pública deben implementar, entre otros, un Equipo de Respuestas ante Incidentes de Seguridad Digital – CSIRT (Computer Security Incident Response Team) cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

Que, el numeral 104.1 del artículo 104° del Reglamento del Decreto Legislativo N.° 1412, aprobado mediante Decreto Supremo N.° 029-2021-PCM, señala que, el Equipo de Respuestas ante Incidentes de Seguridad Digital es el 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 en las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros. Asimismo, el numeral 104.2 establece que las entidades de la administración pública conforman un Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional, los cuales 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, siendo comunicada su conformación a la Secretaría de Gobierno Digital mediante los mecanismos dispuesto para tal fin;

De acuerdo con la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad, elaborada por el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno Digital, creado de conformidad con el artículo 7° del Decreto de Urgencia N.° 007-2020, establece, entre otros, las funciones que deben desarrollar los equipos, las responsabilidades, así como, los roles básicos de los integrantes mínimos del equipo conformado. Asimismo, describe la misión, funciones y objetivos que debe cumplir el equipo técnico por conformarse. El numeral 4.1.12 de la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad establece que: "(...) El apoyo al CSIRT debe provenir de los más altos niveles gerenciales de la institución (...) La aprobación de la creación del equipo CSIRT se realiza mediante la emisión de una resolución de conformación de equipo de respuestas ante incidentes de seguridad digital o la tercerización de este (...)";

De acuerdo con la Cuadragésima Octava Disposición Complementaria Final del Reglamento del Decreto Legislativo N.° 1412, se establece que las entidades de la Administración Pública conforman sus equipos de Respuestas ante Incidentes de Seguridad Digital.

Que, mediante documento de Visto, el Jefe de la Oficina de Tecnología de la Información de la Institución, en su condición de responsable de la conformación del equipo CSIRT, solicita se emita Resolución Rectoral aprobando la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital CSIRT – UNSAAC (Computer Security Incident Response Team/Equipo de respuesta a incidentes de seguridad informáticos) – UNSAAC, aclarando que dicha conformación es considerada como fase inicial y que estratégicamente, agrupará más profesionales según crecimiento digital de la UNSAAC acorde al Gobierno Digital;

Que, los principales servicios fundamentales que el equipo CSIRT de la UNSAAC ofrecerá, serán por etapas y están enmarcadas en las siguientes áreas: Gestión de eventos de seguridad de la información; Gestión de Incidentes de Seguridad de la Información; Gestión de Vulnerabilidades, Conciencias Situacional y Transferencia de Conocimiento, cuyo detalle es anexo de la presente Resolución;

Que, mediante Oficio N°. 0308-2025-URH/DIGA-UNSAAC, la jefe de la Unidad de Recursos Humanos, emite el Informe Escalafonario N°. 583-2025-SUEP-URH-DIGA/UNSAAC (VIRTUAL) emitido por la Sub Unidad de Escalafon y Pensiones e Informe N°. 0203-2025-SUSE/URH emitido por la Sub Unidad de Selección y Evaluacion, documentos que obran en el expediente;

Que, la Autoridad Universitaria ha tomado conocimiento de la petición del Jefe de la Oficina de Tecnología de la Información y ha dispuesto la emisión de la Resolución correspondiente;

Estando a lo referido, Decreto Supremo N°. 085-2023-PCM, Decreto de Urgencia N.° 007-2020, Reglamento del Decreto Legislativo N.° 1412, aprobado mediante Decreto Supremo N.° 029-

2021-PCM y en uso a las atribuciones conferidas a este Rectorado por Ley 30220 y el Estatuto Universitario;

RESUELVE:

PRIMERO.- CONFORMAR el Equipo de Respuestas ante Incidentes de Seguridad Digital de la Universidad Nacional de San Antonio Abad del Cusco (CSIRT UNSAAC) de naturaleza permanente, como responsable de gestionar los eventos e incidentes de la seguridad digital cuyo objetivo principal es coordinar las acciones necesarias p ara la protección de los activos de información frente a amenazas que atenten o comprometan la seguridad digital, el cual está integrado por los siguientes miembros:

1. **DR. DARÍO FRANCISCO DUEÑAS BUSTINZA**
   JEFE DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN o quien haga sus veces, en el rol de **Coordinador Del CSIRT-UNSAAC (***Persona que gestionará todas las actividades de gestión del CSRIT – UNSAAC, y es el punto de contacto con el CSRIT Nacional del Centro Nacional de Seguridad Digital***).**

2. **ING. AGUEDO HUAMANI HUAYHUA**
   JEFE DE LA UNIDAD DEL CENTRO DE COMPUTO, en el rol de **Gestor de Infraestructuras Digitales (***Será el responsable de la seguridad de los servidores e infraestructuras de nube, determina las reglas de seguridad a nivel del sistema operativo y aplicaciones***).**

3. **ING. BENJAMIN ESPEJO ALVAREZ**
   JEFE DE LA UNIDAD DE RED DE COMUNICACIONES o quien haga sus veces, en el rol de **Gestor de Redes y Comunicaciones y Gestor de Infraestructuras Digitales (***Responsable de la seguridad de la red de comunicaciones de la Universidad Nacional de San Antonio Abad del Cusco, el cual deberá implementar medidas de cifrado para la protección de la confidencialidad de las comunicaciones, así mismo deberá coordinar con todo el equipo el modelo de monitorización de las mismas***).**

4. **ING. LIZY VANNY PINTO PAZ**
   ESPECIALISTA Y REPRESENTANTE DE LA OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN o quien haga sus veces, en el rol de **Gestor de Incidentes (***Responsable de la gestión de los incidentes de seguridad digital, así como también de la comunicación del incidente al Centro Nacional de Seguridad Digital***).**

5. **BR. JOHANN MERCADO LEON**
   ESPECIALISTA EN TELECOMUNICACIONES DE LA UNIDAD DE RED DE COMUNICACIONES o quien haga sus veces, en el rol de **Miembro Del CSRIT-UNSAAC (***Miembro del CSRIT 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***).**

SEGUNDO.- El Equipo de Respuestas ante incidentes de Seguridad Digital de la Universidad Nacional de San Antonio Abad del Cusco, conformado en el primer numeral de la presente Resolución, tiene la siguientes funciones:

a) Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.

b) Se adoptará medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la UNSAAC.
c) Se deberá difundir alertas tempranas sobre riesgos e incidentes de seguridad digital en la UNSAAC, por medio de avisos e información.
d) Se deberá coordinar y asegurar acciones de investigación y cooperación efectiva, eficiente y segura en estrecha coordinación con el Centro Nacional de Seguridad Digital.
e) Coordinar continuamente con la Autoridad universitaria, así como los diferentes funcionarios de la UNSAAC, para que puedan proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
f) Coordinar constantemente con el equipo de desarrollo de software, app y otros, el cumplimiento de estándares normas técnicas y mejores prácticas de seguridad.
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) Contar con una buena relación con las diferentes unidades, áreas, recursos humanos, lo cual ayudara a resolver los incidentes o consultas sobre posibles acciones a tomar.
i) Otras que determine la Oficina de Tecnologías de la Información de la UNSAAC.

TERCERO.- DEJAR ESTABLECIDO que los principales servicios fundamentales que el equipo CSIRT de la UNSAAC ofrecerá, serán por etapas y están enmarcadas en las siguientes áreas: Gestión de eventos de seguridad de la información; Gestión de Incidentes de Seguridad de la Información; Gestión de Vulnerabilidades, Conciencias Situacional y Transferencia de Conocimiento, cuyo detalle es anexo de la presente Resolución.

CUARTO.- DISPONER que la Unidad de Trámite Documentario de la UNSAAC, notifique con la presente resolución a las instancias y dependencias administrativas y académicas de la Universidad Nacional de San Antonio Abad del Cusco, así como a los miembros integrantes del Equipo de Respuestas ante Incidentes de Seguridad Digital de la Universidad Nacional de San Antonio Abad del Cusco (CSIRT – UNSAAC).

QUINTO.- DISPONER la publicación de la presente Resolución Rectoral en el Portal Institucional de la Universidad Nacional de San Antonio Abad del Cusco https://www.unsaac.edu.pe/ y su comunicación a la Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

REGISTRESE, COMUNIQUESE Y ARCHIVESE.

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
RECTORADO
DR. ELEAZAR CRUCINTA UGARTE
RECTOR

TR. VRAC.-VRIN.- OCI.- OFICINA DE PLANEAMIENTO Y PRESUPUESTO- UNIDAD DE PLANEAMIENTO Y PRESUPUESTO.- DIGA.- U FINANZAS.-U. ABASTECIMIENTO.- U RECURSOS HUMANOS-S. EMPLEO.-S ESCALAFÓN Y PENSIONES (02).- SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL (SGTD).- PCM.- OFICINA DE TECNOLOGIA DE LA INFORMACION.- UNIDAD DE CENTRO DE COMPUTO.- OF COMUNICACIÓN E IMAGEN INSTITUCIONAL.- U RED DE COMUNICACIONES.- ARCHIVO CENTRAL.- ARCHIVO.-SG: ECU/MMVZ/MQL.

Lo que transcribo a Ud., para su conocimiento y fines consiguientes.
Atentamente.

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
SECRETARÍA GENERAL
ABOG. M. MYLUSKA VILLAGARCIA ZERECEDA
SECRETARIA GENERAL (e)

SERVICIOS FUNDAMENTALES

Los principales servicios fundamentales que el equipo CSIRT de la UNSAAC ofrecerá, serán por etapas, el cual subirá de nivel a través de la madurez del equipo (Conocimientos, Experiencia, Capacitaciones constantes, Actualización de información, entre otros)

AREAS DE SERVICIO				
GESTIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE VULNERABILIDADES	CONCIENCIA SITUACIONAL	TRANSFERENCIA DE CONOCIMIENTO
Monitoreo y detección • Gestión de registros • Gestión de casos de uso de detección • Gestión de datos contextuales **Análisis de Eventos** • Correlación • Calificación	**Aceptación del informe de incidentes de seguridad de la información** • Recepción de informes de incidentes de seguridad de la información **Análisis de incidentes de seguridad de la información** • Recopilación de información • Coordinación de análisis detallado • Análisis de causa raíz de incidentes de seguridad de la información • Correlación entre los incidentes **Mitigación y recuperación** • Establecimiento del plan de respuesta. • Restauración del sistema **Coordinación de incidentes de seguridad de la información** • Comunicación • Distribución de información • Coordinación de actividades **Apoyo a la gestión de crisis** • Informe del estado de seguridad de la información • Comunicación de decisiones estratégicas	**Descubrimiento/Investigación de vulnerabilidades** • Descubrimiento de vulnerabilidades de respuesta a incidentes • Investigación de vulnerabilidades **Reporte de Vulnerabilidades** • Recepción de informe de vulnerabilidades • Clasificación y procesamiento de los informes de vulnerabilidad. **Análisis de vulnerabilidad** • Categorización de las vulnerabilidades identificadas • Análisis de la causa raíz de la vulnerabilidad • Desarrollo de remediación de vulnerabilidades **Coordinación de vulnerabilidad** • Informe de Vulnerabilidad • Coordinación de actores de vulnerabilidad **Divulgación de vulnerabilidad** • Política de divulgación de vulnerabilidades y mantenimiento de infraestructura **Respuesta de vulnerabilidad** • Detección/ escaneo de vulnerabilidades • Reparación de vulnerabilidades	**Adquisición de datos** • Asignación de activos a funciones, roles, acciones y riesgos clave. • Procesamiento y preparación de datos. **Análisis y síntesis** • Detección de eventos (a través de alertas y/o búsqueda) • Soporte de decisiones de gestión de incidentes de seguridad de la información • Impacto situacional **Comunicación** • Comunicación interna y externa • Informes y recomendaciones • Implementación • Gestión del intercambio de información • Realimentación	**Sensibilización** • Investigación de la información • Elaboración de informes y materiales de sensibilización • Difusión de información **Formación y educación** • Recopilación de requisitos de conocimientos, habilidades y capacidades. • Temas y desarrollo de capacitaciones. • Desarrollo profesional constante del personal del CSIRT-UNSAAC **Asesoramiento técnico y normativo** • Apoyo a la gestión de riesgos • Apoyo a la planificación de la continuidad del negocio y la recuperación ante desastres • Apoyo a las Políticas de seguridad • Asesoramiento técnico

Aprobado por Resolución R.
N° 245-2025-UNSAAC