Universidad Nacional de Cajamarca

"NORTE DE LA UNIVERSIDAD PERUANA"

Fundada por Ley N°14015, del 13 de Febrero de 1962

CAJAMARCA – PERÚ

---- o ----

Resolución de Consejo Universitario n.°3377-2025-UNC
Cajamarca, 18 de agosto de 2025

Vistos, el Oficio n.°729-2025-DEPG-UNC, de fecha 12 de junio de 2025, suscrito por la Dra. Leticia N. Zavaleta Gonzales, Directora de la Escuela de Posgrado de la Universidad Nacional de Cajamarca, **contenido en el Expediente Administrativo n.°0084176-2025-UNC,** los acuerdos tomados en Sesión Ordinaria de Consejo Universitario de fecha 18 de agosto de 2025; y,

CONSIDERANDO:

Que, conforme al artículo 18 de la Constitución Política del Perú, la Universidad Pública es una entidad de Derecho Público, que goza de autonomía gubernativa, normativa, académica, administrativa y económica;

Que, la autonomía universitaria se ejerce de conformidad con lo establecido en la Constitución, la Ley Universitaria, el Estatuto y las demás normas jurídicas vigentes (artículo 8 de la Ley N° 30220, Ley Universitaria);

Que, conforme a lo sostenido por el Tribunal Constitucional (Exp. N°00037-2009-PI), en lo referente a la autonomía universitaria, puede ser entendida *"como la facultad de autorregulación que tienen todas las universidades ya sea en el ámbito* ***normativo, de gobierno, académico, administrativo y económico, destacando además que dicha autorregulación no implica autonomía absoluta, sino relativa pues su ejercicio debe ser compatibilizado con otros bienes constitucionales****"*;

Que, el numeral 22 del artículo 27 del Estatuto de la Universidad Nacional de Cajamarca, señala que es una de las atribuciones de Consejo Universitario el de: *"Ratificar los reglamentos internos de las Facultades y de la Escuela de Posgrado, a propuesta de sus respectivos Consejos"*;

Que, el artículo 164 del Estatuto de la Universidad Nacional de Cajamarca, establece que la finalidad de la Escuela de Posgrado es: *"la formación de académicos e investigadores, con competencias humanísticas, científicas, tecnológicas e investigativas."*;

Que, asimismo, el artículo 194 del mismo cuerpo normativo legal citado, *supra*, señala en el inciso 8 que, es una de las atribuciones de Coordinación del Consejo de Coordinación de Escuela la de *"Planificar, organizar y ejecutar, en coordinación con las Unidades de Posgrado, las actividades de la Escuela de Posgrado"*;

Que, en ese sentido, con Oficio n.°729-2025-DEPG-UNC, de fecha 12 de junio de 2025, la Dra. Leticia N. Zavaleta Gonzales, Directora de la Escuela de Posgrado de la Universidad Nacional de Cajamarca, remite la Resolución de Sesión Extraordinaria de Consejo de Coordinación de Escuela de Posgrado n.°920-2025-EPG-UNC, de fecha 10 de junio de 2025, mediante la cual, se resuelve: *"ARTICULO PRIMERO. – APROBAR, la Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca"*;

Que, la Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca, tiene como finalidad garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos de la Escuela de Posgrado de la Universidad Nacional de Cajamarca (UNC), en el marco de sus programas de Diplomados, Maestría y Doctorado. Reconociendo el creciente impacto de las tecnologías de la información en el entorno académico presencial y no presencial, esta directiva busca proteger los activos de información contra amenazas internas y externas, asegurando un ambiente digital seguro para estudiantes, docentes y personal administrativo;

Que, con fecha 18 de agosto de 2025, se convocó a Sesión Ordinaria de Consejo Universitario, según lo regulado en el artículo 28 del Estatuto de la Universidad Nacional de Cajamarca, oportunidad en la que se trató en la documentación mencionada en los considerandos anteriores;

Resolución de Consejo Universitario n.°3377-2025-UNC
Cajamarca, 18 de agosto de 2025

Que, en dicha sesión, luego de la exposición, análisis y discusión de la propuesta planteada por la Dra. Leticia Noemí Zavaleta Gonzales, Directora de la Escuela de Posgrado de esta Casa Superior de Estudios, los miembros del Consejo Universitario de la Universidad Nacional de Cajamarca, por unanimidad, acordaron: a) **RATIFICAR**, la Resolución de Sesión Extraordinaria de Consejo de Coordinación de Escuela de Posgrado n.°920-2025-EPG-UNC, de fecha 10 de junio de 2025, expedida por las autoridades de la Escuela de Posgrado de la Universidad Nacional de Cajamarca; b) APROBAR, la Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca;

Estando a lo expuesto, y, en uso de las atribuciones conferidas por los artículos 59, 62 y 73 de la Ley Universitaria N°30220, y el artículo 27 y 289 del Estatuto de la Universidad Nacional de Cajamarca;

SE RESUELVE:

ARTÍCULO PRIMERO. – RATIFICAR, la Resolución de Sesión Extraordinaria de Consejo de Coordinación de Escuela de Posgrado n.°920-2025-EPG-UNC, de fecha 10 de junio de 2025, expedida por las autoridades de la Escuela de Posgrado de la Universidad Nacional de Cajamarca.

ARTÍCULO SEGUNDO. –APROBAR la **DIRECTIVA PARA LA SEGURIDAD INFORMÁTICA DE LA ESCUELA DE POSGRADO DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA**, que como anexo adjunto, forma parte integrante de la presente resolución.

ARTÍCULO TERCERO. – PUBLICAR, la presente Resolución en el portal web de la Universidad Nacional de Cajamarca, www.unc.edu.pe.

ARTÍCULO CUARTO. – HACER CONOCER, la presente Resolución al Rectorado, Oficina de Tecnología de la Información y Escuela de Posgrado, para los fines pertinentes.

Regístrese, comuníquese y archívese.

DOCUMENTO FIRMADO DIGITALMENTE
POR **SEGUNDO BERARDO ESCALANTE ZUMAETA**
RECTOR
UNIVERSIDAD NACIONAL DE CAJAMARCA

DOCUMENTO FIRMADO DIGITALMENTE
POR **DELIA ESPERANZA BARRANTES MEDINA**
SECRETARÍA GENERAL
UNIVERSIDAD NACIONAL DE CAJAMARCA

Firmado digitalmente por:
ESCALANTE ZUMAETA Segundo
Berardo FAU 20148258601 hard
Motivo: Soy el autor del
documento
Fecha: 26/08/2025 08:59:11-0500

Firmado digitalmente por:
BARRANTES MEDINA Delia
Esperanza FAU 20148258601 ha
Motivo: Doy fe
Fecha: 25/08/2025 15:01:25-050

UNIVERSIDAD NACIONAL DE CAJAMARCA

ESCUELA DE POSGRADO

DIRECTIVA PARA LA SEGURIDAD INFORMÁTICA DE LA ESCUELA DE POSGRADO DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA

Cajamarca-Perú, mayo de 2025.

Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca

Artículo 1. Finalidad

La presente Directiva establece los principios, normas y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos de la Escuela de Posgrado de la Universidad Nacional de Cajamarca (UNC), en el marco de sus programas de Diplomados, Maestría y Doctorado. Reconociendo el creciente impacto de las tecnologías de la información en el entorno académico presencial y no presencial, esta directiva busca proteger los activos de información contra amenazas internas y externas, asegurando un ambiente digital seguro para estudiantes, docentes y personal administrativo.

Artículo 2. Objetivos

a. Proteger la confidencialidad de la información sensible y personal de estudiantes, egresados, docentes y personal administrativo.
b. Asegurar la integridad de los datos y sistemas, previniendo alteraciones no autorizadas o accidentales.
c. Garantizar la disponibilidad de los sistemas informáticos y la información para el desarrollo de las actividades académicas y administrativas.
d. Establecer un marco de responsabilidades claras en materia de seguridad informática.
e. Promover una cultura de seguridad de la información y buenas prácticas entre todos los usuarios.
f. Cumplir con la normativa legal vigente en materia de seguridad de la información y protección de datos.

Artículo 3. Base Legal

La presente Directiva se sustenta en la siguiente normativa:

a. Ley N° 30220, Ley Universitaria.
b. Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento (Decreto Supremo N° 003-2013-JUS).
c. Ley N° 30096, Ley de Delitos Informáticos, y su Reglamento (Decreto Supremo N° 009-2017-JUS).
d. Estatuto de la Universidad Nacional de Cajamarca.
e. Normas Técnicas Peruanas (NTP) y estándares internacionales relacionados con la seguridad de la información (ISO/IEC 27001).
f. Reglamento de la Escuela de Posgrado de la UNC.

UNIVERSIDAD NACIONAL DE CAJAMARCA Escuela de Posgrado DIRECCIÓN

Artículo 4. Alcance

Esta Directiva aplica al Consejo de Coordinación, unidades académicas y administrativas, asesores, miembros de comités científicos, docentes y estudiantes de la Escuela de Posgrado, así como sistemas informáticos, redes, equipos, software, datos y servicios de información que sean propiedad o estén bajo la administración de la Escuela de Posgrado de la UNC, así como a aquellos utilizados para fines académicos o administrativos relacionados con sus programas de Diplomados, Maestría y Doctorado.

Artículo 5. Principios de Seguridad Informática

El tratamiento y gestión de la información en la Escuela de Posgrado se rige por los siguientes principios:

a. **Confidencialidad:** La información no debe ser revelada a individuos, entidades o procesos no autorizados.
b. **Integridad:** La información debe ser completa, exacta y protegida contra modificaciones no autorizadas o accidentales.
c. **Disponibilidad:** La información y los sistemas informáticos deben ser accesibles y utilizables por los usuarios autorizados cuando sea necesario.
d. **Autenticidad:** Asegurar la veracidad y el origen de la información y la identidad de los usuarios.
e. **No Repudio:** Garantizar que las partes involucradas en una comunicación o transacción no puedan negar su participación.
f. **Legalidad:** Todas las actividades de seguridad informática deben cumplir con la normativa legal vigente.
g. **Conciencia:** Todos los usuarios deben ser conscientes de sus responsabilidades en materia de seguridad informática.
h. **Mejora Continua:** Los procesos y medidas de seguridad deben ser revisados y mejorados constantemente.

Artículo 6. Políticas de Seguridad Informática

6.1. **Gestión de Cuentas y Contraseñas:**

a. Los usuarios son responsables de la confidencialidad de sus credenciales de acceso.
b. Las contraseñas deben ser robustas, cambiadas periódicamente y no compartidas.
c. Se implementarán políticas de bloqueo de cuentas por intentos fallidos de acceso.

6.2. **Control de Acceso:**

a. El acceso a los sistemas y la información se otorgará basándose en el principio de "necesidad de conocer" y "privilegio mínimo".
b. Los permisos de acceso serán revisados periódicamente y revocados cuando ya no sean necesarios.

6.3. **Uso Aceptable de Recursos Informáticos:**

a. Los recursos informáticos de la Escuela de Posgrado deben ser utilizados principalmente para fines académicos y administrativos.
b. Se prohíbe el uso de los recursos para actividades ilegales, no éticas o que comprometan la seguridad.

6.4. **Protección contra Malware:**

a. Todos los equipos conectados a la red de la Escuela de Posgrado deben contar con software antivirus y antimalware actualizado.
b. Se prohíbe la instalación de software no autorizado o de origen dudoso.

6.5. **Copia de Seguridad y Recuperación de Desastres:**

a. Se establecerán procedimientos para la realización periódica de copias de seguridad de la información crítica.
b. Se desarrollarán planes de recuperación de desastres para asegurar la continuidad de las operaciones ante incidentes mayores.

6.6. **Seguridad de la Información en Tránsito:**

a. Se utilizarán protocolos de comunicación seguros para la transmisión de información sensible.

6.7. **Seguridad de Equipos y Dispositivos:**

a. Los equipos y dispositivos de la Escuela de Posgrado deben ser protegidos físicamente contra robo o acceso no autorizado.
b. Se recomienda el uso de cifrado para dispositivos portátiles que almacenen información sensible.

6.8. **Gestión de Incidentes de Seguridad:**

a. Se establecerá un procedimiento para la detección, reporte, análisis y respuesta a incidentes de seguridad informática.
b. Todo incidente de seguridad debe ser reportado a la instancia responsable de manera inmediata.

Artículo 7. Responsabilidades

a. **Escuela de Posgrado:** Responsable de la ejecución y supervisión de la Directiva, así como de la asignación de recursos para su implementación.

b. **Oficina General de Tecnologías de Información (OTI) de la UNC:** Responsable de la implementación técnica y el mantenimiento de las medidas de seguridad, la gestión de la infraestructura tecnológica, la respuesta a incidentes de seguridad y la capacitación técnica.
c. **Secretaría Académica y Unidades Administrativas.** Responsables de aplicar las políticas de seguridad en sus procesos diarios, gestionar los accesos a la información bajo su custodia y asegurar la confidencialidad de los datos que manejan.
d. **Docentes.** Responsables de proteger la información académica y personal a su cargo, educar a los estudiantes sobre buenas prácticas de seguridad y reportar cualquier vulnerabilidad o incidente.
e. **Asesores y miembros de Comités Científicos.** Responsables de verificar el cumplimiento de la presente Directiva en las tesis y trabajos de investigación.
f. **Estudiantes.** Responsables de cumplir con todas las políticas de seguridad, proteger sus credenciales de acceso, utilizar los recursos informáticos de manera responsable y reportar cualquier actividad sospechosa.

Artículo 8. Medidas de Seguridad Específicas

a. **Autenticación Fuerte:** Implementación de autenticación de dos factores (2FA) para el acceso a sistemas críticos.
b. **Segmentación de Redes:** Separación lógica de las redes para limitar el impacto de posibles ataques.
c. **Auditorías de Seguridad:** Realización periódica de auditorías internas y externas para identificar vulnerabilidades y evaluar la efectividad de las medidas de seguridad.
d. **Gestión de Vulnerabilidades:** Proceso sistemático para identificar, evaluar y remediar vulnerabilidades en sistemas y aplicaciones.
e. **Concientización y Capacitación:** Programas continuos de concientización y capacitación en seguridad informática para todos los usuarios.
f. **Monitoreo de Eventos:** Implementación de herramientas para el monitoreo y registro de eventos de seguridad en los sistemas y redes.

Artículo 9. Gestión de Incidentes de Seguridad Informática

a. **Detección:** Los usuarios y los sistemas de monitoreo deben estar atentos a cualquier indicio de un incidente de seguridad.
b. **Reporte:** Cualquier incidente o sospecha debe ser reportado inmediatamente a la OTI o a la instancia designada.
c. **Análisis y Contención:** La OTI analizará el incidente para determinar su alcance, causa e impacto, y tomará medidas para contenerlo y mitigar sus efectos.

UNIVERSIDAD NACIONAL DE CAJAMARCA
Escuela de Posgrado
DIRECCIÓN

d. **Erradicación y Recuperación:** Se eliminará la causa raíz del incidente y se restaurarán los sistemas y datos afectados.

e. **Post-Incidente:** Se realizará un análisis post-incidente para identificar lecciones aprendidas y mejorar las políticas y procedimientos de seguridad.

f. **Notificación:** Se notificará a los afectados y a las autoridades competentes si el incidente implica una violación de datos personales, según lo exige las normativas estatales.

Artículo 10. Revisión y Actualización

La presente Directiva será revisada y actualizada periódicamente, al menos cada dos años, o cuando ocurran cambios significativos en la normativa, la tecnología, el nivel de las amenazas o las necesidades de la Escuela de Posgrado. La revisión incluirá la evaluación de la eficacia de las políticas y medidas implementadas.

Cajamarca, mayo 2025.

UNIVERSIDAD NACIONAL DE CAJAMARCA
Escuela de Posgrado
DIRECCIÓN