Universidad Nacional de Cajamarca

LICENCIADA CON RESOLUCIÓN DE CONSEJO DIRECTIVO N° 080-2018-SUNEDU/CD

Escuela de Posgrado

CAJAMARCA – PERU

RESOLUCIÓN DE SESIÓN EXTRAORDINARIA DE CONSEJO DE COORDINACIÓN DE ESCUELA DE POSGRADO N°920-2025-EPG-UNC.

Cajamarca, 10 de junio de 2025

VISTO:

La **Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca** y el Acuerdo se Sesión Extraordinaria de Consejo de Escuela de Posgrado de fecha 10 de junio de 2025, y;

CONSIDERANDO:

Que, mediante documento de visto, la Directora de la Escuela de Posgrado de la Universidad Nacional de Cajamarca, pone a consideración la **Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca**, en donde se establecen los principios, normas y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos de esta Unidad de Posgrado en el Marco de los Programas que se desarrollan y reconociendo el creciente impacto de las tecnologías de la información en el entorno académico presencial y no presencial, buscando de esta manera proteger los activos de información contra amenazas internas y externas, con el fin de asegurar un ambiente digital seguro tanto para estudiantes, docentes y personal administrativo;

Que, la presente Directiva también tiene por objeto, asegurar la integridad de los datos y sistemas, previniendo alteraciones no autorizadas y accidentales y estableciendo un marco de responsabilidades claras en materia de seguridad informática;

Y, estando expuesto a la Ley Universitaria N° 30220, Decreto Legislativo N°822, Ley N° 30096, Ley de Protección de Datos Personales y su Reglamento, Ley N° 30096, Ley de Delitos Informáticos y su Reglamento, Modelo de Licenciamiento de Programas en las modalidades semipresencial y a Distancia Resolución, del Consejo Directivo N°033-2023-SUNEDU/DE., Artículo 22° inciso h) del Reglamento Interno de la Escuela de Posgrado y al acuerdo de la Sesión Extraordinaria de Consejo de Coordinación de Escuela de Posgrado, de la fecha.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR, la **Directiva para la Seguridad Informática de la Escuela de Posgrado de la Universidad Nacional de Cajamarca,** la misma que consta de 10 Artículos.

ARTÍCULO SEGUNDO.- ELEVAR, la presente Resolución, al Honorable Consejo Universitario para su Ratificación.

Regístrese, Comuníquese y Archívese.

UNIVERSIDAD NACIONAL DE CAJAMARCA
ESCUELA DE POSGRADO
Dra. Leticia N. Zavaleta Gonzáles
DIRECTORA

UNIVERSIDAD NACIONAL DE CAJAMARCA
Secretaría Académica
Escuela de Posgrado

UNIVERSIDAD NACIONAL DE CAJAMARCA
ESCUELA DE POSGRADO
Dra. Irma A. Mostacero Castillo
SECRETARIA ACADÉMICA

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.
Se implementarán políticas de bloqueo de cuentas por intentos fallidos de acceso.

UNIVERSIDAD NACIONAL DE CAJAMARCA Escuela de Posgrado DIRECCIÓN

5

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.

UNIVERSIDAD NACIONAL DE CAJAMARCA Escuela de Posgrado DIRECCIÓN

6

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

7

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.

UNIVERSIDAD NACIONAL DE CAJAMARCA
Escuela de Posgrado
DIRECCIÓN

Cajamarca, mayo 2025.