RESOLUCIÓN RECTORADO Nº 045/2026

QUE APRUEBA LAS POLÍTICAS Y LOS LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DEL RECTORADO DE LA UNIVERSIDAD NACIONAL DE CAAGUAZÚ - VERSIÓN 1.

Coronel Oviedo, 16 de febrero del 2026

VISTO: El Memorándum SI N° 02/2026, proveniente del Departamento de Seguridad de la Información, por medio del cual solicita la aprobación de las Políticas y Lineamientos de Seguridad de la Información del Rectorado de la Universidad Nacional de Caaguazú – Versión 1".

La Norma ISO/IEC 27001; la ISO/iec 27002 y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y la Comunicación.

La Ley Nº 3385/2007 "*Que aprueba la Carta Orgánica de la Universidad Nacional de Caaguazú, con sede en Coronel Oviedo*".

CONSIDERANDO: Que, la Universidad Nacional de Caaguazú, en su carácter de institución pública de educación superior, administra información académica, administrativa, financiera, científica y personal cuya adecuada protección resulta esencial para el cumplimiento de sus fines misionales, la preservación de la confianza pública y la garantía de los derechos de la comunidad universitaria.

Que, la transformación digital y el creciente uso de tecnologías de la información y la comunicación en los procesos institucionales exigen la adopción de un marco normativo que establezca criterios claros para la protección de la confidencialidad, integridad y disponibilidad de la información.

Que, la norma internacional ISO/IEC 27001 establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), y la ISO/IEC 27002 proporciona directrices para la aplicación de controles de seguridad, constituyéndose en estándares de referencia reconocidos a nivel mundial.

Que, la normativa nacional vigente en materia de tecnologías de la información, gobierno digital y protección de datos, así como los lineamientos y directrices emitidos por el Ministerio de Tecnologías de la Información y Comunicación (MITIC) y el CERT-PY, recomiendan la adopción de medidas institucionales orientadas a fortalecer la ciberseguridad y la resiliencia organizacional.

Que, el documento en cuestión establece el marco institucional que regirá la gestión de la seguridad de la información y corresponde a la máxima autoridad institucional aprobar los instrumentos normativos necesarios para asegurar el adecuado funcionamiento administrativo y la protección de los recursos estratégicos de la Universidad.

Claudia P. Godoy Sosa
Secretaria General

María Gloria Martínez Blanco
Rectora

RESOLUCIÓN RECTORADO Nº 045/2026

QUE APRUEBA LAS POLÍTICAS Y LOS LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DEL RECTORADO DE LA UNIVERSIDAD NACIONAL DE CAAGUAZÚ - VERSIÓN 1.

Que, la Ley 3385/2007 "*Que aprueba la Carta Orgánica de la Universidad Nacional de Caaguazú, con sede en Coronel Oviedo*", en su Artículo 19 establece: *"De las Atribuciones y Deberes del Rector: Inc. f) adoptar las medidas necesarias y urgentes para el buen gobierno de la Universidad..."* que se ajusta a la presente circunstancia.

POR TANTO, en uso de sus atribuciones, y fundada en el considerando precedente,

LA RECTORA DE LA UNIVERSIDAD NACIONAL DE CAAGUAZÚ
RESUELVE:

Art. 1°) APROBAR las **Políticas y Lineamientos de Seguridad de la Información del Rectorado de la Universidad Nacional de Caaguazú – Versión 1,** que foliado, sellado y rubricado forma parte íntegra de la presente Resolución.

Art. 2°) COMUNICAR a quienes corresponda, tomar nota respectiva y cumplido archivar.

Claudia Patricia Godoy Sosa
Secretaria General

UNIVERSIDAD NACIONAL DE CAAGUAZÚ Coronel Oviedo PARAGUAY ARANDU POTY RECAVO 2007

María Gloria Martínez Blanco
Rectora

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN
Rectorado - Universidad Nacional de Caaguazú - Versión 1

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1 Declaración de Compromiso

La Universidad Nacional de Caaguazú reconoce que la información constituye un activo estratégico fundamental para el cumplimiento de sus funciones académicas, administrativas, científicas y de extensión.

El Rectorado se compromete a:

- Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001.
- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con la normativa nacional vigente, lineamientos del MITIC y recomendaciones del CERT-PY.
- Asignar recursos necesarios para la gestión eficaz de la seguridad.
- Promover la mejora continua del SGSI.

1.2 Objetivo

El objetivo de la presente política es establecer el marco institucional para la gestión integral de la seguridad de la información en el Rectorado, mediante la identificación, análisis y tratamiento de los riesgos asociados; la protección adecuada de los activos de información institucionales; la prevención y gestión oportuna de incidentes de seguridad; la garantía de la continuidad operativa de los servicios académicos y administrativos; y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

1.3 Alcance

La presente política es de aplicación obligatoria en el ámbito del Rectorado y alcanza a todas sus dependencias, direcciones y unidades administrativas, así como a las autoridades, funcionarios administrativos, docentes y técnicos que prestan servicios en dicha instancia. Asimismo, aplica a proveedores, contratistas y terceros que tengan acceso a información o recursos tecnológicos del Rectorado, incluyendo los sistemas académicos, administrativos y financieros bajo su administración, la infraestructura tecnológica correspondiente y toda documentación en formato físico o digital gestionada en el ámbito del Rectorado.

1.4 Principios

El Rectorado adoptará un enfoque integral de seguridad de la información basado en la gestión de riesgos, asegurando que las decisiones y controles implementados respondan a la identificación y evaluación sistemática de amenazas y vulnerabilidades. Se aplicará el principio de mínimo privilegio, otorgando a los usuarios únicamente los accesos estrictamente necesarios para el cumplimiento de sus funciones, y se implementará una estrategia de defensa mediante la combinación de controles organizacionales, físicos y tecnológicos. La seguridad será entendida como una responsabilidad compartida por todo el Rectorado, promoviendo una cultura institucional de protección de la información. Asimismo, el Sistema de Gestión de Seguridad de la Información se desarrollará bajo un esquema de mejora continua conforme al ciclo .../...

Claudia P. Godoy Sosa
Secretaria General

Coronel Oviedo PARAGUAY ARANDU POTY REGAVO 2007

María Gloria Martínez Blanco
Rectora

…//…Planificar-Hacer-Verificar-Actuar (PHVA), garantizando el cumplimiento de la normativa nacional vigente, los estándares internacionales aplicables, la mejora continua y el control de la gestión pública.

2. GOBERNANZA DEL SGSI (ISO 27001)

2.1 Contexto Organizacional

El Departamento de Seguridad de la Información del Rectorado deberá identificar y analizar de manera permanente el contexto interno y externo que pueda afectar la seguridad de la información bajo su ámbito de competencia. Para ello, considerará a las partes interesadas relevantes, tales como autoridades del Rectorado, dependencias administrativas, organismos del Estado, proveedores tecnológicos y demás actores vinculados. Asimismo, deberá determinar y mantener actualizados los requisitos legales, regulatorios y contractuales aplicables, incluyendo la normativa nacional vigente y los lineamientos emitidos por el MITIC y el CERT-PY.

2.2 Roles y Responsabilidades

El Rectorado, en su carácter de máxima autoridad institucional dentro de su ámbito, será responsable de aprobar la política de seguridad de la información, asignar los recursos necesarios para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), y promover una cultura organizacional orientada a la protección de la información. El Departamento de Seguridad de la Información será el órgano técnico responsable de administrar el SGSI, gestionar los riesgos de seguridad, supervisar la implementación de controles organizacionales, físicos y tecnológicos, y coordinar acciones con el MITIC y el CERT-PY ante situaciones que así lo requieran. Los responsables de activos deberán asegurar la correcta clasificación de la información bajo su custodia y definir los niveles de acceso correspondientes, mientras que todos los usuarios del ámbito del Rectorado deberán cumplir las políticas establecidas, proteger adecuadamente sus credenciales y reportar cualquier incidente o sospecha de incidente de seguridad.

3. GESTIÓN DE RIESGOS

El Departamento de Seguridad de la Información implementará y mantendrá un proceso formal y documentado de gestión de riesgos conforme a la Cláusula 6 de la ISO/IEC 27001, el cual se articulará con la metodología institucional de gestión de riesgos adoptada en el marco de la Norma de Requisitos Mínimos MECIP:2015, a fin de garantizar coherencia, integración y evitar duplicidad de registros. Dicho proceso contempla la identificación de los activos de información del Rectorado, el análisis de amenazas y vulnerabilidades asociadas, la evaluación del impacto y la probabilidad de ocurrencia, la determinación del nivel de riesgo y la definición de planes de tratamiento apropiados. El análisis de riesgos deberá revisarse al menos una vez al año o cuando se produzcan cambios significativos en el entorno tecnológico, organizacional o normativo, o cuando así lo exijan los lineamientos del MECIP o las recomendaciones emitidas por el MITIC y el CERT-PY.

4. LINEAMIENTOS DE SEGURIDAD (ISO 27002)

4.1 Controles Organizacionales

Claudia P. Godoy Sosa
Secretaria General

UNIVERSIDAD NACIONAL DE CAAGUAZÚ Coronel Oviedo PARAGUAY ARAUDO POTT RECALDE 2007

María Gloria Martínez Blanco
Rectora

4.1.1 Gestión de Activos

El Departamento de Seguridad de la Información deberá mantener un inventario actualizado de los activos de información del Rectorado, asegurando que cada activo tenga un propietario formalmente asignado y una clasificación definida. La información será categorizada como Pública, de Uso Interno, Confidencial, sensible o crítica, debiendo considerarse como mínimo Confidencial aquella que contenga datos personales, información académica, administrativa o financiera sensible. Asimismo, se establecerán normas de uso aceptable de los recursos tecnológicos, quedando expresamente prohibido compartir credenciales de acceso, instalar software no autorizado o hacer uso indebido de los sistemas institucionales. En relación con proveedores y terceros, deberán formalizarse acuerdos de confidencialidad, cláusulas de protección de datos y mecanismos de evaluación periódica del cumplimiento de requisitos de seguridad.

4.2 Controles de Personas

Los contratos y designaciones de los funcionarios del Rectorado deberán incluir cláusulas de confidencialidad y compromisos de cumplimiento de las políticas de seguridad de la información. El Departamento de Seguridad de la Información promoverá programas de capacitación anual obligatoria en materia de seguridad y ciberseguridad. Asimismo, deberá existir un procedimiento formal de desvinculación que contemple la revocación inmediata de accesos y la recuperación de activos institucionales.

4.3 Controles Físicos

El acceso a las áreas críticas, como salas de servidores del Rectorado, deberá estar restringido y controlado. Se mantendrán registros de visitantes y se asegurará el resguardo de documentos físicos sensibles en muebles o archiveros bajo llave. Toda información escrita que deba ser desechada por motivos de mala impresión, errores operativos u obsolescencia, deberá ser triturada previamente antes de su disposición final en los contenedores de basura, garantizando la irrecuperabilidad de los datos. El tiempo de obsolescencia dependerá de cada dependencia. Asimismo, deberán implementarse medidas de protección contra incendios, fallas eléctricas, inundaciones y otros riesgos ambientales que puedan afectar la infraestructura física y tecnológica.

4.4 Controles Tecnológicos

El acceso a los sistemas deberá realizarse mediante autenticación individual, con contraseñas robustas y, en sistemas críticos, mecanismos de autenticación multifactor. Los privilegios de acceso deberán revisarse periódicamente. Se implementarán soluciones de protección contra malware, tales como antivirus o EDR (**Endpoint Detection and Response**) actualizados, junto con políticas de actualización automática de sistemas. El Departamento deberá gestionar vulnerabilidades mediante la aplicación oportuna de parches, la realización de escaneos periódicos y la corrección de debilidades identificadas. Todos los equipos de escritorio deberán contar con el disco duro particionado, separando el Sistema Operativo de los datos del usuario, a fin de facilitar la recuperación ante fallos y optimizar la gestión de respaldo. Se establecerán mecanismos de respaldo periódico de la información crítica y resguardo seguro de copias tanto locales como externas. Los equipos portátiles (notebooks) deberán tener activado obligatoriamente el cifrado de disco duro completo mediante Bitlocker o solución equivalente según el sistema operativo, garantizando la protección de la información en caso de robo, pérdida o acceso físico no autorizado, las claves de recuperación …//…

Claudia P. Godoy Sosa
Secretaria General

María Gloria Martínez Blanco
Rectora

…//… deberán custodiarse centralizadamente por el Departamento de Seguridad de la Información. La información sensible deberá cifrarse adicionalmente durante su transmisión por redes públicas o inseguras. Asimismo, se implementarán mecanismos de registro y monitoreo de eventos, con conservación de logs conforme a la normativa aplicable y capacidad de detección de actividades sospechosas.

5. Gestión de Incidentes

El Departamento de Seguridad de la Información deberá implementar un procedimiento formal de gestión de incidentes que contemple su identificación, registro, clasificación, contención, erradicación, recuperación y elaboración de informe final. Los incidentes críticos o que puedan afectar significativamente la operación institucional deberán ser notificados al CERT-PY conforme a los protocolos nacionales vigentes, sin perjuicio de las comunicaciones internas correspondientes.

6. Continuidad Operativa

En el ámbito del Rectorado, el Departamento de Seguridad de la Información deberá coordinar la elaboración de un Plan de Gestión de la Continuidad Operativa y un Plan de Recuperación ante Desastres, los cuales deberán ser probados periódicamente y mantenerse actualizados, a fin de garantizar la disponibilidad y funcionamiento de los servicios críticos.

7. Concienciación y cultura de seguridad

El Departamento promoverá campañas internas de concienciación sobre riesgos como el phishing u otros, realizará simulaciones de ataques cuando corresponda y difundirá alertas de seguridad emitidas por el CERT-PY u otras autoridades competentes, fortaleciendo una cultura preventiva dentro del Rectorado.

8. Auditoría y Mejora Continua

El Sistema de Gestión de Seguridad de la Información deberá someterse a auditorías internas periódicas. Se gestionarán las no conformidades detectadas y se implementarán acciones correctivas. El desempeño del SGSI será medido mediante indicadores definidos, promoviendo la mejora continua conforme a las cláusulas 9 y 10 de la ISO/IEC 27001.

9. Cumplimiento y Sanciones

El incumplimiento de la presente política y lineamientos podrá derivar en medidas disciplinarias, suspensión de accesos a sistemas, responsabilidades administrativas y, cuando corresponda, acciones legales conforme a la legislación paraguaya vigente.

10. Revisión y actualización

La presente política deberá ser revisada al menos una vez al año, así como ante incidentes graves, cambios tecnológicos relevantes, modificaciones normativas o recomendaciones emitidas por el MITIC o el CERT-PY, garantizando su actualización y adecuación continua.

Claudia P. Godoy Sosa
Secretaria General

UNIVERSIDAD NACIONAL DE CAAGUAZÚ Coronel Oviedo PARAGUAY ARANDU ÑOTI RECAVO 2007

María Gloria Martínez Blanco
Rectora