UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

RESOLUCIÓN Nº 1007/2025

POR LA CUAL SE APRUEBA Y SE HABILITA EL PROYECTO DEL CURSO DE SEGURIDAD DE DATOS DEL ÁREA DE CIBERSEGURIDAD, CONVOCATORIA OCTUBRE – 2025.

12 de agosto de 2025

VISTO Y CONSIDERANDO: El Memorando DGCITIC/0178/2025, del Director, Lic. Juan Fernando Duré, de la Dirección de Gestión del Centro de Innovación en TIC de la FP-UNA, en el que solicita la habilitación del Curso de Seguridad de Datos del Área de Ciberseguridad, Convocatoria Octubre – 2025, elaborado por el Prof. Mgrt. Carlos Alberto Martínez Galeano.

Que la propuesta esta diseñada para abordar temas claves como criptografía simétrica y asimétrica, modelos de control de acceso, gestión de riesgos, protección, protección de la privacidad y normativa legal aplicable (como la Ley N° 06534/20 y estándares internacionales como ISO/IEC 27001). Asimismo, se analizan las implicancias éticas vinculadas al uso, protección y divulgación de la información, promoviendo una mirada crítica y responsable en la toma de decisiones.

Que el curso está estructurado en 40 horas reloj (8 semanas de duración) a ser desarrollados en la modalidad virtual, la distribución del contenido será de 40 horas de clases virtuales (sincrónicas), fecha de inicio: 06/10/2025, la fecha de finalización: 28/11/2025.

Que el curso dará apertura con una convocatoria de 5 (cinco) matriculados como mínimo.

La Ley N° 4995/2013 de Educación Superior.
El Estatuto de la Universidad Nacional de Asunción.

POR TANTO: en uso de sus facultades y atribuciones legales,

LA DECANA DE LA FACULTAD POLITÉCNICA
RESUELVE:

Art. 1º Aprobar el Proyecto del Curso de Seguridad de Datos del Área de Ciberseguridad, Convocatoria Octubre – 2025, detallado en el ANEXO de la presente Resolución.

Art. 2º Habilitar el Proyecto del Curso de Seguridad de Datos del Área de Ciberseguridad, Convocatoria Octubre – 2025, en la modalidad virtual.

Art. 3° Comunicar, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario de la Facultad

Prof. Ing. Silvia Teresa Leiva León, MSc.
Decana

ANEXO RESOLUCIÓN Nº 1007/2025

Universidad Nacional de Asunción

Facultad Politécnica

Centro de Innovación TIC

Proyecto Curso de corta duración

Título: Seguridad de Datos del Área de Ciberseguridad

Modalidad: Virtual

Docente

Prof. Mgrt. Carlos Alberto Martínez Galeano

Sede Central, San Lorenzo

Octubre, 2025

..//..

ANEXO RESOLUCIÓN Nº 1007/2025

Información básica

[Información del curso]

1	Título	*Seguridad de los Datos*
2	Código	-
3	Año propuesto	*2025/2026*
4	Semestre propuesto	*Segundo*
5	Departamento	*Centro de Innovación TIC (FPUNA)*
6	Año Objetivo/Carrera	*Intermedio*
7	Horas de créditos	*No aplica*
	Formato de clase (tipo)	*Clases interactivas, sesiones prácticas.*

[Horario y Lugar]

1	Días	*Lunes y miércoles*
2	Horario	*de 19:00 a 21.30*
3	Ubicación	*Online en la plataforma institucional*

[Información del instructor/a]

1	Nombre	*Prof. Lic. Carlos Alberto Martínez Galeano*
2	Oficina (si aplica)	*José Guerrero No. 352 esquina Fidel Maíz – M. R. Alonso*
3	Contacto (correo)	*carlos.martinezgaleano@gmail.com*
4	Contacto (teléfono)	*(0971)142.841*

* Si el curso se imparte en equipo con asistente(s), añada más cuadros para describirlos a todos.

[Horario de oficina]

Si se han previsto horas de oficina, describa la hora y el horario con detalles.

[Notas adicionales]

..//..

□ Prerrequisitos

Los estudiantes deberán contar con conocimientos básicos en:

- Redes de computadoras.
- Sistemas operativos (Windows y Linux).
- Fundamentos de seguridad informática.

□ Descripción del curso

El presente curso está diseñado para estudiantes de nivel básico/intermedio interesados en adquirir competencias técnicas y estratégicas en la protección de la información. A lo largo del curso, los participantes explorarán herramientas, metodologías y marcos legales que permitan garantizar la confidencialidad, integridad y disponibilidad de los datos en entornos digitales.

Las clases combinan sesiones magistrales con dinámicas interactivas, donde el análisis de casos reales y debates éticos permiten una comprensión contextualizada de los desafíos actuales en materia de ciberseguridad. A esto se suman laboratorios prácticos, en los que los estudiantes implementarán técnicas de cifrado, configurarán controles de acceso, evaluarán vulnerabilidades y aplicarán medidas de protección en el almacenamiento y transmisión de datos.

El curso aborda temas clave como criptografía simétrica y asimétrica, modelos de control de acceso, gestión de riesgos, protección de la privacidad y normativa legal aplicable (como la Ley N.o6534/20 y estándares internacionales como ISO/IEC 27001). Asimismo, se analizan las implicancias éticas vinculadas al uso, protección y divulgación de la información, promoviendo una mirada crítica y responsable en la toma de decisiones.

Durante el desarrollo del programa, los estudiantes interactuarán con el Docente Titular y en casos puntuales con Docentes Especializados en el Sector en charlas especializadas, lo que permitirá vincular los contenidos teóricos con escenarios del mundo real. El componente final del curso incluye un proyecto de análisis de vulnerabilidades, aplicación de activos de información y mapa de riesgos donde cada grupo deberá diseñar una estrategia de seguridad de datos para una organización simulada, aplicando los conocimientos adquiridos en un entorno práctico y colaborativo.

El enfoque del curso es multidisciplinario, integrando dimensiones técnicas, jurídicas y éticas, con el objetivo de formar profesionales capaces de enfrentar los riesgos digitales con una visión integral y actualizada. Al finalizar el curso, el estudiante será capaz de identificar vulnerabilidades, aplicar mecanismos de defensa y comprender el marco normativo que rige la protección de datos, contribuyendo activamente a la cultura de la ciberseguridad en cualquier entorno profesional tanto público como privado.

□ Objetivo del curso

Al finalizar con éxito este curso los estudiantes serán capaces de:

- Desarrollar habilidades técnicas, legales y éticas en la protección y seguridad de los datos mediante el estudio y aplicación de técnicas de ciberseguridad, normas legales, control de acceso, cifrado, transmisión segura y gestión de riesgos.

Y las descripciones detalladas de los subtemas se incluyen aquí.

- Comprender los fundamentos y técnicas de criptografía simétrica y asimétrica.
- Aplicar mecanismos de control de acceso en diferentes entornos digitales.
- Identificar los Activos de la Información.

..//..

- Identificar y mitigar riesgos asociados al almacenamiento y transmisión de datos.
- Realizar la matriz de riesgos para la adopción de medidas correctivas.
- Analizar marcos legales y éticos sobre privacidad y protección de datos.
- Implementar buenas prácticas en gestión de seguridad de datos con herramientas estándares del sector.

□ **Política de calificación**

□ Calificación absoluta

El esquema de calificación del presente curso se basa en una evaluación integral del desempeño del estudiante, considerando comprensión teórica, aplicación práctica y participación activa. Se distribuye de la siguiente manera:

- Asistencia y participación: 10%
- Tareas y cuestionarios: 20%
- Prácticas de laboratorio: 30%
- Examen parcial: 15%
- Examen final: 15%
- Proyecto final: 10%

Libros de texto y otros materiales necesarios

Bibliografía principal (libros de texto online/offline):

- Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.) Pearson.
- Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications.
- Solms, B., & van Niekerk, J. (2017). Information Security Governance. Springer.

Libros de texto online recomendados y de acceso compartible:

- Open Web Application Security Project (OWASP). OWASP Top 10. https://owasp.org/www-project-top-ten/
- ISO/IEC 27001 Summary Guidelines – online summaries y documentos públicos de libre acceso.
- European Union Agency for Cybersecurity (ENISA). Threat Landscape Reports. https://www.enisa.europa.eu/publications
- Instituto Nacional de Ciberseguridad INCIBE. España. https://www.incibe.es/incibe-cert/publicaciones/guias-y-estudios

Otros materiales requeridos:

Software (SW):

- Wireshark
- OpenSSL
- GPG (GNU Privacy Guard)
- VeraCrypt o BitLocker
- VirtualBox o VMware Player
- Kali Linux (máquina virtual)

Hardware (HW):

- Computadora con mínimo 8 GB de RAM y procesador multinúcleo
- Acceso a red con capacidad para simulaciones
- Almacenamiento externo (USB seguro) para prácticas de cifrado

Referencias adicionales:

- Andress, J. (2019). The Basics of Information Security (3rd ed.). Syngress.

..//..

- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
- Ley N.o 6534/20 – "De protección de datos personales en Paraguay".
- ISO/IEC 27001 y 27002 – Normas sobre sistemas de gestión de seguridad de la información (SGSI).
- COBIT.

□ Tarea(s) y examen(es)

Las tareas están orientadas a reforzar los conceptos teóricos abordados en clase y promover la aplicación práctica de los mismos mediante el uso de herramientas reales de ciberseguridad. Se realizarán de forma individual y grupal, y estarán distribuidas a lo largo del curso.

Tipos de tareas:

- Tarea 1: Análisis de un caso de violación de datos reales (ensayo corto).
- Tarea 2: Simulación de cifrado y descifrado con GPG y OpenSSL (laboratorio).
- Tarea 3: Configuración de control de acceso en sistemas operativos (laboratorio práctico)
- Tarea 4: Elaboración de una matriz de riesgos y propuesta de mitigación para un escenario simulado basado en la matriz de riesgos.
- Tarea 5 (opcional): Participación en una plataforma online (TryHackMe o similar) para ejercicios prácticos.

Exámenes:

Los exámenes están diseñados para evaluar la comprensión integral de los conceptos teóricos y su aplicación práctica.

- Examen Parcial (semana 6 y 7):
  - Preguntas de opción múltiple, verdadero/falso y desarrollo corto.
  - Enfoque en criptografía, control de acceso y privacidad de datos.
- Examen Final (semana 8):
  - Casos prácticos a resolver + preguntas teóricas.
  - Evaluación de contenidos integrados (gestión de riesgos, normativas legales, ética y medidas técnicas).

□ Actividades del curso

Las actividades del curso están diseñadas para que los estudiantes se involucren activamente con los materiales, refuercen su comprensión y desarrollen habilidades prácticas. Estas actividades van desde conferencias y debates interactivos hasta laboratorios prácticos y proyectos en grupo.

- Clases interactivas con preguntas en vivo, resolución de dudas y pequeños sondeos participativos.
- Debates guiados sobre estudios de casos reales de filtración de datos, con enfoque técnico y ético.
- Laboratorios prácticos orientados a la configuración de herramientas de cifrado, control de acceso y análisis de tráfico.
- Proyecto en grupo al final del curso, que integrará todos los conocimientos en una propuesta de seguridad para una organización simulada.
- Charla invitada de un profesional del sector, con espacio para preguntas y discusión.

..//..

□ **Cronograma del curso**

Semana	Tema	Tipo de clases	Materiales
1	Fundamentos de seguridad de los datos y clasificación de activos	Clase interactiva	Presentación teórica, lectura base, artículos introductorios
2	Criptografía aplicada: simétrica, asimétrica y hash	Clase interactiva	Manual OpenSSL/GPG, guías de laboratorio, videos explicativos
3	Control de acceso y privacidad de datos	Clase interactiva	Estudio de caso, marco legal (Ley N.o 6534/20), lectura dirigida
4	Laboratorios prácticos: cifrado, control de acceso, privacidad	Clase interactiva	Kali Linux, Wireshark, VeraCrypt, GPG
	Examen Parcial	Evaluación escrita (de ser posible presencial)	Examen tipo mixto (teórico-práctico)
5	Seguridad en almacenamiento y transmisión de datos	Clase interactiva	Guías técnicas, prácticas con VPN, HTTPS, SFTP
6	Gestión de riesgos y normativas ISO/IEC 27001	Formato de Taller	Lectura de norma resumida, matriz de riesgos, presentación grupal
7	Cibernética y marco legal aplicado a protección de datos	Ponencia invitada	Exposición + foro, análisis normativo.
8	Proyecto integrador: propuesta de seguridad para una organización	Taller	Plantilla de proyecto, rúbrica de evaluación, revisión por pares.
	Examen Final	Evaluación práctica	Caso aplicado, análisis y resolución con defensa oral

* Un curso está diseñado para un periodo de 8 semanas y un total de 40 horas requeridas (5 horas por semana). Una semana puede incluir varias sesiones cortas y combinaciones de actividades.

□ **Contenidos del curso**

Semana 1: Fundamentos de seguridad de los datos y clasificación de activos
Objetivo: Comprender los principios básicos de la seguridad de la información y la clasificación de datos.
Tipo de clase: Clase interactiva con presentación, preguntas y discusión.
Materiales y referencias: Capítulo 1 – Fundamentos de Seguridad en Redes. Stallings (2020); Matriz de Activos de Información. Artículos introductorios en PDF (proporcionados por el docente).

Semana 2: Criptografía aplicada: simétrica, asimétrica y hash
Objetivo: Aplicar técnicas básicas de criptografía para la protección de datos.
Tipo de clase: Clase interactiva con demostraciones y ejercicios guiados.

Materiales y referencias: Capítulos 2-4 - Fundamentos de Seguridad en Redes. Stallings (2020); Manual OpenSSL (https://docs.openssl.org/master/man3/); GPG Documentation (https://www.gnupg.org/gph/es/manual.html).
Semana 3: Control de acceso y privacidad de datos
Objetivo: Entender modelos de control de acceso y su relación con la privacidad de datos personales.

..//..

Tipo de clase: Debate sobre casos reales y análisis normativo.
Materiales y referencias: Ley 6534/20; lectura complementaria.
Semana 4: Laboratorios prácticos y examen parcial
Objetivo: Poner en práctica técnicas de cifrado, control de acceso y protección de la privacidad.
Tipo de clase: Laboratorio práctico y evaluación escrita parcial.
Materiales y referencias: Kali Linux, Wireshark, GPG, VeraCrypt; guía de ejercicios entregada en clase.

Semana 5: Seguridad en almacenamiento y transmisión de datos
Objetivo: Implementar mecanismos de protección de datos en tránsito y en reposo.
Tipo de clase: Clase interactiva con simulaciones técnicas.
Materiales y referencias: Capítulo 8 - Fundamentos de Seguridad en Redes. Stallings (2020); recursos en línea sobre SSL/TLS y cifrado de disco.

Semana 6: Gestión de riesgos y normativas ISO/IEC 27001
Objetivo: Identificar riesgos e implementar controles conforme a normas reconocidas.
Tipo de clase: Seminario con análisis grupal y trabajo aplicado.
Materiales y referencias: ISO/IEC 27001 resumen ejecutivo (PDF); PCI. Plantilla de matriz de riesgos.

Semana 7: Cibernética y marco legal aplicado a protección de datos
Objetivo: Analizar dilemas éticos y el marco jurídico vigente sobre protección de datos.
Tipo de clase: Ponencia invitada y discusión guiada.
Materiales y referencias: Ley 6534/20; ENISA Threat Landscape 2024 (fragmentos); caso Facebook-Cambridge Analytica.

Semana 8: Proyecto integrador y examen final
Objetivo: Aplicar todos los conocimientos adquiridos en un caso práctico integrador.
Tipo de clase: Taller grupal con defensa del proyecto y evaluación final.
Materiales y referencias: Plantilla de proyecto (proporcionado por el Docente), rúbrica, acceso a herramientas de laboratorio.

..//..