



Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

RESOLUCIÓN N° 0714/2025

POR LA CUAL SE APRUEBA Y SE HABILITA EL CURSO DE INTRODUCCIÓN A LA CIBERSEGURIDAD Y A LA SEGURIDAD DE REDES – PRIMERA COHORTE DEL AÑO 2025.

25 de junio de 2025

VISTO Y CONSIDERANDO: El Memorando DGCITIC/0142/2025, del Director, Lic. Juan Fernando Duré, de la Dirección de Gestión del Centro de Innovación en TIC de la FP-UNA, en el cual solicita la aprobación y la habilitación del Curso de Introducción a la Ciberseguridad y a la Seguridad de Redes – primera cohorte del año 2025, presentado por el Prof. Chrystian David Ruiz Díaz Centurión.

Que la propuesta está diseñada para una introducción fundamental al mundo de la ciberseguridad y la seguridad de redes, orientado a estudiantes que deseen iniciarse en la protección de sistemas y datos digitales. A lo largo del curso, se proporciona una visión clara de los principios esenciales de la ciberseguridad, abordando desde los tipos de amenazas y ataques más comunes hasta las estrategias básicas para mitigar riesgos en entornos digitales. Que dicho curso está estructurado en base a 40 horas (8 semanas de duración), a ser desarrolladas en la modalidad virtual. La fecha de inicio 05/08/2025, la fecha de finalización: 25/09/2025.

Que dicho curso está estructurado en base a 40 horas (8 semanas de duración), a ser desarrolladas en la modalidad virtual. La fecha de inicio 05/08/2025, la fecha de finalización: 25/09/2025.

Que el curso estima dar apertura con una convocatoria de 5 (cinco) matriculados como mínimo y máximo y 50 matriculados como máximo.

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. 1°** Aprobar el Programa del Curso de Introducción a la Ciberseguridad y a la Seguridad de Redes – Primera cohorte del año 2025, detallado en el ANEXO de la presente Resolución.
- Art. 2°** Habilitar el Curso de Introducción a la Ciberseguridad y a la Seguridad de Redes – Primera cohorte del año 2025, ofrecido por la FP-UNA.
- Art. 3°** Comunicar, copiar y archivar.

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

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





Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

ANEXO RESOLUCIÓN N° 0714/2025

Pág. 1/8

Universidad Nacional de Asunción

Facultad Politécnica

Centro de Innovación en TIC



Proyecto Curso de corta duración

Título: *Introducción a la Ciberseguridad y a la Seguridad de Redes*

Modalidad: *Online*

Docente

Prof. Chrystian David Ruiz Diaz Centurión

Sede Central, San Lorenzo

Junio, 2025

..//..





UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

ANEXO RESOLUCIÓN N° 0714/2025

Pág. 2/8

Inteligencia Artificial

Información básica

1	Título	Introducción a la ciberseguridad y a la seguridad de redes
2	Código	Código del curso
3	Año propuesto	2025
4	Semestre propuesto	Primero
5	Departamento	Centro de Innovación TIC (FP-UNA)
6	Nivel	Básico
7	Horas de créditos	Crédito total: 3 Créditos de clase: 1 Créditos experimentales/prácticos: 2 Créditos de diseño: 0 Otros: 0
8	Formato de clase (tipo)	Clases interactivas Sesiones prácticas Laboratorios

[Horario y Lugar]

1	Días	Martes y Jueves
2	Horario	de 19:00 a 22:00
3	Ubicación	Online - Asíncronas

[Información del instructor/a]

1	Nombre	Prof. Chrystian David Ruiz Diaz Centurión
2	Oficina (si aplica)	
3	Contacto (correo)	<i>Chrystiandavid2000@pol.una.py</i>
4	Contacto (teléfono)	(0982) 508.890

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



..//..



UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

ANEXO RESOLUCIÓN Nº 0714/2025

Pág. 3/8

[Perfil Profesional]

Prof. Chrystian David Ruiz Diaz Centurión

[Horario de oficina]

El Docente se encuentra disponible para contacto por whatsapp o correo electrónico. Las llamadas pueden ser coordinadas previamente según disponibilidad.

Prerrequisitos

Ninguno.

Descripción del curso

Este curso ofrece una introducción fundamental al mundo de la ciberseguridad y la seguridad de redes, orientado a estudiantes que deseen iniciarse en la protección de sistemas y datos digital es. A lo largo del curso, se proporciona una visión clara de los principios esenciales de la ciberseguridad, abordando desde los tipos de amenazas y ataques más comunes hasta las estrategias básicas para mitigar riesgos en entornos digitales.

El plan de estudios combina teoría y práctica, permitiendo que los participantes aprendan mediante ejercicios aplicados y sesiones de laboratorio con herramientas estándar del sector. Entre los contenidos clave se incluyen: fundamentos de ciberseguridad, protocolos de seguridad, análisis de vulnerabilidades, gestión de incidentes, y buenas prácticas para proteger redes e infraestructuras tecnológicas.

El curso también incorpora temas de actualidad, como la seguridad en la nube, la protección en dispositivos del Internet de las Cosas (IoT) y el uso de inteligencia artificial en la ciberdefensa, manteniéndose alineado con las normas y tendencias del sector tecnológico.

Además del enfoque técnico, se pone énfasis en los aspectos éticos y legales que rigen la ciberseguridad, incluyendo el hacking ético, la privacidad digital y los marcos normativos nacionales e internacionales. Esto fomenta una comprensión integral del campo, destacando la importancia de la responsabilidad profesional.

Al finalizar, los estudiantes habrán adquirido las competencias básicas para identificar y prevenir amenazas cibernéticas, así como una base sólida para continuar su formación en áreas más avanzadas de la ciberseguridad

Objetivo del curso

Objetivo General:

- Brindar a los estudiantes una comprensión básica y actualizada de los principios, herramientas y prácticas fundamentales de la ciberseguridad y la seguridad de redes, con el fin de que puedan identificar amenazas, aplicar medidas de protección y valorar los aspectos éticos y legales del entorno digital.

Objetivos Específicos:

- Comprender los conceptos fundamentales de la ciberseguridad y la seguridad de redes, incluyendo amenazas, vulnerabilidades, riesgos y controles.
- Reconocer los principales tipos de ciberataques y sus mecanismos de acción, así como sus efectos sobre la información y los sistemas.
- Aplicar protocolos y buenas prácticas básicas de seguridad informática para proteger datos, dispositivos y redes frente a accesos no autorizados.
- Utilizar herramientas básicas del sector para la detección y mitigación de riesgos, a través de actividades prácticas y laboratorios dirigidos.
- Analizar tendencias emergentes en ciberseguridad, tales como la seguridad en la nube, el IoT y la inteligencia artificial aplicada a la defensa digital.



[Handwritten signature]

..//..



UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

ANEXO RESOLUCIÓN Nº 0714/2025

Pág. 4/8

- Reflexionar sobre los marcos éticos y legales que regulan la ciberseguridad, promoviendo una práctica profesional responsable y consciente de la privacidad y la legalidad.

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

1. Comprender los conceptos fundamentales de la ciberseguridad y la seguridad de redes, incluyendo amenazas, vulnerabilidades, riesgos y medidas de protección básicas.
2. Identificar los principales tipos de ciberataques y sus mecanismos, evaluando su impacto sobre la información y los sistemas tecnológicos.
3. Aplicar protocolos y buenas prácticas de seguridad informática, orientadas a la protección de datos, dispositivos y redes frente a accesos no autorizados o maliciosos.
4. Manejar herramientas básicas del sector para la detección, análisis y mitigación de riesgos digitales, mediante actividades prácticas y laboratorios guiados.
5. Describir y analizar las tendencias actuales en ciberseguridad, tales como la seguridad en la nube, el Internet de las Cosas (IoT) y el uso de inteligencia artificial en ciberdefensa.
6. Reconocer los marcos éticos y legales que regulan la ciberseguridad, aplicando principios de responsabilidad, privacidad y cumplimiento normativo en contextos digitales. Y las descripciones detalladas de los subtemas se incluyen aquí.

Política de calificación.

Calificación absoluta Calificación relativa

Criterios de Evaluación:

La calificación final del curso se determinará mediante la evaluación de los siguientes componentes:

Actividad	Porcentaje
Participación y Asistencia: Asistencia regular a las sesiones. Participación activa en debates y actividades en clase.	15%
Participación en Foros: Contribuciones significativas en foros en línea y debates relacionados con los temas del curso.	10%
Trabajos Prácticos y Laboratorios: Entrega puntual y completa de ejercicios prácticos. Demostración de habilidades adquiridas en sesiones de laboratorio.	30%
Proyecto Final: Desarrollo y presentación de un proyecto integrador que aplique los conocimientos adquiridos durante el curso.	45%

Libros de texto y otros materiales necesarios

- BUENDIA, J. F. (2013). Seguridad informática. España: McGraw-Hill.
- ESCRIVA, G. R. (2013). Seguridad Informática. España: Macmillan Iberia SA.
- GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad.



..//..



UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

ANEXO RESOLUCIÓN N° 0714/2025

Pág. 5/8

- INCIBE. (18 de 03 de 2021). INCIBE - Taxonomía. Obtenido de <https://www.incibe-cert.es/taxonomia>
- INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Análisis de Riesgos: <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>
- STEWART, J. M. (2013). Network Security, Firewalls and VPNs. Jones & Bartlett Publishers.
- VIEITES, Á. G. (2014). Gestión de Incidentes de Seguridad Informática. . RA-MA Editori

Materiales

- Acceso a internet
- Computadora
- Software para virtualización
- Kali Linux
- Herramientas de pentest (open source)

□ Tarea(s) y examen(es)

- Debates y participación para fomentar para el aprendizaje colaborativo y el desarrollo del pensamiento crítico.
- Cuestionarios para medir la comprensión de conceptos teóricos y prácticos
- Prácticas de Laboratorio para que los alumnos adquieran habilidades técnicas y experimenten con herramientas y técnicas de ciberseguridad en un entorno controlado.
- Trabajo Practico Final que integren y apliquen los conocimientos adquiridos a lo largo del curso en un proyecto significativo.

□ Actividades del curso

1. Clases Interactivas: Sesiones dinámicas que incorporan preguntas y respuestas en tiempo real, encuestas interactivas y discusiones abiertas para promover el pensamiento crítico y la participación activa.
2. Sesiones de Debate: Análisis y discusión de estudios de caso reales relacionados con incidentes de ciberseguridad, donde los estudiantes evalúan situaciones, identifican amenazas y proponen soluciones.
3. Prácticas de Laboratorio: Ejercicios prácticos que incluyen la configuración de sistemas seguros, análisis de vulnerabilidades, implementación de protocolos de seguridad y resolución de desafíos técnicos en entornos controlados.
4. Proyectos en Grupo: Desarrollo colaborativo de proyectos que abordan problemas específicos de ciberseguridad, incluyendo talleres de planificación, ejecución y sesiones de revisión por pares para evaluar el progreso y la calidad del trabajo.

□ Cronograma del curso

Semana	Tema	Tipo de Clases	Materiales
1	Fundamentos de Ciberseguridad d y Seguridad de Redes	Clase interactiva. Laboratorio Práctico	KALI Linux
2	Amenazas y Vulnerabilidades en el Entorno Digital	Clase interactiva/ Practica	Base de datos Vulnerabilidad d
3	Protocolos y Arquitecturas de Redes Seguras	Debate/Laboratorio	Software virtualización
4	Criptografía y Mecanismos de Autenticación	Clase Practica	Kali
5	Gestión de Incidentes y Respuesta ante Ciberataques	Clase interactiva	MSAT
6	Seguridad en Aplicaciones y Desarrollo Seguro	Clase Practica/ Laboratorio	OWASP
7	Tendencias Emergentes: Seguridad en la Nube y IoT	Ponencia invitada. Laboratorio Práctico	Honeypot de IBM (altoro)
8	Aspectos Éticos y Legales en Ciberseguridad	Clase interactiva	Material sobre legislación del Paraguay en materia de ciberseguridad

..//..





Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

UNIVERSIDAD NACIONAL DE ASUNCIÓN FACULTAD POLITÉCNICA

ANEXO RESOLUCIÓN Nº 0714/2025

Pág. 6/8

Contenidos del curso

Descripción Semanal Detallada – Curso: Introducción a la ciberseguridad y a la seguridad de redes.

Semana 1: Fundamentos de Ciberseguridad y Seguridad de Redes

Tipo de clase: Clase interactiva/práctica

Objetivo: Comprender los conceptos esenciales de la ciberseguridad y la seguridad de redes, incluyendo su importancia y los principios fundamentales.

Actividades:

- Introducción a la ciberseguridad: definiciones, objetivos y relevancia en el contexto actual.
- Discusión interactiva sobre la tríada CIA (Confidencialidad, Integridad y Disponibilidad) y su aplicación en la protección de la información.
- Ejercicio práctico: análisis de un caso real de vulneración de seguridad y debate sobre las medidas preventivas que podrían haberse implementado.

Materiales:

- Libro: "Seguridad informática" (Buendía, J. F., 2013) – Capítulo 1: Introducción a la seguridad informática.
- Kali Linux
- Presentaciones y recursos adicionales disponibles en la plataforma educativa.

Semana 2: Amenazas y Vulnerabilidades en el Entorno Digital

Tipo de clase: Clase interactiva/práctica

Objetivo: Identificar y analizar las principales amenazas y vulnerabilidades que afectan a los sistemas y redes en el entorno digital.

Actividades:

- Presentación de los diferentes tipos de amenazas cibernéticas, como malware, phishing y ataques de denegación de servicio (DoS).
- Análisis de vulnerabilidades comunes en sistemas operativos y aplicaciones. ❖ Taller práctico: utilización de herramientas de escaneo para detectar vulnerabilidades en un entorno controlado.

Materiales:

- Libro: "Seguridad Informática" (Escrivá, G. R., 2013) – Capítulo 2: Amenazas y vulnerabilidades en sistemas informáticos.
- Flipper Zero
- Artículos y estudios de caso proporcionados en la plataforma educativa.

Semana 3: Protocolos y Arquitecturas de Redes Seguras

Tipo de clase: Debate/Laboratorio

Objetivo: Entender los protocolos de comunicación seguros y las arquitecturas de red diseñadas para minimizar riesgos y proteger la integridad de los datos.

Actividades:

- Debate sobre la importancia de la segmentación de redes y el uso de zonas desmilitarizadas (DMZ) en la seguridad perimetral.
- Laboratorio práctico: configuración de un firewall y establecimiento de reglas de acceso para controlar el tráfico de red.
- Análisis de casos prácticos donde se implementaron arquitecturas de red seguras y discusión sobre su efectividad.

Materiales:

- Libro: "Network Security, Firewalls and VPNs" (Stewart, J. M., 2013) – Capítulo 4: Firewalls y su papel en la seguridad de redes.
- Guías de laboratorio y software de simulación de redes disponibles en la plataforma educativa.

..//..





Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

ANEXO RESOLUCIÓN Nº 0714/2025

Pág. 7/8

Semana 4: Criptografía y Mecanismos de Autenticación

Tipo de clase: Clase práctica

Objetivo: Explorar los fundamentos de la criptografía y los diversos mecanismos de autenticación utilizados para garantizar la seguridad de la información.

Actividades:

- Explicación teórica sobre algoritmos de cifrado simétrico y asimétrico, y su aplicación en la protección de datos.
- Práctica: generación y gestión de claves criptográficas utilizando herramientas específicas.
- Implementación de certificados digitales y configuración de una infraestructura de clave pública (PKI) en un entorno de laboratorio.

Materiales:

- Libro: "Seguridad informática" (Buendía, J. F., 2013) – Capítulo 5: Criptografía y su aplicación en la seguridad de la información.
- Software de criptografía y manuales de usuario disponibles en la plataforma educativa.

Semana 5: Gestión de Incidentes y Respuesta ante Ciberataques

Tipo de clase: Clase interactiva

Objetivo: Desarrollar habilidades para la gestión efectiva de incidentes de seguridad y la respuesta adecuada ante ciberataques.

Actividades:

- Presentación del ciclo de vida de la gestión de incidentes: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.
- Simulación interactiva de un incidente de seguridad y discusión sobre las acciones a tomar en cada fase del proceso.
- Elaboración de un plan de respuesta a incidentes adaptado a un escenario específico.

Materiales:

- Libro: "Gestión de Incidentes de Seguridad Informática" (Vieites, Á. G., 2014) – Capítulo 3 : Procedimientos y técnicas para la gestión de incidentes.
- Plantillas y guías para la elaboración de planes de respuesta a incidentes disponibles en la plataforma educativa.

Semana 6: Seguridad en Aplicaciones y Desarrollo Seguro

Tipo de clase: Clase práctica/Laboratorio

Objetivo: Identificar prácticas de desarrollo seguro y técnicas para asegurar la integridad y confidencialidad en aplicaciones.

Actividades:

- Revisión de las vulnerabilidades más comunes en aplicaciones según el OWASP Top Ten.
- Laboratorio práctico: análisis de código fuente para detectar y corregir vulnerabilidades como inyecciones SQL, cross-site scripting (XSS) y desbordamientos de búfer. ❖ Implementación de controles de seguridad durante el ciclo de vida del desarrollo de software.

Materiales:

- Libro: "Seguridad informática" (Buendía, J. F., 2013) – Capítulo 7: Seguridad en el desarrollo de software.
- Herramienta OWASP
- Herramientas de análisis estático y dinámico de código disponibles en el laboratorio.

Semana 7: Tendencias Emergentes: Seguridad en la Nube y IoT

Tipo de clase: Clase práctica

Objetivo: Analizar los desafíos y soluciones de seguridad en entornos de computación en la nube y en el Internet de las Cosas (IoT).



..//..



UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

Campus de la UNA
SAN LORENZO-PARAGUAY

..//..

ANEXO RESOLUCIÓN N° 0714/2025

Pág. 8/8

Actividades:

- Presentación sobre los conceptos fundamentales de la seguridad en la nube y cómo difiere de la ciberseguridad tradicional.
- Discusión sobre las vulnerabilidades específicas de los dispositivos IoT y las implicaciones de su integración con servicios en la nube.
- Laboratorio práctico: configuración de medidas de seguridad en una plataforma de nube y simulación de ataques a dispositivos IoT para identificar y mitigar riesgos.

Materiales:

- Artículo: "Diferencia entre Ciberseguridad y Seguridad en la Nube" (Web Nephos IT).
- Artículo: "¿Qué es la seguridad de IoT?" (Web Zscaler).
- Plataformas de nube y dispositivos IoT configurados para prácticas en el laboratorio.

Semana 8: Aspectos Éticos y Legales en Ciberseguridad

Tipo de clase: Clase interactiva

Objetivo: Comprender las consideraciones éticas y el marco legal que rige la ciberseguridad, así como la importancia de la integridad profesional y la responsabilidad legal en este campo.

Actividades:

- Análisis de los principales marcos legales relacionados con la ciberseguridad y la protección de datos a nivel nacional e internacional.
- Debate sobre dilemas éticos en ciberseguridad, como el hacking ético y la divulgación responsable de vulnerabilidades.
- Estudio de casos donde se han presentado conflictos éticos y legales en el ámbito de la ciberseguridad.

Materiales:

- Aspectos Legales y Éticos de la Seguridad Informática en Paraguay.
- Documentos legales y códigos de ética profesional disponibles en la plataforma educativa.

Acceso a Materiales:

Todos los recursos del curso estarán centralizados en la plataforma educativa, facilitando un acceso organizado y eficiente. Los materiales disponibles incluirán:

- Lecturas Asignadas: Enlaces directos a capítulos específicos de los libros de texto requeridos, permitiendo una consulta rápida y focalizada.
- Guías Prácticas: Documentos detallados que complementan las lecciones teóricas, diseñados para reforzar y aplicar los conceptos aprendidos.
- Herramientas Recomendadas: Acceso a software y aplicaciones esenciales para las actividades prácticas del curso, con instrucciones claras para su instalación y uso.
- Recursos Adicionales: Enlaces a sitios web de acceso libre, artículos académicos y otros materiales complementarios que enriquecen el aprendizaje y ofrecen perspectivas adicionales.



d