DIPLOMATURA EN CIBERSEGURIDAD APLICADA – Cursada 2026

UTN Facultad Regional La Plata – Formación para la comunidad, Municipios y Empresas

Desde la UTN La Plata, comprometidos con la formación profesional y el desarrollo de capacidades clave en el ámbito tecnológico, presentamos la Diplomatura en Ciberseguridad Aplicada, la cual brindará una formación integral en identificación, análisis y mitigación de amenazas cibernéticas.

1) Requisitos de ingreso y criterios de selección

La diplomatura está dirigida a:

- profesionales, estudiantes y empleados que deseen adquirir una base sólida en ciberseguridad
- administradores de sistemas, analistas de seguridad, desarrolladores y entusiastas de la seguridad informática.

Se requiere contar con los siguientes conocimientos y habilidades básicas:

- arquitectura de computadoras
- programación y base de datos: conocer qué es un lenguaje de programación y qué es una base de datos.
- Sistemas operativos: manejo básico de Linux y Windows
- Habilidades tecnológicas: agilidad en el uso de PC y herramientas básicas.
- Instalación de software: capacidad para instalar programas y configurar entornos de trabajo.

2) Fundamentos y justificación

La ciberseguridad se ha convertido en una necesidad fundamental en todos los sectores, y esta formación busca preparar a los participantes para enfrentar los desafíos actuales en el ciberespacio.

3) Objetivo

- Brindar conocimientos teóricos y prácticos en ciberseguridad
- Desarrollar habilidades esenciales y explotar las habilidades blandas para identificar, analizar y mitigar las amenazas cibernéticas.
- Proporcionar herramientas y metodologías para la protección de sistemas y datos.

- Formar profesionales capaces de aplicar estrategias de ciberseguridad en entornos laborales.

4) Estructura del programa

Este programa está compuesto por cuatro módulos, con una duración total de 160 horas.

Cada módulo aprobado otorga un certificado individual. Los participantes que completen y aprueben los cuatro módulos obtendrán el Certificado Oficial de Diplomatura en Ciberseguridad Aplicada, avalado por la UTN La Plata.

Con este enfoque modular, ofrecemos flexibilidad para que tanto individuos como empresas y municipios puedan capacitar a sus equipos en las áreas más críticas de la seguridad digital.

MODULO I: Seguridad en redes y servicios

Carga horaria: 30 horas.

Descripción: Este módulo está pensado para que el alumno obtenga una visión global en la protección de redes, sistemas de comunicación y servicios, abordando la configuración de firewalls, protocolos seguros (VPN, HTTPS) y detección de intrusiones.

Conocimientos previos: Conceptos básicos de informática y redes. Familiaridad con sistemas operativos (Windows y Linux). Nociones de programación y bases de datos (no excluyente). Estudiantes de carreras de sistemas o afines. Personas con experiencia laboral en informática.

Orden: Primer módulo y obligatorio para avanzar con la diplomatura.

Desarrollo del módulo I:

Redes

Introducción a las redes, Modelo OSI, Topología de red, Dispositivos de red, Modelo TCP/IP. Instalación y configuración de redes.

Potenciales riesgos en redes informáticas: Amenazas y ataques, Servicios de red.

Protocolos: SSL, SSH, PGP.

Métodos HTTP. Cookies, sesiones. Codificación.

Seguridad aplicada a redes informáticas: Dispositivos de seguridad, estructura de una red segura, armado de una red segura.

Servicios

Roles y funciones de un servidor, Instalación y configuración de servidores, Soporte, mantenimiento y solución de problemas

Conceptos de máquinas virtuales, hypervisor. Concepto de contenedores. Contenedores vs. Máquinas Virtuales. Docker.

Configuración segura de hipervisores. Aislamiento de contenedores, control de acceso y auditoria en entornos virtuales.

Configuración de servicios críticos: servidor web, correo, base de datos.

PRÁCTICA: Instalación de Kali Linux en entorno virtual

Hardening

Introducción e implementaciones de seguridad, configuraciones y servicios.

Seguridad aplicada: Potenciales ataques, escaneo de vulnerabilidades y comparación de resultados antes-después.

MODULO II: Fundamentos de Ciberseguridad

Carga horaria: 50 horas.

Descripción: Este módulo proporciona una visión integral de los conceptos fundamentales de ciberseguridad, abarcando amenazas comunes, técnicas de ataque y métodos de defensa. Se introduce a los estudiantes en la detección de ataques, ingeniería social, denegación de servicio, phishing, fuerza bruta, XSS, SQL Injection, análisis de malware, seguridad en redes inalámbricas y dispositivos móviles. Además, se exploran los principios del ethical hacking, criptografía y pentesting, con un enfoque práctico mediante la utilización de herramientas especializadas.

Conocimientos previos: Conceptos básicos de informática y redes. Familiaridad con sistemas operativos (Windows y Linux). Nociones de programación y bases de datos (no excluyente). Estudiantes de carreras de sistemas o afines. Personas con experiencia laboral en informática.

Orden: Aprobar el Módulo I: Seguridad en redes y servicios, o demostrar conocimientos equivalentes mediante evaluación.

Desarrollo del módulo II:

Qué es la ciberseguridad

Amenazas comunes y como reconocerlas: Detección de ataques.

Ingeniería social: ¿qué es? Habilidades técnicas y psicológicas, tipos de ingeniería social. Detección, simulación de ataques, análisis de casos reales.

Denegación de servicio: Dos/DDoS, ¿qué es? Tipos de DoS y DDoS, wireshark, implementación de medidas de firewall, uso de herramientas Hping3 o Slowloris
Phishing: ¿qué es? Tipos, Análisis de email headers, configuración de filtros y reglas de servidores.
Fuerza bruta: ¿qué es? Tipos de FB, implementación de medidas de seguridad (bloqueos, 2FA)
Cross site scripting: (XSS) qué es? Tipos, detectar vulnerabilidades XSS, simulación de ataque con Damn Vulnerable WebApp
SQL injection: ¿qué es? Tipos, SQLmap, detectar y explotar SQLInjection, métodos de defensa.
Malware: introducción al análisis de malware, definición y tipos, detección, ejecución. Análisis dinámico, identificar IOCs
Seguridad Wireless: tipos de ataques que pueden recibir las redes inalámbricas.
Seguridad mobile: tipos de ataques, análisis de aplicaciones, evaluar seguridad de app.

Introducción al ethical hacking: Tareas del ethical hacker, Métodos de control de vulnerabilidades.

Introducción a la criptografía: El abc de la criptografía, Sistemas criptográficos.

Introducción al pentesting: El abc del pentesting, Reconocimiento pasivo/activo, Escaneo de vulnerabilidades.

MODULO III: Gestión de Riesgos y Cumplimiento en Ciberseguridad
Carga horaria: 30 horas.
Descripción: Este módulo aborda la gestión de riesgos y de la seguridad de la información, el cumplimiento normativo y los estándares internacionales (ISO 27001, normas de seguridad en materia de protección de datos personales). Los participantes desarrollarán habilidades para implementar estrategias de mitigación de riesgos y asegurar el cumplimiento de normativas.
Conocimientos previos: Conceptos básicos de informática y redes. Familiaridad con sistemas operativos (Windows y Linux). Nociones de programación y bases de datos (no excluyente). Estudiantes de carreras de sistemas o afines. Personas con experiencia laboral en informática.
Orden: Aprobar el Módulo II: Fundamentos de Ciberseguridad, o demostrar conocimientos equivalentes mediante evaluación.

Desarrollo del módulo III:

Principios de seguridad de la información.

Seguridad informática, seguridad de la información y ciberseguridad.
Política, Estándares y Proceso: Conceptos, contextos, ejemplos.
Estrategia de Ciberseguridad: Planes y programas de ciberseguridad. Ejemplos, etapas, alcances.
Nociones de auditoría, las tres líneas de defensa.
Instituciones que emiten estándares y marcos internacionales: Temas y objetivos.
Gestión de Riesgos: Conceptos relacionados, tolerancia, capacidad, metodologías, ejemplos.
Gobierno de Seguridad de la Información. Principios, responsabilidades, alcances Gestión de la Seguridad de la información.
Estándares, SGSI, PDCA, ISO 27001:2022, ISO27002:2022, Controles CIS. Framework NIST.
Introducción a la protección de datos personales. Resolución AAIP 47/2018. Seguridad de la Información en protección de datos personales.
Introducción a la gestión de incidentes de ciberseguridad. (en profundidad en el siguiente módulo)
Perfiles en ciberseguridad

CISO, CSO, CTO, Gobierno de la ciberseguridad, Asesoría legal y cumplimiento, Seguridad informática, Auditoría de ciberseguridad.

MODULO IV: Respuesta a Incidentes y Análisis Forense Digital
Carga horaria: 50 horas.
Descripción: Este módulo brinda los conocimientos teóricos y prácticos fundamentales para gestionar incidentes de ciberseguridad y realizar análisis forense digital. Se abordan técnicas y metodologías utilizadas en la respuesta a incidentes, desde la detección hasta la recuperación y la revisión posterior, incluyendo el uso de tecnologías avanzadas como EDR, SIEM y SOAR. También se estudia la informática forense, cubriendo desde la recolección y preservación de evidencia digital hasta su análisis y presentación en informes técnicos.
Conocimientos previos: Conceptos básicos de informática y redes. Familiaridad con sistemas operativos (Windows y Linux). Nociones de

programación y bases de datos (no excluyente). Estudiantes de carreras de sistemas o afines. Personas con experiencia laboral en informática y análisis forense.

Orden: Aprobar el Módulo III: Gestión de Riesgos y cumplimiento en Ciberseguridad, o demostrar conocimientos equivalentes mediante evaluación.

Desarrollo del módulo IV:

Definición de Respuesta a Incidentes de Ciberseguridad

Definición de Incidentes de Ciberseguridad. Ransomware. Phishing e Ingeniería Social. DDoS. Ataques a la cadena de suministros. Amenazas internas. Ataques de escalada de privilegios. MITM.

Planificación de la Respuesta a Incidentes.

Funcionamiento de la Respuesta a Incidentes. Preparación. Detección y Análisis. Contención. Erradicación. Recuperación. Revisión posterior al incidente.

Tecnologías de respuesta a incidentes. ASM (Gestión de la superficie de ataque). EDR (Detección y respuesta de endpoints). SIEM (Gestión de eventos e información de seguridad). SOAR (Orquestación de seguridad, automatización y respuesta). UEBA (Análisis del comportamiento de usuarios y entidades). XDR (Detección y respuesta ampliadas)

Inteligencia Artificial y respuesta a incidentes de ciberseguridad

Vulnerabilidad. Amenaza. Incidente de Seguridad. Ejemplos.
Seguridad de la Información. Triángulo CIA. Ejemplos de ataques que afectan Disponibilidad, Integridad, Confiabilidad.
Ciberataques. Ejemplo: Stutnex.

Definición de Gestión de Incidentes. Ejemplos de malas gestiones de incidentes.

Concepto de Informática Forense: Evidencia Digital. Cadena de Custodia. DFIR: análisis forense digital y respuesta a incidentes.

Fases del proceso de investigación forense digital.

Fase de Recolección: Relevamiento inicial. Admisión del caso. Valoración de la evidencia. Escena del crimen. Fuentes de información: computadora, componentes, memorias, dispositivos de control de acceso, cámaras digitales,

discos duros (internos y externos), tarjetas de memoria, impresoras y scanners, medios extraíbles, unidades flash, dispositivos portátiles, periféricos, redes de computadoras.

Fase de Examen: Adquisición de Discos: duplicador de disco, bloqueador de escritura, tipos de imágenes de disco, identificación de discos, copia forense. Forensia en vivo. Adquisición de Memoria. Adquisición de una Máquina Virtual. Captura de tráfico de red. Conceptos de Unidades, Particiones, MBR, GPT, Sistemas de Archivos.

Fase de Análisis: Definición de Artefacto Forense. Definiciones de Timestamp (MACB time), File Carving, Timeline. Herramientas para análisis forense.

Fase de Reporte: Redacción del informe. Tipos de informes.

5) Modalidad de cursado

Virtual, utilizando las herramientas de conectividad propuestas por la UTN y herramientas open source.

6) Criterios de evaluación

Cada módulo será evaluado de manera independiente. Al aprobar un módulo, el participante recibirá el certificado de aprobación de este. Al finalizar los 4 módulos, el participante recibirá el Certificado Oficial de Diplomatura en Ciberseguridad Aplicada.

7) Directores académicos, docentes y ayudantes

7.1 Directora:

Ing. Alejandra Lavore Bourg

Ing. Alejandra Lavore Bourg. Ingeniera en Sistemas de Información recibida de la Universidad Tecnológica Nacional, Regional La Plata (UTN-FRLP). Maestrando en Ciberdefensa y Ciberseguridad en la Universidad de Buenos Aires (UBA). Especialista en Ciberseguridad, Pentesting y Ethical Hacking. Vicepresidenta del Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires (CPCIBA). Docente Universitaria en la carrera de Ingeniería en Sistemas de Información, en las materias Análisis de Sistemas de Información y Seguridad en Sistemas de Información de la UTN-FRLP. Coordinadora del equipo de Gestión e Investigación en Ciberseguridad (GIC) y semillero de

ciberseguridad, perteneciente al laboratorio de investigación, desarrollo y aplicación de tecnologías innovadoras LINES UTN-FRLP. Coordinadora del laboratorio abierto de ciberseguridad de la UTN-FRLP. Actualmente brindando conocimientos y servicios en el Poder Judicial de la Nación en el Juzgado Federal N° 1 La Plata.
Ganadora del premio CyberWomen Challenge Argentina 2020
Ganadora del premio internacional CyberWomen Challenge Regional 2021
Reconocimiento como profesional destacada del año FEPUBA 2024

7.2 Docentes:

Ing. Marcela Pallero

Ingeniera en sistemas de información por la Universidad Tecnológica Nacional (UTN), Especialista en criptografía y seguridad teleinformática por la Escuela Superior Técnica del Ejército y profesora en el Instituto del Profesorado técnico, UTN. Diplomado en Derecho informático en la UBA. Trabajó en delitos informáticos en la Policía Federal Argentina, en el equipo de respuesta a incidentes de seguridad de gobierno, ArCERT fue el equipo de Respuesta ante incidentes del Sector Público Nacional, en la Autoridad Nacional de Firma Digital en ONTI y como Analista en el Banco Central de la República Argentina en la Gerencia de Seguridad de la información. En la actualidad es Directora del Programa Seguridad en TIC de la Fundación Manuel Sadosky de Argentina. Docente de Ciberseguridad en el Programa Derecho en Tecnologías Digitales en CETyS (Centro de Estudios en Tecnología y Sociedad) de la Universidad de San Andrés y en la Escuela de Innovación del ITBA. Miembro revisor de trabajos del Simposio Argentino de Ciberseguridad y Ciberdefensa en las 53 Jornadas Argentinas de Informática JAIIO 2024, 2025 y en las VII Edición de Argencon 2024. IEEE de Argentina, en el track de Ciberseguridad y Ciberdefensa.

Ing. Sandra Mariela Zilla

Ingeniera en Sistemas de Información, Magíster en Redes de Datos y especialista en Ciberseguridad con una sólida trayectoria en el ámbito público y privado. Actualmente se desempeña como Analista Forense Digital, y es docente en las cátedras de "Desarrollo Seguro de Aplicaciones" e "Introducción a la Forensia Digital" en la Facultad de Informática de la UNLP.

Cuenta con certificaciones internacionales como ISO/IEC 27032 Lead Cybersecurity Manager e ISO/IEC 27035 Lead Incident Manager, y una extensa experiencia en auditoría tecnológica, seguridad en la nube, investigación de delitos informáticos y concientización en ciberseguridad. Ha coordinado equipos técnicos y proyectos vinculados a la protección de infraestructuras críticas, ha sido expositora en eventos nacionales e internacionales, y ha brindado capacitaciones a fuerzas de seguridad.

Con una firme vocación docente e investigadora, Sandra integra espacios de formación y divulgación sobre ingeniería social, OSINT, análisis forense y cultura de la ciberseguridad, aportando una mirada integral, técnica y humana a la disciplina.

Ing. Ariel Ferreyra

Ingeniero en Sistemas de Información (UTN). Director de Investigaciones Criminales en Subsecretaría de Inteligencia Criminal del Ministerio de Seguridad Bs. As. Perito informático de la SCJBA en Ministerio Público Bs.As. Docente en IUV (Instituto Universitario Vucetich): “Introducción a la Inteligencia Artificial”, "Tecnologías aplicadas a la Investigación Criminal" y "Análisis de los Sistemas de Comunicaciones". Director de la Diplomatura universitaria en Gestión de la información para la Investigación.

Director y docente de los cursos “Introducción a la Informática Forense”, “Inteligencia en Fuentes Abiertas (OSINT)” e “Ingeniería Social para la Investigación Criminal” del Centro de Altos Estudios y Especialidades Policiales (CAEEP).

Ex docente e investigador en UTN Facultad Regional Trenque Lauquen.

8) Cronograma de clases

Martes y jueves: clases virtual sincrónico y clases asincrónicas. Dependiendo el módulo se enviará el cronograma del mismo.

9) Fecha de inicio.

Inicio: martes 7 de abril 2026.
Horario: de 18 a 21 virtual.

10) Precio de la Diplomatura y formas de pago

- **Terceros**: $ 750.000,- en un pago. O 4 cuotas de $ 250.000.-
- **Graduados UTN y Docentes UTN**: 30% descuento: $ 525.000,- En un pago. O 4 cuotas de $ 175.000,-
- **Alumnos UTN**: 50% descuento: $ 375.000,- En un pago. O 4 cuotas de $ 125.000,-

11) Inscripción

Si has leído todo lo anterior, y estás de acuerdo en hacer la Diplomatura, te pedimos que te anotes en el siguiente formulario:

https://forms.office.com/r/74ykv4Gecm?origin=lprLink

Luego recibirás un correo con información de la documentación que deberás enviarnos, básicamente será un documento leído y firmado (Acta de Compromiso del Alumno), y el comprobante de pago. Para esto último te enviaremos un link de pagos que deberás abonar el monto correspondiente a la 1° cuota. En caso que optes por el pago contado, el resto lo abonarás durante el mes de abril de 2026, se congelará el valor.