Resolución de Consejo Directivo **829 / 2026 - EXA -UNSa**
EXP. 170/2022 Dr. Sergio ROCABADO MORENO eleva Programa Analítico y Régimen de Regularidad y Promoción de la Asignatura OPTATIVA III: CIBERSEGURIDAD de Licenciatura en Análisis de Sistemas, Plan 2010
**De: EXACTAS-Secretaria Académica y de Investigación**

Salta, 02/11/2026

VISTO: La nota presentada por el Dr. Sergio ROCABADO MORENO mediante la cual solicita la aprobación del Programa Analítico y Régimen de Regularidad y Promoción de la asignatura OPTATIVA III: CIBERSEGURIDAD de la carrera Licenciatura en Análisis de Sistemas Plan 2010, y

CONSIDERANDO:

Que la Comisión de Carrera de la Licenciatura en Análisis de Sistemas y el Departamento de Informática emiten opinión favorable para la aprobación del Programa Analítico y del Régimen de Regularidad y Promoción.

Que la Comisión de Docencia e Investigación aconseja aprobar el Programa Analítico y el Régimen de Regularidad y Promoción.

Que la RCD 32/2026 EXA-UNSa dispone un formato único para la presentación de los programas de cada una de las asignaturas de las carreras que se dictan en esta Unidad Académica.

Que el Consejo Directivo, en su 18° Sesión Ordinaria realizada el 21 de octubre de 2026, aprobó el despacho de la Comisión de Docencia e Investigación.

Que, el Estatuto de la Universidad Nacional de Salta en el Artículo 117 inciso 8, establece que "*entre los deberes y atribuciones que le confiere al Consejo Directivo, incluye aprobar los programas Analíticos y la reglamentación sobre el régimen de regularidad y promoción propuesto por los módulos Académicos*".

Por ello,

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS

R E S U E L V E:

ARTÍCULO 1°.- Aprobar el Programa Analítico, Régimen de Regularidad y Promoción de la asignatura OPTATIVA III: CIBERSEGURIDAD de la Carrera Licenciatura en Análisis de Sistemas (Plan 2010), que como Anexo forma parte integrante de la presente Resolución.

ARTÍCULO 2°.- Notifíquese al Dr. Sergio ROCABADO MORENO, docente responsable de la asignatura OPTATIVA III: CIBERSEGURIDAD. Comuníquese a las Autoridades y Secretarías de esta Unidad Académica, a la Comisión de Carrera de Licenciatura en Análisis de Sistemas, al Departamento de Informática, a la Dirección de Mesa de Entradas, Archivo y Digesto y a la Dirección de Alumnos para su toma de conocimiento, registro y demás efectos. Publíquese en el Boletín Oficial y en la Página WEB de la Facultad. Cumplido, archívese.

MFL

FACULTAD DE CIENCIAS EXACTAS UNSa

LIC. MARCELA F. LÓPEZ
SECRETARIA ACADÉMICA Y DE INVESTIGACIÓN
FACULTAD DE CS. EXACTAS - UNSa

UNIVERSIDAD NACIONAL DE SALTA Facultad Cs. Exactas

Dr. JOSÉ RAMÓN MOLINA
DECANO
FACULTAD DE CS. EXACTAS - UNSa

# PROGRAMA ANALÍTICO Y RÉGIMEN DE REGULARIDAD

1. **Departamento Docente:** Departamento de Informática
2. **Cátedra:** No corresponde.
3. **Asignatura:** Optativa III – CIBERSEGURIDAD.
4. **Carrera:** Licenciatura en Análisis de Sistemas (Plan de estudios 2010, resolución CS N° 262/2012).
5. **Último programa vigente:** 2024 (RCD-712-2024-EXA-UNSa)
6. **Equipo Docente.**

   Profesor Responsable: Dr. Sergio Hernán Rocabado Moreno

   Docente Auxiliar: C.U. Miguel Aguirre

7. **Ubicación en el plan de estudios.**

   Se dicta en el segundo cuatrimestre de quinto año de la Carrera Licenciatura en Análisis de Sistemas, plan de estudios 2010.

   Carga horaria total: 120 horas, distribuidas en 60 horas de teoría y 60 horas de práctica.

   Carga horaria semanal: 8 horas semanales, distribuidas en 4 horas de teoría y 4 horas de práctica.

8. **Contenidos mínimos.**

   En concordancia con lo establecido para las asignaturas optativas en el plan de estudios 2010, el presente programa define los contenidos mínimos de la asignatura Optativa III - Ciberseguridad.

   A continuación, se presentan los contenidos mínimos establecidos y su correspondencia con las unidades en las que se desarrollan, a fin de evidenciar su adecuada cobertura.

| | |
|---|---|
| Fundamentos de seguridad y ciberseguridad | Unidad 1 |
| Gestión de riesgos, amenazas y vulnerabilidades | Unidad 1 |
| Ciberataques y contramedidas | Unidad 1 |
| Normas y estándares | Unidad 1 |
| Confidencialidad, integridad y disponibilidad | Unidad 2 |
| Control de acceso, autenticación y auditoría | Unidad 2 |
| Seguridad de infraestructura | Unidad 3 |
| Seguridad en entornos virtualizados | Unidad 3 |
| Seguridad de sistemas operativos | Unidad 4 |
| Seguridad de redes | Unidad 5 |
| Protocolos seguros | Unidad 5 |
| Criptografía | Unidad 5 |
| Infraestructura de clave pública y certificados digitales | Unidad 5 |
| Análisis de vulnerabilidades y pruebas de penetración | Unidad 6 |
| Migración, contención y recuperación ante incidentes | Unidad 6 |

FACULTAD DE CIENCIAS EXACTAS UNSa

## 9. Correlatividades.

Para cursar la asignatura, se debe tener regularizada la asignatura Redes de Computadoras II y aprobadas las asignaturas Sistemas Operativos, Sistemas de Información y Bases de Datos II.
Para rendir el examen final de la asignatura, se deben tener aprobadas las asignaturas Teoría de la Computación III y Redes de Computadoras II.

## 10. Justificación.

### 10.1 Fundamentación de la asignatura.

La asignatura se incorpora en el plan de estudios de la Licenciatura en Análisis de Sistemas ante la creciente necesidad de fortalecer la protección de activos informáticos e infraestructuras tecnológicas en entornos organizacionales interconectados.

El incremento de la exposición de los sistemas a amenazas y vulnerabilidades informáticas impacta en la confidencialidad, integridad y disponibilidad de la información, afectando la continuidad operativa de los servicios tecnológicos. En este contexto, se reconoce la relevancia de incorporar conocimientos vinculados a la seguridad informática desde una perspectiva técnica orientada al análisis de amenazas, la identificación de vulnerabilidades y la aplicación de mecanismos de protección.

La formación propuesta busca complementar el perfil del Licenciado en Análisis de Sistemas mediante el desarrollo de competencias vinculadas a la ciberseguridad, que incluyen el análisis de entornos tecnológicos, la identificación de riesgos y vulnerabilidades, y la aplicación de controles y herramientas de seguridad en escenarios controlados de práctica, en el marco de normas y estándares internacionales de la especialidad.

### 10.2 Articulación académica.

- Articulación vertical anterior: Se vincula con asignaturas de formación básica y tecnológica, particularmente con redes de computadoras, sistemas operativos y bases de datos, que proporcionan los conocimientos necesarios para comprender el funcionamiento de las infraestructuras tecnológicas sobre las que se aplican los mecanismos de seguridad. Además, aprovecha los contenidos de la asignatura Derecho informático, que permiten comprender los aspectos legales vinculados a la protección de la información, la privacidad y los delitos informáticos.
- Articulación vertical posterior: No corresponde, la asignatura se dicta en el último cuatrimestre de la carrera.
- Articulación horizontal: Se integra con la asignatura Administración de Proyectos Informáticos, en la cual se promueve la incorporación de prácticas de gestión que consideren la seguridad como un componente transversal en el desarrollo e implementación de sistemas. Asimismo, se vincula con el Seminario de Sistemas, instancia en la que los estudiantes realizan el análisis y diseño de un sistema de información, pudiendo incorporar criterios y buenas prácticas de seguridad a lo largo de las distintas etapas del desarrollo.

### 10.3 Aporte al perfil profesional.

La asignatura contribuye a los siguientes alcances del título de Licenciado en Análisis de Sistemas establecidos en el plan de estudios:

- Elaboración de métodos y normas relativos a la seguridad y privacidad de la información procesada y/o generada por los sistemas de información. Participación en la determinación de acciones a seguir en esta materia y en la evaluación de sus aplicaciones. - Elaboración de métodos y normas referentes a la salvaguarda y control de los recursos físicos y lógicos de un sistema de computación.

FACULTAD DE CIENCIAS EXACTAS UNSa

- Determinación y control del cumplimiento de pautas técnicas que rigen el funcionamiento y la utilización de recursos informáticos en cada información.
- Arbitrajes, pericias y tasaciones judiciales y extrajudiciales referidas a los sistemas de información y a los medios de procesamiento de datos.
- Auditorías en Áreas de Sistemas y Centros de Cómputos, así como de los sistemas de información utilizados.

### 10.4 Ejes transversales abordados.

ET01 – Identificación, formulación y resolución de problemas de informática — ALTO
ET04 – Utilización de técnicas y herramientas de aplicación en la informática — MEDIO
ET06 – Fundamentos para el desempeño en equipos de trabajo — MEDIO
ET08 – Fundamentos para la acción ética y responsable — MEDIO ET10 – Fundamentos para el aprendizaje continuo — MEDIO

## 11. Objetivos generales.

Al finalizar la asignatura, el estudiante será capaz de:

- Analizar los fundamentos de la ciberseguridad y aplicar buenas prácticas para el uso seguro de las tecnologías de la información.
- Identificar y evaluar riesgos, amenazas, vulnerabilidades e incidentes de seguridad en distintos entornos tecnológicos y organizacionales.
- Seleccionar mecanismos y herramientas de seguridad informática para la protección de activos digitales, considerando normas y estándares de ciberseguridad.
- Implementar medidas de protección y mitigación para resguardar infraestructuras, sistemas, redes y servicios que procesan, almacenan o transmiten información digital.
- Desarrollar actividades prácticas integradoras orientadas a la resolución de problemas de ciberseguridad, tanto en forma individual como grupal, comunicando y fundamentando técnicamente las soluciones y resultados obtenidos.

## 12. Programa analítico:

### Unidad 1.- Introducción.

**Objetivos específicos:**

- Analizar los elementos fundamentales de la seguridad, considerando activos, vulnerabilidades, amenazas, riesgos e impactos asociados.
- Identificar conceptos fundamentales de ciberseguridad, incluyendo ciberamenazas, ciberataques y ciberdelitos.
- Reconocer tipos de ataques, técnicas utilizadas y contramedidas orientadas a la protección de activos digitales.
- Describir el rol de los equipos de respuesta a incidentes en la gestión y recuperación ante incidentes de seguridad.
- Identificar normas, estándares y marcos de referencia de ciberseguridad, reconociendo su importancia en la gestión de la seguridad y el cumplimiento normativo.

**Contenidos:** Seguridad. Activo. Vulnerabilidad. Amenaza. Ataque. Riesgo. Evaluación y gestión. Impacto. Ciberespacio. Ciberseguridad. Ciberamenaza. Ciberataques. Ciberdelitos. Ciberdelincuencia. Consecuencias. Técnicas utilizadas. Contramedidas. Gestión de la Ciberseguridad. Equipos de Respuesta a Incidentes de Seguridad. Normas y estándares. Legislación y regulaciones. Introducción a marcos de referencia: ISO/IEC 27001, NIST Cybersecurity Framework y normativas locales. Ética y responsabilidad profesional en el ciberespacio.



FACULTAD DE CIENCIAS EXACTAS UNSa

**Unidad 2.- Fundamentos de ciberseguridad.**

**Objetivos específicos:**

- Analizar los principios de confidencialidad, integridad y disponibilidad y su importancia en la protección de la información.
- Identificar y diferenciar mecanismos de identificación, autenticación, autorización, auditoría y control de acceso utilizados en sistemas informáticos.
- Reconocer mecanismos de no repudio, privacidad y anonimato aplicados a la protección de la información y las comunicaciones.
- Aplicar buenas prácticas de ciberseguridad orientadas a la protección de la información y al uso seguro de los sistemas informáticos.

**Contenidos:** Confidencialidad, Integridad y Disponibilidad. Identificación. Autenticidad y autenticación. No repudio. Autorización y Auditoría. Control de acceso. Privacidad y anonimato. Buenas prácticas.

**Unidad 3.- Seguridad de infraestructura**

**Objetivos específicos:**

- Identificar riesgos asociados a la infraestructura física y ambiental de los sistemas informáticos.
- Detectar y analizar vulnerabilidades en servidores, end points y dispositivos conectados.
- Aplicar principios y medidas de seguridad en entornos virtualizados y contenedores.
- Implementar medidas de protección orientadas a fortalecer la seguridad y continuidad de las infraestructuras tecnológicas.

**Contenidos:** Seguridad física y ambiental. Seguridad en servidores y redundancia. Seguridad en end points: estaciones de trabajo y dispositivos móviles. Seguridad en entornos virtualizados y contenedores. Estrategias de recuperación ante fallas y continuidad del servicio.

**Unidad 4.- Seguridad y protección de sistemas operativos.**

**Objetivos específicos:**

- Identificar y evaluar vulnerabilidades en sistemas operativos.
- Aplicar estrategias de mitigación orientadas a la reducción de vulnerabilidades en sistemas operativos.
- Implementar políticas de gestión de parches y actualizaciones para el mantenimiento seguro de los sistemas.
- Aplicar mecanismos de control de acceso y administración de permisos para proteger la información.
- Implementar estrategias de backup, recuperación y restauración de sistemas para garantizar la disponibilidad de la información.
- Aplicar técnicas de hardening y configuración segura de sistemas operativos para fortalecerlos frente a posibles ataques.

**Contenidos:** Protección y reducción de vulnerabilidades en sistemas operativos. Gestión de parches y actualizaciones. Controles de acceso y administración de permisos. Estrategias de backup, recuperación y restauración de sistemas. Hardening y configuración segura de sistemas operativos.

FACULTAD DE CIENCIAS EXACTAS UNSa

**Unidad 5.- Seguridad en redes, comunicaciones y criptografía.**

**Objetivos específicos:**

- Aplicar principios de criptografía simétrica y asimétrica, así como funciones hash, para la protección de la información.
- Configurar e implementar protocolos seguros para garantizar la seguridad de las comunicaciones.
- Implementar infraestructura de clave pública, certificados digitales y firma digital para garantizar autenticidad, integridad y confidencialidad de la información.
- Gestionar mecanismos de seguridad en redes, incluyendo firewalls, IDS/IPS, VPN para proteger las comunicaciones frente a ciberataques.
- Aplicar medidas de seguridad en redes inalámbricas para la protección de las comunicaciones.

**Contenidos:** Criptografía simétrica y asimétrica. Funciones hash. Protocolos seguros: SSL/TLS. Infraestructura de clave pública (PKI), certificados y firmas digitales. Seguridad en redes y comunicaciones: firewalls, IDS/IPS, VPN. Seguridad en redes inalámbricas.

**Unidad 6.- Análisis de vulnerabilidades y pruebas de penetración.**

**Objetivos específicos:**

- Detectar y priorizar vulnerabilidades en aplicaciones, sistemas operativos y redes.
- Aplicar herramientas y técnicas de análisis de vulnerabilidades para la identificación de fallas de seguridad.
- Ejecutar pruebas de penetración utilizando metodologías y herramientas específicas, respetando principios éticos y marcos legales vigentes.
- Diseñar estrategias de mitigación, contención y recuperación ante incidentes de seguridad.

**Contenidos:** Análisis de vulnerabilidades: identificación, clasificación y priorización. Herramientas y técnicas de análisis. Pruebas de penetración: fundamentos y metodologías. Aspectos legales. Estrategias de mitigación, contención y recuperación ante incidentes.

## 13. Programa de Trabajos Prácticos.

| TP | Temas que aborda | Objetivo | Unidad | Clases estimadas |
|---|---|---|---|---|
| 1 | Gestión del riesgo | Identificar activos de información, analizar vulnerabilidades potenciales y realizar una evaluación básica de riesgos junto con posibles medidas de mitigación. | 1 | clases 01-02 |
| 2 | Ciberataques | Analizar el funcionamiento de ataques informáticos mediante la explotación controlada de vulnerabilidades en entornos de prueba. | 1 | clases 03-04 |
| 3 | Sniffing y análisis de vulnerabilidades en comunicaciones | Capturar y analizar tráfico de red mediante herramientas de monitoreo para identificar información transmitida sin cifrado y posibles vulnerabilidades en las comunicaciones. | 1 | clases 05 |
| 4 | Gestión de identidades y autenticación en sistemas Linux | Implementar mecanismos de control de acceso en sistemas Linux mediante gestión de usuarios, autenticación basada en clave pública y autenticación multifactor (2FA), evaluando su impacto en la protección frente a accesos no autorizados. | 2 | clases 06-07 |

| | | | | |
|---|---|---|---|---|
| 5 | Confidencialidad y cifrado | Implementar contenedores cifrados para la protección de información sensible y evaluar su uso en escenarios de producción. | 2 | Clases 08 |
| 6 | Seguridad en servidores | Implementar configuraciones RAID y analizar su impacto en la disponibilidad de la información como componente de la seguridad y la continuidad de los sistemas. | 3 | Clases 09-10 |
| 7 | Hardening | Aplicar técnicas de hardening en sistemas Linux, para reducir la superficie de ataque, mejorar la configuración segura del sistema e implementar mecanismos básicos de monitoreo y registro de eventos de seguridad. | 4 | Clases 11-13 |
| 8 | Protocolos seguros | Configurar servicios de comunicación seguros mediante HTTPS (HTTP over TLS) y SFTP/FTPS, utilizando certificados | 5 | Clases 14-17 |
| | | digitales para garantizar la confidencialidad e integridad de las comunicaciones. | | |
| 9 | Firma Digital | Aplicar mecanismos de firma digital mediante certificados digitales y analizar sus diferencias con la firma electrónica, evaluando sus propiedades de autenticidad, integridad y no repudio. | 5 | Clases 18-20 |
| 10 | Firewall | Diseñar e implementar políticas básicas de filtrado de tráfico mediante un firewall, configurando zonas de red (LAN y DMZ) para segmentar y proteger las comunicaciones. | 5 | Clases 21-22 |
| 11 | OpenVPN | Configurar una VPN mediante autenticación basada en certificados y contraseñas para establecer túneles seguros de comunicación. | 5 | Clases 23-24 |
| 12 | Seguridad en redes inalámbricas | Configurar y asegurar redes inalámbricas mediante la implementación de mecanismos de autenticación, cifrado (WPA2/WPA3) y control de acceso, para mitigar vulnerabilidades en entornos Wi-Fi | 5 | Clases 25-26 |
| 13 | Test de penetración | Realizar pruebas de penetración controladas siguiendo una metodología básica de pentesting que incluya reconocimiento, escaneo y explotación controlada, con el fin de identificar vulnerabilidades y proponer medidas de mitigación. | 6 | Clases 27-30 |

## 14. Laboratorios.

La asignatura no incluye prácticas de laboratorio en el sentido experimental característico de las ciencias naturales o de la salud. Sin embargo, se desarrollan actividades prácticas en el aula y en entornos informáticos, que permiten aplicar y reforzar los contenidos teóricos.

## 15. Estrategias de enseñanza.

El dictado de la asignatura combina exposiciones teóricas con actividades prácticas. Las clases teóricas brindan a los estudiantes los conocimientos necesarios para su posterior aplicación en los trabajos prácticos.

Para la presentación de los contenidos se utilizan técnicas visuales, como diapositivas y pizarrón, que facilitan un desarrollo lógico y dinámico de cada tema, estableciendo vínculos con contenidos previos y finalizando con una síntesis de los conceptos abordados. Durante las clases se plantean preguntas a los estudiantes para promover su participación activa y favorecer la comprensión y el análisis de los contenidos.

FACULTAD DE CIENCIAS EXACTAS UNSa

Dado el carácter aplicado de la asignatura, los docentes realizan demostraciones prácticas mediante una computadora conectada a proyector, mostrando el uso de herramientas específicas y la configuración de servicios o mecanismos de seguridad. Estas demostraciones permiten a los estudiantes observar procedimientos técnicos y metodologías que posteriormente replican en las actividades prácticas, desarrollando habilidades de análisis, resolución de problemas y aplicación de conocimientos en contextos simulados. Se incorporan herramientas basadas en inteligencia artificial para apoyar la preparación y automatización de entornos de prueba utilizados en dichas actividades.

Los trabajos prácticos se desarrollan bajo supervisión docente, asegurando la correcta aplicación de los conocimientos teóricos. En estas instancias se promueve además el trabajo colaborativo, la interpretación de resultados y la elaboración de informes técnicos fundamentados, favoreciendo la comunicación técnica y la integración de conocimientos.

## 16. Estrategias de evaluación.

La evaluación se realiza mediante diversos instrumentos que permiten valorar tanto la comprensión conceptual como la capacidad de aplicación de los contenidos.

En este marco, se implementan evaluaciones parciales escritas y trabajos prácticos orientados a la resolución de problemas y al uso de herramientas tecnológicas, tales como la virtualización aplicada a la implementación de entornos de prueba, a la simulación de escenarios de ataque y defensa, y a la validación de mecanismos de seguridad.

Los trabajos prácticos se desarrollan en modalidad grupal e incluyen la elaboración de informes técnicos. En el caso de los trabajos integradores, se contempla además una instancia de defensa oral destinada a evaluar el conocimiento de los contenidos, así como la capacidad de argumentación y fundamentación técnica por parte de los estudiantes.

Estas instancias permiten verificar el logro de las capacidades previstas en la asignatura mediante evidencias de desempeño vinculadas con el análisis de vulnerabilidades, la implementación de mecanismos de seguridad, la resolución de problemas, la aplicación de buenas prácticas de ciberseguridad y el uso ético y responsable de las herramientas y técnicas utilizadas.

## 17. Recursos materiales.

Para el desarrollo de la asignatura se requiere un gabinete de informática con computadoras conectadas a internet, proyector, pizarrón y acceso a un curso en línea de la Facultad, el cual posibilita la interacción con los estudiantes a través de foros, la publicación de materiales (contenidos, reglamento interno, diapositivas, apuntes teóricos y trabajos prácticos) y el seguimiento de las actividades de cada estudiante.

Se utiliza software de libre distribución para la implementación de escenarios de práctica virtualizados. También se emplean herramientas basadas en inteligencia artificial, incluyendo modelos de lenguaje (LLMs), como apoyo para la configuración y el análisis de los entornos de práctica.

Estos recursos se complementan con la bibliografía específica de la asignatura.

## 18. Condiciones para regularizar.

a) Asistencia: asistencia mínima del 80 % a las clases prácticas.

b) Aprobación de Trabajos Prácticos: presentación y aprobación de la totalidad de los trabajos prácticos requeridos.

FACULTAD DE CIENCIAS EXACTAS UNSa

c) Aprobación de Laboratorios: no corresponde, dado que la asignatura no contempla prácticas de laboratorio en sentido experimental.

d) Aprobación de Parciales: aprobación de dos evaluaciones parciales con una calificación mínima de 60 puntos sobre 100, cada una con su correspondiente instancia de recuperación.

## 19. Condiciones para acreditar

La asignatura se aprueba mediante examen final. La calificación mínima de aprobación es de 4 (cuatro) puntos sobre 10 (diez).

En el examen final, el estudiante regular es evaluado mediante la resolución de un caso de estudio de ciberseguridad, en el cual deberá proponer, desarrollar y fundamentar una estrategia de solución técnica, así como exponer los fundamentos teóricos involucrados en su resolución.

El estudiante libre deberá aprobar una evaluación práctica integradora orientada a verificar conocimientos, habilidades y desempeños equivalentes a los requeridos para la regularización de la asignatura, incluyendo la resolución de problemas y la aplicación de contenidos prácticos. Una vez superada, accederá a una instancia de características equivalentes a la aplicada a los estudiantes regulares.

## 20. Bibliografía

**20.1 Bibliografía especifica:** - Brooks, C. J. (2018). *Cybersecurity essentials* (1st ed.). John Wiley & Sons. https://doi.org/10.1002/9781119362395

- Pinchao, R., Hernández, C., Macías, R., & Gesicap, Ediciones. (2025). *Fundamentos de seguridad informática y ciberseguridad* (ISBN 978-9942-62625-7).

**20.2 Bibliografía general o ampliatoria:**

- McNab, C. (2017). *Network security assessment* (3rd ed.). O'Reilly. https://doi.org/10.1002/9781491910955
- Roa Buendía, J. F. (2013). *Seguridad informática* (2nd ed.). McGraw-Hill.
- Rocabado, S. (2014). *Caso de estudio de comunicaciones seguras sobre redes móviles ad hoc.* UNLP. https://doi.org/10.35537/10915/33571
- Stallings, W., & Brown, L. (2023). *Computer security: Principles and practice* (5th ed.). Pearson. https://doi.org/10.1002/9780138091712
- Tevault, D. A. (2018). *Linux security and hardening.* Packt Publishing. https://doi.org/10.1002/9781788620307

FACULTAD DE CIENCIAS EXACTAS UNSa

LIC. MARCELA F. LÓPEZ
SECRETARIA ACADÉMICA Y DE INVESTIGACIÓN
FACULTAD DE CS. EXACTAS - UNSa

UNIVERSIDAD NACIONAL DE SALTA Facultad Cs. Exactas

Dr. JOSÉ RAMÓN MOLINA
DECANO
FACULTAD DE CS. EXACTAS - UNSa