Seguridad Informática

Planificación Ciclo lectivo 2026

1. Datos administrativos de la asignatura			
Departamento:	Sistemas de Información	Carrera	Ing. en Sistemas de Información
Asignatura:	**Seguridad Informática**		
Nivel de la carrera	5to Año	Duración	Cuatrimestral
Plan	2023 Ord. 1877	Modalidad	Presencial
Bloque Curricular:	Ciencias y Tecnologías Complementarias		
Área	Computación y Comunicación de Datos	RTF	
Horas cátedra semanal:	3	Horas reloj anual total:	72
Carga horaria no presencial semanal	----------	% horas no presenciales	----------
Profesor/es Titular/Asociado/Adjunto:	Fernando Boiero	Dedicación:	Simple
Auxiliar/es de 1°/JTP		Dedicación:	
Competencias	Específicas	Genéricas	
	CE1.1 - CE 2.1 - CE 3.1 - 4.1 - CE5.1 - CE7.1	-	

2. Presentación, Fundamentación

El Ingeniero en Sistemas de Información es un profesional con una formación analítica sólida, capaz de interpretar y resolver problemas complejos mediante el empleo de metodologías avanzadas y tecnologías de procesamiento de información. Este profesional está preparado para el planeamiento, desarrollo, dirección y control de sistemas de información, administrando eficientemente los recursos humanos, físicos y de software implicados. Además, posee capacidades para desempeñar funciones gerenciales, liderar proyectos de investigación y desarrollo, y transmitir conocimientos de manera efectiva.

Importancia de la Seguridad Informática en la Formación del Ingeniero:

La Seguridad Informática es fundamental en la formación del Ingeniero en Sistemas de Información, ya que proporciona las competencias necesarias para proteger la integridad, confidencialidad y disponibilidad de la información en un entorno tecnológico en constante evolución. Esta asignatura prepara al futuro profesional para identificar, analizar y mitigar riesgos de seguridad en sistemas de información, desarrollando estrategias de defensa ante amenazas cibernéticas y vulnerabilidades en la infraestructura tecnológica.

Relación de la asignatura con el perfil de egreso.

Los contenidos desarrollados en la asignatura de Seguridad Informática cubren aspectos esenciales como la criptografía, la seguridad de redes, la seguridad de aplicaciones y la gestión de políticas de seguridad. Estos conocimientos permiten al estudiante comprender y enfrentar los desafíos de seguridad en sistemas de información complejos, incluyendo la protección contra ataques informáticos y la implementación de medidas de seguridad en aplicaciones y redes. La capacidad para diseñar, evaluar y gestionar sistemas seguros es una competencia clave que habilita al ingeniero para asegurar la confidencialidad, integridad y disponibilidad de la información, elementos críticos para el éxito de cualquier organización en la era digital.

Relación de la asignatura con los alcances del título.

A través del aprendizaje en Seguridad Informática, el alumno adquiere competencias para identificar y responder a las amenazas de seguridad actuales y emergentes, diseñar sistemas seguros y aplicar tecnologías y protocolos de seguridad avanzados. Esta formación le permite discernir entre diferentes estrategias de seguridad, evaluar riesgos y seleccionar las soluciones más adecuadas para la protección de sistemas de información. Los conocimientos adquiridos son esenciales para el desarrollo, implementación y gestión de proyectos de sistemas de información seguros, preparando al ingeniero para afrontar los desafíos de seguridad en un contexto de constante cambio tecnológico.

3. Relación de la asignatura con las competencias de egreso de la carrera

Se detalla en la siguiente tabla, la relación de la asignatura con las competencias de egreso específicas, genéricas tecnológicas, sociales, políticas y actitudinales de la carrera. Indicando a cuáles competencias de egreso tributa y en qué nivel (No Tributa, 1=bajo, 2=medio, 3=alto).

Competencias	Nivel
Competencias genéricas tecnológicas (CG):	
CG. 1. Identificar, formular y resolver problemas de ingeniería.,	No Tributa
CG. 2. Concebir, diseñar y desarrollar proyectos de ingeniería.	No Tributa
CG. 3. Gestionar, planificar, ejecutar y controlar proyectos de ingeniería.	No Tributa
CG. 4. Utilizar de manera efectiva las técnicas y herramientas de aplicación en la ingeniería.	No Tributa
CG. 5. Contribuir a la generación de desarrollos tecnológicos y/o innovaciones tecnológicas.	No Tributa
Competencias Genéricas Sociales Políticas y Actitudinales (CG):	
CG. 6. Desempeñarse de manera efectiva en equipos de trabajo.	No Tributa
CG. 7. Comunicarse con efectividad	No Tributa
CG. 8. Actuar con ética, responsabilidad profesional y compromiso social, considerando el impacto económico, social y ambiental de su actividad en el contexto local y global.	No Tributa
CG. 9. Aprender en forma continua y autónoma.	No Tributa
CG. 10. Actuar con espíritu emprendedor	No Tributa
Competencias Específicas (CE):	
CE. 1.1. Especificar, proyectar y desarrollar sistemas de información para concebir soluciones tecnológicas que permitan resolver situaciones en las organizaciones mediante el empleo de metodologías de sistemas y tecnologías asociadas a los sistemas de información	2
CE. 1.2. Especificar, proyectar y desarrollar sistemas de comunicación de datos, evaluando posibles soluciones tecnológicas disponibles para dar soporte a los sistemas de información en lo referido al procesamiento y comunicación de datos.	No Tributa
CE. 1.3. Especificar, proyectar y desarrollar software para la elaboración de soluciones informáticas con el propósito de resolver problemas estratégicos y operativos, así como de servicios y de negocios, en el marco de una actividad económica que sea social y ambientalmente sustentable.	No Tributa

CE. 2.1. Proyectar y dirigir lo referido a seguridad informática para seleccionar y aplicar técnicas, herramientas, métodos y normas, garantizando la seguridad y privacidad de la información procesada y generada por los sistemas de información.	2
CE. 3.1. Establecer métricas y normas de calidad de software para medir, evaluar, controlar y monitorear el rendimiento, impulsando mejoras de acuerdo a técnicas y normas vigentes definidas por los organismos de estandarización.	2
CE. 4.1. Certificar el funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software para asegurar la generación de los resultados deseados en función de restricciones de tiempo y recursos establecidos.	2
CE. 5.1. Dirigir y controlar la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software, a los fines de alcanzar los objetivos fijados por la organización.	2
CE. 6.1. Asesorar y capacitar a organizaciones, empresas, organismos públicos o privados en la adquisición, instalación y uso, en lo que respecta a sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software, a los fines de un uso correcto de los sistemas intervinientes.	No Tributa
CE. 7.1. Realizar pericias, tasaciones y arbitrajes relacionados con su actividad profesional, respetando marcos normativos y jurídicos con el objeto de asesorar a las partes o a los tribunales de Justicia.	2

4. Propósito

El propósito principal de la asignatura Seguridad Informática es dotar a los estudiantes de la carrera de Ingeniería en Sistemas de Información con un conocimiento profundo y comprensivo sobre las amenazas, vulnerabilidades y medidas de protección críticas en el ámbito de la tecnología de la información. Los estudiantes adquirirán habilidades prácticas y teóricas para identificar riesgos de seguridad, implementar políticas de seguridad efectivas, y utilizar herramientas y técnicas avanzadas para la prevención, detección y respuesta ante incidentes de seguridad cibernética.

A lo largo del curso, se enfatizará en la importancia de la seguridad en diferentes capas, incluyendo la seguridad de redes, la seguridad de aplicaciones, la criptografía y la gestión de la seguridad de la información. Se explorarán conceptos clave como la autenticación, la

autorización, la integridad de datos, y la privacidad, así como el impacto de las nuevas tecnologías y tendencias, como la nube, el Internet de las Cosas (IoT) y la inteligencia artificial en la seguridad informática.

Además, se promoverá una comprensión integral de los aspectos legales y éticos asociados con la seguridad informática, preparando a los estudiantes para navegar en el complejo entorno regulatorio y normativo actual. Al finalizar la asignatura, los estudiantes estarán capacitados para diseñar e implementar estrategias de seguridad robustas y eficaces, preparándolos para afrontar con solvencia los desafíos de seguridad en el entorno profesional y contribuir a la protección de la infraestructura tecnológica crítica en diversos sectores.

5. Objetivos establecidos en la asignatura

- Comprender los Principios Fundamentales de la Seguridad Informática: Adquirir un entendimiento sólido sobre los conceptos básicos de seguridad informática, incluyendo la confidencialidad, integridad, y disponibilidad de la información.
- Fundamentos de Criptografía y Firma Digital:
- Comprender los Principios y Técnicas de Criptografía: Profundizar en el estudio de la criptografía, incluyendo cifrado simétrico y asimétrico, funciones hash, y protocolos criptográficos.
- Aplicar la Firma Digital: Aprender sobre firmas digitales, su importancia en la autenticación y la no repudiación, y cómo implementarlas de manera segura en diferentes contextos.
- Identificar y Analizar Amenazas y Vulnerabilidades: Conocer y analizar las diversas formas de amenazas cibernéticas y vulnerabilidades para implementar estrategias de mitigación efectivas.
- Implementar Medidas de Seguridad y Protección: Aplicar técnicas y herramientas avanzadas para proteger sistemas y redes contra ataques cibernéticos.
- Sistemas de Gestión de la Seguridad Informática y Norma ISO/IEC 27001:
- Introducción a los Sistemas de Gestión de la Seguridad de la Información (SGSI): Comprender los componentes y procesos clave de un SGSI efectivo.
- Implementar y Gestionar la Seguridad Conforme a ISO/IEC 27001: Aprender sobre la norma ISO/IEC 27001, su alcance, requisitos, y proceso de certificación, enfocándose en la implementación de controles de seguridad efectivos y la gestión del riesgo.
- Desarrollar Habilidades Prácticas en Seguridad Informática: Ganar experiencia práctica en la configuración de sistemas seguros, realización de pruebas de penetración, y estrategias de respuesta ante incidentes.
- Evaluar la Seguridad en Aplicaciones y Servicios: Dominar las mejores prácticas para asegurar aplicaciones web y servicios en la nube.

- Introducción a Blockchain y su Impacto en la Seguridad Informática: Comprender cómo la tecnología blockchain y los contratos inteligentes pueden ser utilizados para crear aplicaciones descentralizadas seguras.
- Promover la Conciencia sobre la Ética y la Legalidad en Seguridad Informática: Fomentar un comportamiento ético y comprender la legislación relevante en el ámbito de la seguridad informática.
- Preparación para la Innovación y Adaptación a Nuevas Tecnologías: Estar preparados para adoptar y adaptarse a las tecnologías emergentes, entendiendo su impacto en la seguridad informática.

6. Contenidos Mínimos establecidos en el Diseño Curricular

No Aplica

7. Resultados de aprendizaje

Se describen los Resultados de aprendizaje (RA) a promover en el desarrollo de la asignatura.

Identificador del RA	Redacción
RA1:	Identifica y explica los conceptos fundamentales de la seguridad informática, incluyendo la confidencialidad, integridad, y disponibilidad de la información, así como los principios básicos de la criptografía y la aplicación de firmas digitales.
RA2:	Analiza y evalúa las amenazas y vulnerabilidades a las que están expuestos los sistemas de información, aplicando técnicas de análisis de riesgos para identificar y mitigar potenciales brechas de seguridad.
RA3:	Diseña e implementa estrategias de seguridad utilizando herramientas y tecnologías avanzadas para proteger sistemas y redes contra ataques cibernéticos, incluyendo la configuración de firewalls, sistemas de detección de intrusiones y protocolos de cifrado.
RA4:	Desarrolla, configura y evalúa políticas y procedimientos de seguridad conforme a la norma ISO/IEC 27001, comprendiendo el proceso de implementación y gestión de un Sistema de Gestión de Seguridad de la Información (SGSI).
RA5:	Aplica conocimientos prácticos en la realización de pruebas de penetración y en la implementación de estrategias de respuesta ante incidentes, demostrando habilidades en la identificación y corrección de vulnerabilidades en sistemas de información.
RA6:	Evalúa la seguridad en aplicaciones web y servicios en la nube, identificando riesgos específicos y aplicando medidas de seguridad para proteger aplicaciones y datos alojados en entornos de nube.
RA 7	Comprende y discute el impacto de las tecnologías emergentes como blockchain en la seguridad informática, evaluando cómo estas tecnologías pueden ser utilizadas para mejorar la seguridad y la transparencia en aplicaciones descentralizadas.

RA 8	Demuestra conciencia de los aspectos éticos y legales relacionados con la seguridad informática, incluyendo la privacidad de datos, la legislación sobre ciberdelitos, y las responsabilidades profesionales en el manejo de incidentes de seguridad.
RA 9	Muestra habilidades para la innovación y adaptación a nuevas tecnologías, evaluando críticamente cómo las tendencias emergentes en tecnología impactan la seguridad informática y desarrollando soluciones que aborden estos desafíos.

8. Asignaturas correlativas previas

Para cursar debe tener cursada:

- Asignatura: Redes de Datos.

Para cursar debe tener aprobada:

- Asignatura: Ninguna.

Para rendir debe tener aprobada:

- Asignatura: Redes de Datos.

9. Asignaturas correlativas posteriores

- No aplica

10. Programa analítico, Contenidos temáticos

Ejes temáticos	Contenidos
Introducción a la Seguridad Informática	Conceptos básicos: confidencialidad, integridad, y disponibilidad. Historia y evolución de la seguridad informática.
Criptografía	Principios de criptografía: cifrado, hash, firmas digitales.
Seguridad en Redes	Seguridad en redes: firewalls, VPNs, IDS/IPS. Protocolos de seguridad: SSL/TLS, SSH.
Gestión de Seguridad y Normativas	Normativas de seguridad: ISO/IEC 27001, GDPR.
Seguridad en Aplicaciones Web	Vulnerabilidades web: SQL Injection, XSS, CSRF.
Análisis Forense y Respuesta a Incidentes	Estrategias de respuesta ante incidentes. ○ Introducción al análisis forense digital.
Seguridad en la Nube y Virtualización	Modelos de servicio en la nube: IaaS, PaaS, SaaS.
Blockchain y Criptomonedas en Seguridad	Fundamentos de blockchain en seguridad informática. ○ Aplicaciones de blockchain para mejorar la seguridad.
Inteligencia Artificial y Seguridad Informática	Aplicaciones de la IA en seguridad: detección de amenazas, análisis de comportamiento.

Cuadro de Carga Horaria de Formación Práctica

Tipo de Formación Práctica	Carga horaria	
	Presencial	**A Distancia**
Instancias supervisadas de formación práctica (prácticas en diferentes ámbitos tales como aula, laboratorios, campo u otros)	24 hs.	
Proyecto Integrador		
Práctica profesional supervisada		
Carga horaria total	24 hs.	

11. Metodología de enseñanza

La metodología de enseñanza de la materia de seguridad informática está diseñada para fomentar la participación activa del alumno y la integración de los conceptos adquiridos en unidades temáticas previas. Para lograr este objetivo se utilizan diversas estrategias didácticas que incluyen el método de casos, Realidad – Teoría - Práctica (R-T-P), aula invertida y aprendizaje cooperativo.

El uso del método de casos tiene como propósito el desarrollo de habilidades de análisis, pensamiento crítico y toma de decisiones en el alumno. Por otro lado, la metodología R-T-P tiene como objetivo fomentar la inferencia y reelaboración de conocimientos en vez de recibir el conocimiento terminado, y esto se logra a través de la participación activa del alumno. En unidades que lo permitan, se utiliza la metodología de aula invertida, que consiste en dedicar el tiempo de clases a la resolución de casos de estudio, trabajo en equipo y otras actividades, mientras que los contenidos teóricos son presentados previamente al alumno para su estudio individual.

Por último, el aprendizaje cooperativo se utiliza para fomentar el trabajo en equipo y la resolución de problemas en grupo. En las clases teóricas se espera que el alumno incorpore gradualmente los conocimientos relacionados a la cátedra y se desarrollen habilidades de liderazgo y colaboración a través de la participación activa en las discusiones y consultas.

En las clases prácticas se busca el aprendizaje experimental y la resolución de casos de estudio, lo que permite a los estudiantes trabajar de manera colaborativa y autodidacta. Se desarrollan ejercicios de aplicación para cada una de las unidades y se fomenta la resolución de problemas individuales y grupales.

Resumen de Competencias - Resultados de Aprendizaje - Metodologías de Enseñanza de la asignatura.

COMPETENCIA - NIVEL DE TRIBUTACIÓN	RESULTADO DE APRENDIZAJE (RA)
CE1.1(2) - CE 2.1(2) - CE 3.1(2) - CE4.1(2) - CE5.1(2) - CE7.1(2)	**RA1 - RA2 - RA3- RA4 - RA5 - RA6 - RA7 - RA8 - RA9**

EJES TEMÁTICOS - CONTENIDOS

Introducción a la Seguridad Informática - Criptografía - Seguridad en Redes - Gestión de Seguridad y Normativas - Seguridad en Aplicaciones Web - Análisis Forense y - Respuesta a Incidentes - Seguridad en la Nube y Virtualización - Blockchain y Criptomonedas en Seguridad -Inteligencia Artificial y Seguridad Informática

ACTIVIDADES DEL ESTUDIANTE (FORMATIVAS)

El **estudiante** deberá realizar las siguientes actividades para alcanzar los **RA** propuestos:

- Lectura y análisis de material bibliográfico.
- Trabajo Práctico Integrador
- Trabajo Práctico Grupal
- Cuestionarios.
- Resolución de Estudio de Casos
- Instancia de Evaluación Individual
- Resolución de problemas
- Exposición oral

ESTRATEGIAS DE ENSEÑANZA

El **docente** diseñará las siguientes **actividades pedagógicas**:

- Clase expositiva dialogada
- Taller / Seminario.
- Acompañamiento continuo.
- Diseño de problemas/ejercicios.
- Diseño de Casos de Estudios.
- Diseño Instancia de Evaluación.
- Retroalimentación formativa.
- Coordinación de trabajo colaborativo.

12. Recomendaciones para el estudio

1. Es recomendable que los estudiantes realicen una revisión previa de los temas que ya fueron tratados en cátedras de años anteriores correlativas a esta para tener una base sólida que facilite el aprendizaje de las nuevas temáticas abordadas en esta materia.

2. Es fundamental el seguimiento constante de la asignatura durante su desarrollo, cumpliendo con las actividades propuestas y manteniendo el ritmo del aprendizaje. Esto permitirá una mejor comprensión de los conceptos y una mayor capacidad para aplicarlos en situaciones reales.

3. La cátedra pone a disposición de los estudiantes material adicional en el campus virtual que puede complementar el material visto en clase y favorecer la comprensión de los temas.

4. Se recomienda aprovechar al máximo los espacios de consulta para aclarar dudas, tanto teóricas como prácticas. Es importante que los estudiantes se sientan en confianza para plantear sus inquietudes y despejar las dudas que puedan surgir durante el proceso de aprendizaje.

13. Metodología de evaluación

Momentos: Evaluación continua y final.

- Continua a través de la ejercitación práctica, participación en la clase, trabajo en equipo.
- Final: con los instrumentos de evaluación.

Instrumentos: 2 (dos) parciales y 2 (recuperatorios).

Actividades: Para lograr la evaluación continua se considerará la participación por parte del alumno tanto en el desarrollo de las clases teóricas como así también prácticas, criterio, capacidad de análisis, interpretación de resultados, entre otros.
También se considera, la presentación en tiempo y forma de las actividades propuestas en clases y el trabajo en equipo.

Criterios de regularización y promociones:

Regularidad: para alcanzar la condición de regular el alumno deberá cumplir:
1. El porcentaje de asistencias a clases teóricas y prácticas reglamentarias.
2. Tener aprobados las 2 (dos) instancias de evaluación.
3. Recuperatorios aprobados (en caso de usar esta instancia).
4. Si los puntos antes mencionados no se cumplen, el alumno se considera libre.

Promoción práctica: Podrán acceder aquellos alumnos que:

1. Cumple con los ítems de regularización previamente mencionados.
2. Tiene aprobada con un puntaje de 8 o mayor la instancia de evaluación práctica.

Promoción directa de la asignatura: Podrán acceder aquellos alumnos que:

1. Cumple con los ítems mencionados como base para la regularización.

2. Tiene aprobada con un puntaje de 8 o mayor ambas instancias de evaluación.
3. En caso de hacer recuperatorio de cualquiera de las dos instancias evaluativas se pierde la promoción directa.
4. De manera individual puede promocionarse la parte práctica pero no la teórica, es decir, si el alumno NO alcanza una nota de 8 o mayor en el práctico, pero si en las instancias teorías queda con estado regularizado.

FINALES: En caso de no acceder a la promoción directa, ni a la promoción del práctico, el alumno deberá rendir un final teórico-práctico en el turno de examen correspondiente.

14. Cronograma de clases año 2026

Semana	Contenido / Actividad
Semana 1	Presentación de materia. Introducción a la Seguridad Informática
Semana 2	Criptografía. Seguridad en Redes
Semana 3	Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 4	Gestión de Seguridad y Normativas
Semana 5	Gestión de Seguridad y Normativas Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 6	Seguridad en Aplicaciones Web Instancias de Evaluación
Semana 7	Análisis Forense y Respuesta a Incidentes
Semana 8	Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 9	Seguridad en la Nube y Virtualización
Semana 10	Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 11	Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 12	Blockchain y Criptomonedas en Seguridad Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 13	Inteligencia Artificial y Seguridad Informática Aplicabilidad en casos de estudios/Trabajos prácticos
Semana 14	Instancias de Evaluación

Semana 15	Inteligencia Artificial y Seguridad Informática
Semana 16	Recuperatorios

15. Recursos necesarios

Se consideran los siguientes recursos para cumplir los objetivos previstos de la cátedra:

- Aula para clases con equipamiento específico, disponibilidad de acceso a Internet, cañón de imágenes, etc.
- Laboratorio de computación con dispositivos conectados a Internet y software específico de la cátedra instalado.
- Otros: Acceso al campus virtual para material e interacción con los alumnos.

16. Referencias bibliográficas (citadas según Normas APA)

Cybrary. (n.d.). Introduction to IT & Cybersecurity. Recuperado el 10 de enero de 2024, de https://www.cybrary.it/course/intro-to-cyber-security/

lvh. (n.d.). Crypto 101. Recuperado el 10 de enero de 2024, de https://www.crypto101.io/

Open Web Application Security Project. (2021). OWASP Top Ten 2021. Recuperado el 10 de enero de 2024, de https://owasp.org/www-project-top-ten/

IT Governance UK. (n.d.). ISO 27001 & ISO 22301 Free PDF Downloads. Recuperado el 10 de enero de 2024, de https://www.itgovernance.co.uk/shop/category/iso-27001-downloads

Cloud Security Alliance. (n.d.). Security Guidance for Critical Areas of Focus in Cloud Computing. Recuperado el 10 de enero de 2024, de https://cloudsecurityalliance.org/research/guidance/

Open Textbook Library. (n.d.). Computer Forensics. Recuperado el 10 de enero de 2024, de https://open.umn.edu/opentextbooks/textbooks/computer-forensics

Cloud Security Alliance. (n.d.). Security Guidance for Critical Areas of Focus in Cloud Computing V4.0. Recuperado el 10 de enero de 2024, de https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Recuperado el 10 de enero de 2024, de https://link.springer.com/book/10.1007/978-3-319-55578-5

Taddeo, M., & Floridi, L. (2018). Regulation of Artificial Intelligence: from ethical to legal frameworks. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. Recuperado el 10 de enero de 2024, de https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080

17. Función Docencia

La función docente en esta materia se centra en la planificación y desarrollo equilibrado de los contenidos teóricos y prácticos por parte del responsable de cátedra. Se busca que el conocimiento teórico se complemente con la actividad práctica para lograr una comprensión y entendimiento profundos de los conceptos. El objetivo principal es guiar al estudiante en su proceso de aprendizaje, incentivando su participación y promoviendo un ambiente de colaboración y discusión constructiva en el aula.

18. Reuniones de asignatura y área

Desde la cátedra se plantean reuniones y contactos periódicos informales con docentes de asignaturas del mismo nivel y también de niveles inferiores y superiores a efectos de ajustar metodologías y tratamiento de contenidos vinculados. Además, se participa de reuniones de coordinación del área según corresponda.

19. Atención y orientación a las y los estudiantes

Los días de clases. Las y los alumnos podrán coordinar clases de consulta fuera del horario de clases a través del envío de mail al docente para su organización.