Facultad de Ingeniería y Ciencias
Escuela de Informática y Telecomunicaciones

DESCRIPTOR DE ASIGNATURA
Criptografía y seguridad en redes

1. Identificación de la asignatura:

Nombre de la Asignatura: Criptografía y Seguridad en redes	
Códigos: CIT2413	Créditos: 5
Duración: Semestral	Ubicación en el plan de estudios: Semestre 8
Requisitos: CIT2408 Taller de redes y servicios	
Sesiones cátedras semanales: 2 cátedras, 1 laboratorio	
Sesiones de ayudantía: 1	

2. Descripción de la asignatura:

Resulta esencial el poder identificar eventuales fallas de seguridad existentes en los sistemas informáticos o en las redes de datos empresariales, considerando tanto aspectos técnicos como los marcos legales y regulatorios de seguridad de la información. Así también, se debe poder proveer soluciones tecnológicamente factibles y eficientes para asegurar la confidencialidad de la información, la invulnerabilidad de las redes.
En este contexto, este curso entrega las herramientas necesarias para desarrollar de manera apropiada estas tareas, integrando no solo estrategias técnicas y metodologías de seguridad, sino también el conocimiento y aplicación de normativas y regulaciones que rigen la protección de la información y la seguridad informática esperado por la industria.

3. Resultados de Aprendizaje:

1. Diseña medidas de protección y seguridad de la información en medios electrónicos de intercambio de información, para aplicarlos en servicios tales como páginas web, evaluando su performance.
2. Evalúa el desempeño y limitantes de protocolos, esquemas de seguridad, métodos de autenticación y gestión de claves, en sistemas informáticos y redes de datos en el diseño de sistemas integrales de seguridad de datos.
3. Aplica técnicas criptográficas adecuadas en criptosistemas de clave pública, criptosistemas de clave privada y cifradores de flujo, para estimar métricas comparadas de funcionamiento en términos de robustez y uso de recursos.
4. Aplica métodos y algoritmos criptográficos clásicos y modernos, para evaluar la performance comparada mediante mediciones o simulación grupal de sistemas de encriptación de datos, documentando así el desempeño de los algoritmos bajo análisis.
5. Aplica marcos normativos de seguridad de la información, que permitan cumplir las expectativas regulatorias y de desempeño esperado por la industria.

6. Participa en equipos de trabajo, planificando, coordinando y ejecutando tareas con liderazgo y responsabilidad, comunicándose efectivamente y elaborando informes técnicos que reflejen procedimientos, resultados y análisis del trabajo realizado.

4. Unidades Temáticas:

Unidad 1: Introducción

- Conceptos fundamentales, confidencialidad, integridad y disponibilidad de la información, amenazas y métodos de defensa, terminología, componentes y tipos de criptosistemas, NIST e ISO/IEC 27001.

Unidad 2: Criptografía clásica

- Introducción a los criptosistemas clásicos, métodos de cifra monográmica por sustitución, métodos de cifra monográmica por transposición, métodos de cifra poligrámica.
- Criptosistemas de clave privada: Generalidades sobre sistema de clave secreta, algoritmos de Encriptación Simétrica (DES, 3DES, AES), otros cifrados de bloque y flujo. Modos de encriptación (ECB, CBC, CFB, CTR, GCM).
- Criptosistemas de clave pública: Introducción a la cifra con clave pública, protocolo de Diffie y Hellman para el intercambio de claves, cifrador de mochila de Merkle-Hellman, cifrado exponencial RSA, curvas elípticas. Introducción a algoritmos post-cuánticos.

Unidad 3: Funciones y Protocolos

- Funciones de autenticación: El problema de la integridad y autenticación, autenticación de mensajes con sistemas simétricos y asimétricos, firma digital con algoritmos RSA y EC, funciones hash SHA, RIPEMD-160, Bcrypt. ISO/IEC 10118-3.
- Seguridad en redes: El programa PGP (Pretty Good Privacy), autenticidad de correos electrónicos, certificación y entidades certificadoras, TLS y DTLS.
- Protocolos criptográficos: Implementación de protocolos seguros en servicios y análisis de protocolos criptográficos a partir del tráfico de red.

Unidad 4: Brechas de Seguridad

- Se presentarán configuraciones vulnerables relacionadas a implementaciones de servicios web, y sus contramedidas. Asimismo, se introducirán ataques informáticos relacionados a brechas en sistemas de cifrado de llave simétrica y asimétrica, como también en sistemas de autenticación.

5. Descripción general del método de enseñanza:

Se contemplan clases, combinando a lo largo del semestre, 2 sesiones de carácter expositivo (basadas en presentaciones electrónicas, con apoyo adicional de pizarrón, y/o contenido audiovisual) con 1 sesión de resolución de problemas en ayudantía y 1 sesión de laboratorio tecnológico obligatoria que comprende el desarrollo de laboratorios con simulación o implementación; medición y reporte de sistemas asociados al curso.

Se realizará un mínimo de 4 experiencias de laboratorio tecnológico durante el semestre, con personal docente asignado a tal efecto. En estos espacios se desarrollará las habilidades

relacionadas con la expresión escrita, así como de trabajo grupal y procesamiento de datos medidos, a partir de la realización de prácticas de laboratorio y trabajos (con sus respectivos informes).

6. Descripción general de la modalidad de evaluación:

Se contempla la realización de evaluaciones parciales (controles e informes de laboratorio), más dos pruebas solemnes de igual valor y un examen.

Será condición de aprobación la asistencia y realización de todas las experiencias de laboratorio, junto con una nota promedio de estas igual o mayor a 4.0. En caso contrario, el/la estudiante reprobará la asignatura con nota final igual al mínimo entre el promedio de sus experiencias de laboratorio o 3.9.

En caso de inasistencia a una sesión de laboratorio, el/la estudiante deberá justificar a la secretaría de escuela.

Podrán eximirse el/la estudiante que todas sus notas parciales tanto de cátedra como laboratorio sean igual o superior a 4.0 y cuya nota de presentación sea superior a 5.0, que hayan rendido todas sus evaluaciones.

7. Planificación de Sesiones:

La planificación de las sesiones dependerá del calendario académico vigente al momento de dictar la asignatura. En cualquier caso, cada docente que la imparta deberá informar a la Escuela (antes del comienzo del semestre) la planificación de sus actividades, evaluaciones, y mecanismos de diversificación de las mismas.

Esta información será informada al estudiantado durante la primera semana de clases.

8. Bibliografía Básica Obligatoria:

1. Bruce Schneier; Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition, John Wiley & Sons, 2015.
2. Cristof Paar, Jan Pelzl; Understanding Cryptography: A Textbook for Students and Practitioners, 1st Ed., Springer, 2010.
3. Hans Delfs, Helmut Knebl; Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), 3rd Ed., Springer, 2015

PAUTAS ÉTICAS BÁSICAS

El aula es un espacio donde los intercambios buscan generar un clima que potencie el aprendizaje, basado en el respeto y el buen trato. Las diferencias, tanto entre estudiantes, como entre estudiante y docentes, deben abordarse desde este marco de respeto.
La universidad cuenta con dos reglamentos importantes de conocer:

- Reglamento de Convivencia Estudiantil

- Normativa de Prevención y Sanción de Acciones de Discriminación, Violencia Sexual y/o de Género.

Puedes consultar los reglamentos aquí: https://www.udp.cl/universidad/reglamentos-y-politicas/

Así también, el plagio es el uso de las ideas o trabajo de otra persona sin el adecuado consentimiento. El plagio puede ser intencional o no. El plagio intencional es el claro intento de hacer pasar el trabajo o ideas ajenas como el suyo propio para su beneficio. El plagio no intencional puede ocurrir si Ud. no conoce el mecanismo adecuado de referenciar la fuente de sus ideas e información. Si no está seguro de los métodos aceptados para referenciar, debería consultar con su profesor, tutor o personal de biblioteca.
El plagio comprobado es una actitud que puede resultar en severas sanciones disciplinarias y/o en la exclusión de la Universidad (Artículo 44, Reglamento del Estudiante de Pregrado).

Elaborado por: Nicolás Boettcher.
Revisado por: Diego Dujovne
Fecha revisión: Noviembre 2025
Fecha vigencia: Marzo 2026