***Facultad de Ingeniería y Ciencias Escuela de Informática y Telecomunicaciones***

# PROGRAMA DE ASIGNATURA

*Criptografía y seguridad en redes*

# Identificación

| Nombre de la Asignatura: Criptografía y Seguridad en redes | |
| --- | --- |
| Códigos: CIT-2413 | Créditos: 6 |
| Duración: Semestral | Ubicación en el plan de estudios: Semestre 8 |
| Requisitos: CIT-2408 Taller de redes y servicios | |
| Sesiones cátedras semanales: 2 cátedras, 1 laboratorio | |
| Sesiones de Ayudantía: 1 | |

# Descripción del curso

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.

# Resultados de aprendizaje

Al finalizar el curso el/la estudiante será capaz de:

* Diseñar 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.
* Evaluar el desempeño y limitantes de protocolos, esquemas de seguridad, métodos de autenticación y gestión de claves en sistemas informáticos y redes de datos, para diseñar sistemas integrales de seguridad de datos.
* Aplicar técnicas criptográficas adecuadas en criptosistemas de clave pública, criptosistemas de clave privada y cifradores de flujo, para así estimar métricas comparadas de funcionamiento en términos de robustez y uso de recursos.
* Aplicar 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.
* Aplicar marcos normativos de seguridad de la información, que permitan cumplir las expectativas regulatorias y de desempeño esperado por la industria.

# Unidades Temáticas

* 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.
* 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.
* 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.
* 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.
* Aspectos legales de seguridad de la información: Regulaciones y normativas aplicables en ciberseguridad y protección de datos, incluyendo la Ley 21.663 Marco de Ciberseguridad, la Ley 21.459 de delitos informáticos, la Ley 21.719 de Protección y Tratamiento de Datos Personales, y la Ley 19799 de Firma Electrónica en Chile.

1. **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 trabajo en laboratorio donde se realizarán talleres interactivos. Esto será complementado con lectura de textos y material adicional, para la realización de tareas, laboratorios o trabajos de investigación, permitiendo desarrollar habilidades relacionadas con el autoaprendizaje continuo.

Se realizará un mínimo de 5 laboratorios, talleres interactivos o defensa de casos.

Se fomentará la evaluación del conocimiento adquirido, el nivel de comprensión, la capacidad de análisis, síntesis, y aplicación. Esto será medido a través de trabajos periódicos, evaluaciones al finalizar cada campo de conocimiento más dos pruebas solemnes, junto a un examen final escrito en la hora y día que establezca la Dirección de la Escuela.

Se fomentará también el desarrollo de habilidades relacionadas con la expresión oral y escrita, así como de trabajo grupal y procesamiento de datos medidos, a partir de la realización de presentaciones orales, prácticas de laboratorio (con sus respectivos informes) . Esto se evaluará mediante presentaciones orales y en la evaluación de informes escritos (laboratorios, tareas, trabajos).

1. **Descripción general de la modalidad de evaluación:**

Se realizarán prácticos de laboratorio, evaluaciones de campo de conocimiento, dos pruebas solemnes y un examen final.

Las experiencias de laboratorio serán evaluadas mediante informes. Para aprobar la asignatura se debe haber aprobado las experiencias de laboratorio (nota promedio igual o superior a 4.0), donde la asistencia al 100% de las experiencias es una condición necesaria, pero no suficiente. En caso contrario, reprobará la asignatura con nota final igual al promedio de sus experiencias de laboratorio

Nota de Presentación = (25% Solemne 1 + 25% Solemne 2 + 20% Notas Parciales + 30% laboratorios)

Nota Final= 70% Nota de Presentación + 30% Examen.

Podrá eximirse el/la estudiante cuya nota de presentación sea igual o superior a 5.0, que haya rendido todas sus evaluaciones de acuerdo al item “nota de presentación” definido más arriba.

# 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



Elaborado por: Nicolás Boettcher.

Revisado por: Diego Dujovne

Fecha revisión: Marzo de 2025

Fecha vigencia: Marzo de 2025