
 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	FORMATO DE SYLLABUS		Código: AA-FR-003	 SIGUD <small>Sistema Integrado de Gestión</small>
	Macroproceso: Direccionamiento Estratégico		Versión: 01	
	Proceso: Autoevaluación y Acreditación		Fecha de Aprobación: 27/07/2023	

FACULTAD:	Tecnológica				
PROYECTO CURRICULAR:	Tecnología en Electrónica Industrial			CÓDIGO PLAN DE ESTUDIOS:	

I. IDENTIFICACIÓN DEL ESPACIO ACADÉMICO

NOMBRE DEL ESPACIO ACADÉMICO: CRIPTOGRAFÍA Y SEGURIDAD EN REDES

Código del espacio académico:	7409	Número de créditos académicos:			2	
Distribución horas de trabajo:	HTD	2	HTC	2	HTA	5
Tipo de espacio académico:	Asignatura	x	Cátedra			

NATURALEZA DEL ESPACIO ACADÉMICO:

Obligatorio Básico	x	Obligatorio Complementario		Electivo Intrínseco		Electivo Extrínseco	
--------------------	---	----------------------------	--	---------------------	--	---------------------	--

CARÁCTER DEL ESPACIO ACADÉMICO:

Teórico		Práctico		Teórico-Práctico	x	Otros:		Cuál: _____
---------	--	----------	--	------------------	---	--------	--	-------------

MODALIDAD DE OFERTA DEL ESPACIO ACADÉMICO:

Presencial	x	Presencial con incorporación de TIC		Virtual		Otros:		Cuál: _____
------------	---	-------------------------------------	--	---------	--	--------	--	-------------

II. SUGERENCIAS DE SABERES Y CONOCIMIENTOS PREVIOS

Se recomienda que los estudiantes hayan cursado previamente asignaturas como fundamentos de redes, sistemas operativos, y matemáticas discretas. Es deseable tener conocimientos básicos en teoría de números, programación en Python o C/C++, y manejo de entornos de red y simuladores. Esto facilitará la comprensión de algoritmos criptográficos, arquitecturas de red seguras y metodologías de auditoría digital.

III. JUSTIFICACIÓN DEL ESPACIO ACADÉMICO

En un contexto digital donde la seguridad de la información es crítica, esta asignatura permite formar profesionales capaces de proteger datos e infraestructuras ante amenazas cibernéticas. La criptografía moderna, junto con técnicas de seguridad en redes, son fundamentales para garantizar la confidencialidad, integridad, autenticación y disponibilidad de los servicios. Se abordan desde esquemas tradicionales hasta tecnologías emergentes como blockchain, Zero Trust, ciberseguridad en IoT y protección en la nube.

IV. OBJETIVOS DEL ESPACIO ACADÉMICO (GENERAL Y ESPECÍFICOS)

Objetivo General:

Analizar y aplicar métodos y técnicas modernas de criptografía y seguridad en redes para la protección efectiva de sistemas de información en contextos empresariales, industriales y personales.

Objetivos Específicos:

Comprender los fundamentos de la criptografía clásica y moderna.
 Evaluar amenazas, vulnerabilidades y controles en redes digitales.
 Implementar protocolos seguros de comunicación como SSL/TLS, VPNs y IPsec.
 Aplicar herramientas de auditoría, detección de intrusos y pruebas de penetración.

V. PROPÓSITOS DE FORMACIÓN Y DE APRENDIZAJE (PFA) DEL ESPACIO ACADÉMICO

Propósitos de formación:

Fortalecer la capacidad para diseñar arquitecturas seguras en redes y servicios.
 Desarrollar competencias en ciberseguridad y encriptación de datos en redes modernas.
 Fomentar la ética profesional y la gestión responsable de la información.

Resultados de aprendizaje:

Evalúa los riesgos de seguridad en infraestructuras de red.
 Diseña e implementa esquemas de protección criptográfica.
 Configura y valida servicios seguros sobre protocolos TCP/IP.
 Aplica auditorías técnicas y herramientas de análisis forense.

VI. CONTENIDOS TEMÁTICOS

1. Fundamentos de Seguridad de la Información
Principios: confidencialidad, integridad, disponibilidad, autenticación.
Amenazas, vulnerabilidades, riesgos y controles.
Modelos de seguridad Zero Trust y defensa en profundidad.

2. Criptografía Clásica y Moderna
Algoritmos simétricos: AES, 3DES.
Algoritmos asimétricos: RSA, ECC.
Funciones hash: SHA-2, SHA-3, HMAC.

3. Protocolos y Servicios Seguros
SSL/TLS, HTTPS, IPsec y VPNs.
Autenticación multifactor y biométrica.
Infraestructura de clave pública (PKI).

4. Seguridad en Redes y Dispositivos
Firewalls, IDS/IPS, honeypots.
Seguridad en redes inalámbricas.
Protección en redes IoT y edge computing.

5. Legislación, Normas y Auditoría
ISO/IEC 27001, NIST, ENS.
Políticas de seguridad y auditorías técnicas.
Análisis forense digital y pruebas de penetración.

6. Aplicaciones Emergentes y Proyecto Final
Blockchain y criptoactivos.
Seguridad en la nube y contenedores (Docker, Kubernetes).
Desarrollo de un sistema seguro con validación de vulnerabilidades.

VII. ESTRATEGIAS DE ENSEÑANZA QUE FAVORECEN EL APRENDIZAJE

Se empleará una metodología de aprendizaje activo basada en proyectos (ABP), estudios de caso y ejercicios prácticos en laboratorio. Se promoverá el uso de entornos virtualizados, simuladores de redes y herramientas especializadas como Wireshark, OpenSSL, Metasploit, y VirtualBox para ambientes seguros de prueba.

VIII. EVALUACIÓN

De acuerdo con el estatuto estudiantil vigente (Acuerdo No. 027 de 1993 expedido por el Consejo Superior Universitario y en su Artículo No. 42 y al Artículo No. 3, Literal d) el profesor al presentar el programa presenta una propuesta de evaluación como parte de su propuesta metodológica.

Para dar cumplimiento a lo dispuesto en el estatuto estudiantil, los porcentajes por corte se definen como se indica a continuación, con base en las fechas establecidos por el Consejo Académico en el respectivo calendario académico.

Primer corte (hasta la semana 8) à 35%
Segundo corte (hasta la semana 16) à 35%
Proyecto final (hasta la semana 18) à 30%

En todo caso, la evaluación será continua e integral, teniendo en cuenta los avances del estudiante en los siguientes aspectos: i) comprensión conceptual (pruebas escritas, talleres); ii) aplicación práctica (laboratorios, informes técnicos); iii) proyecto integrador final (análisis, diseño, montaje y presentación); y iv) participación y trabajo en equipo. Asimismo, se debe valorar el desarrollo de competencias comunicativas, resolución de problemas, uso de instrumentos, pensamiento lógico y creatividad. Las pruebas se concertarán con el grupo y se ajustarán a las fechas establecidas en el respectivo calendario académico.

IX. MEDIOS Y RECURSOS EDUCATIVOS

Para el adecuado desarrollo de este espacio académico, se requiere el uso de medios institucionales y recursos individuales que faciliten los procesos de enseñanza y aprendizaje, tanto en ambientes presenciales como virtuales. Las actividades teóricas se apoyarán en aulas de clase dotadas de medios audiovisuales (tablero, videobeam, sillas) y plataformas virtuales institucionales como Microsoft Teams o Google Meet. Además, será fundamental el acceso a presentaciones digitales, textos base, hojas de datos, artículos técnicos y bibliotecas digitales.

En cuanto al trabajo práctico, se utilizarán aulas de laboratorio equipadas con fuentes de voltaje DC, generadores de señales, osciloscopios, multímetros y otros instrumentos de medición. Adicionalmente se cuenta con Laboratorio de cómputo con acceso a máquinas virtuales, Kali Linux, Wireshark, GNS3, OpenVPN, herramientas de hashing y criptografía.

Como recursos propios, el estudiante debe disponer de una calculadora científica, conexión estable a internet que la universidad proporciona, un sistema para la toma de apuntes (cuaderno, tablet o computador) y acceso a los materiales de clase. Será responsabilidad del estudiante descargar los insumos digitales y contar con los elementos necesarios que serán especificados previamente en cada práctica o proyecto.

X. PRÁCTICAS ACADÉMICAS - SALIDAS DE CAMPO

Visitas a Centros de Operaciones de Seguridad (SOC), eventos de ciberseguridad y participación en CTF (Capture The Flag). Se podrá articular la asignatura con semilleros de investigación en seguridad digital o emprendimientos de tecnología segura.

XI. BIBLIOGRAFÍA

Stallings, W. (2023). Cryptography and Network Security: Principles and Practice. Pearson.

Kaufman, C., Perlman, R., Speciner, M. (2022). Network Security: Private Communication in a Public World. Prentice Hall.

Paar, C., Pelzl, J. (2010). Understanding Cryptography. Springer.

Smith, R. (2021). Elementary Information Security. Jones & Bartlett Learning.

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

XII. SEGUIMIENTO Y ACTUALIZACIÓN DEL SYLLABUS			
Fecha revisión por Consejo Curricular:			
Fecha aprobación por Consejo Curricular:		Número de acta:	