

**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**  
**FACULTAD DE INGENIERIA**

**SYLLABUS**

**PROYECTO CURRICULAR:**

**NOMBRE DEL DOCENTE:**

**ESPACIO ACADÉMICO(Asignatura):** Criptografía y Blockchain

**Obligatorio ( ) : Básico ( ) Complementario ( )**

**Electivo ( x ) : Intrínsecas ( ) Extrínsecas ( x )**

**CÓDIGO:**

**NUMERO DE ESTUDIANTES: 20**

**GRUPO: 1**

**NÚMERO DE CREDITOS: 4**

**TIPO DE CURSO: TEÓRICO PRACTICO TEO-PRAC: X**

*Alternativas metodológicas:*

*Clase Magistral ( ), Seminario ( ), Seminario – Taller ( X ), Taller ( ), Prácticas ( ), Proyectos tutoriados ( ), Otro: \_\_\_\_\_*

**HORARIO:**

<b>DIA</b>	<b>HORAS</b>	<b>SALON</b>

**I. JUSTIFICACIÓN DEL ESPACIO ACADÉMICO (El Por Qué?)**

*La necesidad de Seguridad de la Información en una organización ha cambiado en las últimas décadas. Antes del uso de las computadoras, la Seguridad de la Información era proporcionada por medios físicos, por ejemplo el uso de cajas fuertes y por medidas administrativas, como los procedimientos de clasificación de documentos.*

*Con el uso de la computadora, y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos. Estas herramientas no sólo permiten proteger a la información, sino también a los Sistemas Informáticos que son los encargados de administrar la información.*

*Mientras que el Blockchain nació estrechamente ligado a las criptomonedas por ser el primer caso de uso en el que se usó esta tecnología, contabilidad compartida que apuntala las criptomonedas, también permite compartir entre compañías, particulares e instituciones todo tipo de datos codificados, desde dinero a registros médicos.*

*El nuevo orden social del siglo XXI implica la pérdida de confianza en las instituciones tradicionales, que no desaparecerán, pero sí cederán espacio para redistribuir las relaciones de poder. Devolviendo el control a la gente, Blockchain desplaza a los intermediarios tradicionales (bancos centrales, oficinas de registro de patentes, discográficas, notarios y depositarios de un contrato, comisiones electorales, empresas energéticas) y abre la puerta a nuevas formas de expresión personal, ecosistemas sociales e interacciones económicas.*

**Conocimientos previos:** *el estudiante debe tener conocimientos previos en Ciencias de la Computación y Estadística. El estudiante deberá tener conocimientos en temas como: Lenguajes y entornos de Programación.*

## **II. PROGRAMACIÓN DEL CONTENIDO (El Qué? Enseñar)**

### **OBJETIVO GENERAL**

*El objetivo principal de la criptografía y Blockchain es proporcionar herramientas que permitan operar la información utilizando la estructura de cifrado de datos en sus diferentes transacciones.*

### **OBJETIVOS ESPECÍFICOS**

- *Conocer la estructura de los algoritmos criptográficos y el cifrado de datos*
- *Conocer que es la criptografía y el blockchain*
- *Conocer las diferentes etapas de la encriptación de datos*
- *Aplicar los algoritmos criptográficos en hardware de uso específicos*
- *Entender el funcionamiento de las criptomonedas Bitcoin y Ethereum.*
- *Minar Bitcoin mediante Bitcoin Scripting.*
- *Conocer las distintas redes Blockchain como IBM Hyperledger y Alastria.*
- *Aprender cómo funcionan los Smart Contracts y el entorno en el que se ejecutan.*
- *Desarrollar y crear tokens (títulos negociables).*

## **PROGRAMA SINTÉTICO:**

### **FUNDAMENTOS DE SEGURIDAD Y CRIPTOGRAFIA (8 Horas – Teórico practicas)**

- Conceptos básicos de seguridad y criptografía
- Matemáticas discretas
- Uso de problemas matemáticos en la criptografía
- Seguridad de los algoritmos criptográficos
- Nociones de teoría de la información
- Codificación de la información

### **CRIPTOGRAFÍA CLÁSICA Y CIFRADO MODERNA (8 Horas – Teórico practicas)**

- Principios de Kersckhoffs
- Clasificación de los sistemas de cifra clásica
- Características de los sistemas de cifra modernos
- Cifra simétrica versus cifra asimétrica y aplicaciones

### **ALGORITMOS DE CIFRADO SIMÉTRICO (8 Horas – Teórico practicas)**

- Generalidades de la cifrado en flujo
- Algoritmos de cifrado en flujo: A5, RC4
- Generalidades de la cifrado en bloque
- Algoritmos de cifra en bloque: DES, 3DES, IDEA, AES

### **AUTENTICACIÓN Y FUNCIONES HASH (8 Horas – Teórico practicas)**

- Integridad y esquemas de autenticación
- Características y propiedades de las funciones hash
- Función hash MD5
- Función hash SHA-1
- Funciones hash SHA-256 y SHA-3

### **ALGORITMOS DE CIFRADO ASIMÉTRICA (8 Horas – Teórico practicas)**

- Generalidades del cifrado asimétrica
- Intercambio de la clave de Diffie y Hellman
- El algoritmo RSA
- El algoritmo de Elgamal

### **BLOCKCHAIN (8 horas- Teóricas)**

- Introducción e historia: Introducción a las Criptomonedas y los tokens.
- Teoría de Juegos y como aplica en Blockchain.
- Usos prácticos de la criptografía como la prueba de trabajo, Hashcash o Merkle Tree.
- Master class: ScytI y el voto electrónico.

## REDES BLOCKCHAIN: BITCOIN Y ETHEREUM (12 Horas)

- Las criptomonedas como usuario: Wallets y Exchanges.
- Funcionamiento de la cadena de bloques, la prueba de trabajo y los protocolos de consenso.
- Funcionamiento de Bitcoin y el Bitcoin Scripting.
- Funcionamiento de Ethereum y la Ethereum Virtual Machine.
- Master class: Bankia Stockmind y plataformas de tokenización.

### III. ESTRATEGIAS (El Cómo?)

#### Metodología Pedagógica y Didáctica:

*(Centrada en núcleos conceptuales y resolución de problemas en pequeños proyectos de investigación en grupos de estudiantes. Explicitar el tipo de metodología científica usada. Están centradas en el trabajo didáctico de los intereses y las ideas previas de los estudiantes. Cada unidad didáctica requiere determinar y trabajar las ideas previas, por ejemplo, en torno a la resolución de pequeños proyectos de investigación). Aun que no se intenta únicamente enseñar a los estudiantes la metodología científica de cada disciplina implicada, si se recomienda seguir los procedimientos que siguen los investigadores de las disciplinas científicas e ingenieriles para resolver problemas similares a los que se plantearan a los estudiantes.*

Se debe procurar incentivar el trabajo de grupo más que el trabajo individual. (se recomienda trabajar en grupos de tres o cuatro estudiantes)

Si es posible diseñar “*tramas conceptuales evolutivas*” que permitan seguir un curso de evolución de las ideas previas de los estudiantes.

En general se debe referenciar el modelo didáctico y pedagógico al cual se suscribe la propuesta de Syllabus.

Tipo de Curso	Horas			Horas profesor/semana	Horas Estudiante/semana	Total Horas Estudiante/semestre	Créditos
	TD	TC	TA	(TD + TC)	(TD + TC +TA)	X 16 semanas	

**Trabajo Presencial Directo (TD):** trabajo de aula con plenaria de todos los estudiantes.

**Trabajo Mediado\_Cooperativo (TC):** Trabajo de tutoría del docente a pequeños grupos o de forma individual a los estudiantes.

**Trabajo Autónomo (TA):** Trabajo del estudiante sin presencia del docente, que se puede realizar en distintas instancias: en grupos de trabajo o en forma individual, en casa o en biblioteca, laboratorio, etc.)

### IV. RECURSOS (Con Qué?)

**Medios y Ayudas:** Estos se refieren tanto a los físicos como humanos necesarios para la actividad pedagógica y didáctica. No sólo se hace referencia a las ayudas audiovisuales: retroproyectores de acetatos, de filminas o diapositivas, y de presentación de imágenes de computador, programas o software, sino también a la posibilidad de recursos para salidas de campo trabajo práctico de laboratorio, requerimientos para la logística y el trabajo con invitados o colaborativos con otros docentes en el aula.

## BIBLIOGRAFÍA

### TEXTOS Guías

Data Driven. DJ Patil

<https://blockchain.usal.es/>

### TEXTOS COMPLEMENTARIOS

### REVISTAS

### DIRECCIONES DE INTERNET

## V. ORGANIZACIÓN / TIEMPOS (De Qué Forma?)

**Espacios, Tiempos, Agrupamientos:**

Se recomienda trabajar una unidad cada cuatro semanas, trabajar en pequeños grupos de estudiantes, utilizar Internet para comunicarse con los estudiantes para revisiones de avances y solución de preguntas (esto considerarlo entre las horas de trabajo cooperativo).


**VI. EVALUACIÓN (Qué, Cuándo, Cómo?)**

*Es importante tener en cuenta las diferencias entre evaluar y calificar. El primero es un proceso cualitativo y el segundo un estado terminal cuantitativo que se obtiene producto de la evaluación. Para la obtención de la información necesaria para los procesos de evaluación se requiere diseñar distintos formatos específicos de autoevaluación, coevaluación y heteroevaluación.*

<b>PRIMERA NOTA</b>	<b>TIPO DE EVALUACIÓN</b>	<b>FECHA</b>	<b>PORCENTAJE</b>
	<b>Evaluación teórica de los conceptos de Seguridad</b>	12/03/2019	<b>20</b>
<b>SEGUNDA NOTA</b>	<b>Primera Entrega del proyecto</b>	<b>26/03/2019</b>	<b>20</b>
<b>TERCERA NOTA</b>	<b>Segunda Entrega del proyecto</b>	<b>23/04/2019</b>	<b>20</b>
<b>EXAM. FINAL</b>	<b>Entrega Fina del proyecto</b>		<b>30%</b>

ASPECTOS A EVALUAR DEL CURSO. El docente explicita y describe los criterios a tener en cuenta al evaluar. Por ejemplo:

1. Evaluación del desempeño docente
2. Evaluación de los aprendizajes de los estudiantes en sus dimensiones: individual/grupo, teórica/práctica, oral/escrita.
3. Autoevaluación:
4. Coevaluación del curso: de forma oral entre estudiantes y docente.

DATOS DEL DOCENTE			
<b>NOMBRE :</b> <b>PREGRADO :</b> Ingeniero Electrónico <b>POSTGRADO :</b> Doctor en Ingeniería, Magíster en ciencias de la Información y las Comunicaciones, Especialización en Telecomunicaciones Móviles <b>E-MAIL:</b>			
ASESORIAS: FIRMA DE ESTUDIANTES			
NOMBRE	FIRMA	CÓDIGO	FECHA
1.			
2.			
3.			
FIRMA DEL DOCENTE			
<div style="text-align: center; height: 150px;">  </div>			
FECHA DE ENTREGA: _____			