


## ASIGNATURA DE SEGURIDAD INFORMÁTICA

<b>1. Competencias</b>	Construir soluciones de software y sistemas inteligentes mediante la gestión de proyectos, integración de metodologías, modelos y herramientas de desarrollo bajo la normatividad aplicable para la optimización de proyectos de investigación, innovación, desarrollo tecnológico y de emprendimiento.
<b>2. Cuatrimestre</b>	SEPTIMO
<b>3. Horas Teóricas</b>	13
<b>4. Horas Prácticas</b>	32
<b>5. Horas Totales</b>	45
<b>6. Horas Totales por Semana Cuatrimestre</b>	3
<b>7. Objetivo de aprendizaje</b>	El alumno implementará mecanismos de seguridad con base en las normas, estándares y leyes aplicables para proteger la integridad y confidencialidad de la información.

Unidades de Aprendizaje	Horas		
	Teóricas	Prácticas	Totales
<b>I. Principios de seguridad informática</b>	4	2	6
<b>II. Criptografía</b>	3	9	12
<b>III. Intercambio de información segura</b>	6	21	27

**Totales**


<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA


## UNIDADES DE APRENDIZAJE

<b>1. Unidad de aprendizaje</b>	<b>I. Principios de seguridad informática</b>
<b>2. Horas Teóricas</b>	4
<b>3. Horas Prácticas</b>	2
<b>4. Horas Totales</b>	6
<b>5. Objetivo de la Unidad de Aprendizaje</b>	El alumno elaborará lineamientos de seguridad informática para cumplir con las normas, estándares y leyes aplicables al manejo de información en el desarrollo de software.

<b>Temas</b>	<b>Saber</b>	<b>Saber hacer</b>	<b>Ser</b>
Aspectos éticos y legales del manejo de la información.	<p>Describir las características de la normatividad nacional e internacional en materia de seguridad</p> <ul style="list-style-type: none"> <li>- Ley General de protección de datos Personales de México</li> <li>- Ley de propiedad industrial</li> <li>- Ley federal de derechos de autor</li> <li>- Ley federal de datos personales en posesión de particulares</li> <li>- Código penal federal</li> <li>- Ley general de transparencia y acceso a la información</li> </ul>	<p>Elaborar aviso de privacidad y confidencialidad de la información</p> <p>Elaborar deslinde de responsabilidad legal para uso de software</p>	<p>AUTODIDACTA</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p> <p>TRABAJO EN EQUIPO</p>
Estándares del manejo de la información.	<p>Describir las características de las normas y estándares:</p> <ul style="list-style-type: none"> <li>- ISO 27001</li> <li>- ISO 17799</li> <li>- COBIT</li> <li>- NIST</li> <li>- ITIL</li> </ul>		<p>AUTODIDACTA</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>RAZONAMIENTO</p> <p>DEDUCTIVO</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p>

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	


<b>Temas</b>	<b>Saber</b>	<b>Saber hacer</b>	<b>Ser</b>
Conceptos de seguridad	<p>Describir los principios de seguridad de la información</p> <ul style="list-style-type: none"> <li>- Accesibilidad</li> <li>- Confidencialidad</li> <li>- Disponibilidad</li> <li>- Autenticación</li> <li>- Integridad</li> <li>- Control de acceso</li> </ul> <p>Identificar el tipo de amenazas, vulnerabilidades y ataques a la ciberseguridad</p>		<p>AUTODIDACTA</p> <p>COGNITIVO</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>RAZONAMIENTO</p> <p>DEDUCTIVO</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p>
Conceptos de criptografía.	<p>Describir los conceptos relacionados a la criptografía</p> <ul style="list-style-type: none"> <li>- Criptografía simétrica</li> <li>- Criptografía asimétrica</li> <li>- Cifrado por bloques y por flujo</li> </ul> <p>Describir conceptos relacionados al criptoanálisis</p>	Elaborará lineamientos de seguridad de la información en el desarrollo de software	<p>AUTODIDACTA</p> <p>COGNITIVO</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>RAZONAMIENTO</p> <p>DEDUCTIVO</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p>

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA

## PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elaborará un documento a partir de un caso de estudio que integre: - Aviso de privacidad y confidencialidad de la información - Deslinde de responsabilidad legal para uso de software - Lineamientos de seguridad de la información en el desarrollo de software	1. Identificar normas, estándares y leyes aplicables al manejo de información 2. Describir los principios de seguridad 3. Describir conceptos de criptografía y criptoanálisis 4. Relacionar lineamientos de seguridad con el desarrollo de software	- Estudio de casos - Rúbrica

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	


# SEGURIDAD INFORMÁTICA

## PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
<ul style="list-style-type: none"><li>- Discusión en grupo</li><li>- Tareas de investigación</li><li>- Análisis de casos</li></ul>	<ul style="list-style-type: none"><li>- Equipos de cómputo</li><li>- Proyector</li><li>- Internet</li><li>- Pizarrón y marcadores</li><li>- Plataformas virtuales</li></ul>

## ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		


ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA

## UNIDADES DE APRENDIZAJE

1.	<b>Unidad de aprendizaje</b>	<b>II. Criptografía</b>
2.	<b>Horas Teóricas</b>	3
3.	<b>Horas Prácticas</b>	9
4.	<b>Horas Totales</b>	12
5.	<b>Objetivo de la Unidad de Aprendizaje</b>	El alumno desarrollará aplicaciones de software integrando algoritmos criptográficos para mantener la confidencialidad de la información.


<b>Temas</b>	<b>Saber</b>	<b>Saber hacer</b>	<b>Ser</b>
Algoritmos de cifrado	Identificar algoritmos de cifrado simétrico y sus aplicaciones  Identificar algoritmos de cifrado asimétrico y sus aplicaciones	Programar aplicaciones de software integrando funciones de cifrado	AUTODIDACTA ANALÍTICO CONFIABLE RAZONAMIENTO DEDUCTIVO ÉTICO HONESTO RESPONSABLE
Algoritmos hash	Identificar los algoritmos hash y sus aplicaciones: - SHA - MD5	Programar aplicaciones de software integrando algoritmos hash	AUTODIDACTA ANALÍTICO CONFIABLE RAZONAMIENTO DEDUCTIVO ÉTICO HONESTO RESPONSABLE

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA

## PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elaborará aplicaciones a partir de un caso práctico que integren: <ul style="list-style-type: none"><li>- Algoritmos de cifrado simétrico</li><li>- Algoritmos de cifrado asimétrico</li><li>- Algoritmos hash</li></ul>	1. Identificar los algoritmos de cifrado simétrico y asimétrico 2. Identificar los algoritmos hash 3. Comprender el uso de bibliotecas de seguridad 4. Relacionar las bibliotecas de seguridad al desarrollo de software	- Ejercicios prácticos - Lista de cotejo

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	


# SEGURIDAD INFORMÁTICA

## PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
<ul style="list-style-type: none"><li>- Prácticas en laboratorios dirigidas y no dirigidas</li><li>- Solución de problemas</li><li>- Tareas de investigación</li></ul>	<ul style="list-style-type: none"><li>- Equipos de cómputo</li><li>- Proyector</li><li>- Internet</li><li>- Pizarrón y marcadores</li><li>- Plataformas virtuales</li><li>- IDE de desarrollo</li></ul>

## ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	<b>x</b>	

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	




# SEGURIDAD INFORMÁTICA

## UNIDADES DE APRENDIZAJE

1.	<b>Unidad de aprendizaje</b>	<b>III. Intercambio de información segura</b>
2.	<b>Horas Teóricas</b>	6
3.	<b>Horas Prácticas</b>	21
4.	<b>Horas Totales</b>	27
5.	<b>Objetivo de la Unidad de Aprendizaje</b>	El alumno implementará protocolos y mecanismos de seguridad para proteger el intercambio de información


<b>Temas</b>	<b>Saber</b>	<b>Saber hacer</b>	<b>Ser</b>
Protocolos de seguridad	<p>Explicar protocolos de seguridad</p> <ul style="list-style-type: none"> <li>- HTTPS</li> <li>- SSL</li> <li>- FTPS</li> <li>- SSH</li> <li>- IPSEC</li> <li>- SET</li> <li>- SCP</li> <li>- SFTP</li> <li>- SMTPS</li> <li>- IMAPS</li> <li>- OAuth.</li> </ul>	<p>Seleccionar protocolos de seguridad de acuerdo al caso de estudio</p> <p>Implementar protocolos de seguridad seleccionados</p>	<p>AUTODIDACTA</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>RAZONAMIENTO</p> <p>DEDUCTIVO</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p>
Integridad de la Información	<p>Identificar la aplicación de firmas digitales</p> <p>Describir las características de los certificados digitales</p> <p>Identificar conceptos y características de blockchain para la seguridad</p>	<p>Demostrar el uso de las firmas y certificados digitales</p> <p>Desarrollar aplicación utilizando blockchain</p>	<p>AUTODIDACTA</p> <p>DISCIPLINADO</p> <p>ANALÍTICO</p> <p>CONFIABLE</p> <p>RAZONAMIENTO</p> <p>DEDUCTIVO</p> <p>ÉTICO</p> <p>HONESTO</p> <p>RESPONSABLE</p>

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA

## PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>Elaborará aplicaciones a partir de un caso práctico que integren:</p> <ul style="list-style-type: none"> <li>- Protocolos de seguridad</li> <li>- Firmas y certificados digitales</li> <li>- Principios de blockchain</li> </ul>	<ol style="list-style-type: none"> <li>1. Identificar los protocolos de seguridad</li> <li>2. Comprender el uso de las firmas y certificados digitales</li> <li>3. Identificar los principios de blockchain</li> <li>4. Relacionar los mecanismos de seguridad al desarrollo de software</li> </ol>	<ul style="list-style-type: none"> <li>- Ejercicios prácticos</li> <li>- Lista de cotejo</li> </ul>

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	


# SEGURIDAD INFORMÁTICA

## PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
<ul style="list-style-type: none"><li>- Prácticas en laboratorios dirigidas y no dirigidas</li><li>- Solución de problemas</li><li>- Tareas de investigación</li></ul>	<ul style="list-style-type: none"><li>- Equipos de cómputo</li><li>- Proyector</li><li>- Internet</li><li>- Pizarrón y marcadores</li><li>- Plataformas virtuales</li><li>- IDE de desarrollo</li></ul>

## ESPACIO FORMATIVO


Aula	Laboratorio / Taller	Empresa
	<b>x</b>	

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

## SEGURIDAD INFORMÁTICA

### CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA


Capacidad	Criterios de Desempeño
Implementar modelos de datos mediante herramientas y sistemas gestores para garantizar la disponibilidad e integridad de la información	<p>1. Entrega un documento que incluya:- Justificación de las herramientas a utilizar para los modelos de datos. - Modelos de datos. - Descripción de metadatos.</p> <p>2. Entrega archivos, credenciales de registro y secuencia de configuración para la creación de los modelos de datos.</p>
Implementar esquemas de seguridad mediante codificación, estándares, protocolos, herramientas e infraestructura para garantizar la privacidad y confidencialidad de la información cumpliendo con leyes y regulaciones aplicables	<p>1. Entrega un documento que incluya: - Listado de las leyes y regulaciones aplicables al proyecto de desarrollo de software. - Descripción de acciones encaminadas a cumplir las leyes y regulaciones aplicables al proyecto de desarrollo de software - Descripción de estándares, protocolos, herramientas e infraestructura para garantizar la privacidad y confidencialidad de la información del proyecto de desarrollo de software. - Reporte de pruebas de seguridad.</p> <p>2. Entrega archivos de código fuente y configuración de los esquemas de seguridad.</p>
Establecer metodologías y herramientas de gestión con base en el tipo y características del proyecto identificando las normas, estándares, leyes y regulaciones aplicables para el cumplimiento de los requerimientos establecidos.	<p>1. Entrega un documento que incluya: - Justificación de la metodología seleccionada. - Justificación de las herramientas de gestión. - Listado de las normas, estándares, leyes y regulaciones aplicables.</p>
Determinar procesos y herramientas de machine learning, data mining y big data mediante el análisis del problema de acuerdo a las características, ubicación de los datos y normativa aplicable para establecer un plan de desarrollo e integración que cubra las necesidades de información.	<p>1. Entrega un plan de desarrollo e integración que incluya: - Planteamiento del problema - Definición necesidades de información. - Descripción de la ubicación y características de los datos. - Justificación de la normativa aplicable. - Justificación las herramientas y procesos a utilizar.</p>

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	

# SEGURIDAD INFORMÁTICA

## FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
José Manuel Ortega Candel	2020 ISBN:97-8842672-8-005	Desarrollo seguro en ingeniería del software. Aplicaciones seguras con Android, NodeJS, Python y C++	Barcelona	España	Marcombo
Luis Hernández Encinas	2016 ISBN:97-8849097-1-079	La Criptografía	Madrid	España	La Catarata
Yuri Diogenes, Erdal Ozkaya	2018 ISBN:97-8178847-5-297	Cybersecurity – Attack and Defense Strategies	Birmingham	United Kingdom	Packt Publishing
Bikramaditya Singhal, Gautam Dhameja, Priyansu Panda	2018 ISBN:97-8148423-4-433	Beginning Blockchain	New York	United States	Apress
Roger A. Grimes	2018 ISBN:97-8842672-6-797	Hackear al hacker. Aprende de los expertos que derrotan a los hackers	Barcelona	España	Marcombo
Yvonne Wilson Abhishek Hingnikar	2019 ISBN:97-8148425-0-945	Solving Identity Management in Modern Applications	New York	United States	Apress
ISO/IEC	2013	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements			

<b>ELABORÓ:</b>	Comité de Directores de la Carrera de Ingeniería en Desarrollo y Gestión de Software	<b>REVISÓ:</b>	Dirección Académica	
<b>APROBÓ:</b>	C. G. U. T. y P.	<b>FECHA DE ENTRADA EN VIGOR:</b>	Septiembre de 2020	