ASIGNATURA DE SEGURIDAD INFORMÁTICA

1. Competencias	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.
2. Cuatrimestre	Séptimo
3. Horas Teóricas	13
4. Horas Prácticas	32
5. Horas Totales	45
6. Horas Totales por Semana Cuatrimestre	3
7. Objetivo de aprendizaje	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**
I. Principios de seguridad informática	4	2	**6**
II. Criptografía	3	9	**12**
III. Intercambio de información segura	6	21	**27**
Totales	**13**	**32**	**45**

SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Principios de seguridad informática**
2. Horas Teóricas	4
3. Horas Prácticas	2
4. Horas Totales	6
5. Objetivo de la Unidad de Aprendizaje	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.

Temas	Saber	Saber hacer	Ser
Aspectos éticos y legales del manejo de la información.	Describir las características de la normatividad nacional e internacional en materia de seguridad - Ley General de protección de datos Personales de México - Ley de propiedad industrial - Ley federal de derechos de autor - Ley federal de datos personales en posesión de particulares - Código penal federal - Ley general de transparencia y acceso a la información	Elaborar aviso de privacidad y confidencialidad de la información Elaborar deslinde de responsabilidad legal para uso de software	Autodidacta Analítico Confiable Ético Honesto Responsable Trabajo En Equipo
Estándares del manejo de la información.	Describir las características de las normas y estándares: - ISO 27001 - ISO 17799 - COBIT - NIST - ITIL		Autodidacta Analítico Confiable Razonamiento Deductivo Ético Honesto Responsable

Conceptos de seguridad.	Describir los principios de seguridad de la información - Accesibilidad - Confidencialidad - Disponibilidad - Autenticación - Integridad - Control de acceso Identificar el tipo de amenazas, vulnerabilidades y ataques a la ciberseguridad		Autodidacta Cognitivo Analítico Confiable Razonamiento Deductivo Ético Honesto Responsable
Conceptos de criptografía.	Describir los conceptos relacionados a la criptografía - Criptografía simétrica - Criptografía asimétrica - Cifrado por bloques y por flujo Describir conceptos relacionados al criptoanálisis	Elaborará lineamientos de seguridad de la información en el desarrollo de software	Autodidacta Cognitivo Analítico Confiable Razonamiento Deductivo Ético Honesto Responsable

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

SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
- Discusión en grupo - Tareas de investigación - Análisis de casos	- Equipos de cómputo - Proyector - Internet - Pizarrón y marcadores - Plataformas virtuales

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		

SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

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

Temas	Saber	Saber hacer	Ser
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

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: - Algoritmos de cifrado simétrico - Algoritmos de cifrado asimétrico - Algoritmos hash	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

SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
- Prácticas en laboratorios dirigidas y no dirigidas - Solución de problemas - Tareas de investigación	- Equipos de cómputo - Proyector - Internet - Pizarrón y marcadores - Plataformas virtuales - IDE de desarrollo

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	x	

SEGURIDAD INFORMÁTICA

UNIDADES DE APRENDIZAJE

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

Temas	Saber	Saber hacer	Ser
Protocolos de seguridad	Explicar protocolos de seguridad - HTTPS - SSL - FTPS - SSH - IPSEC - SET - SCP - SFTP - SMTPS - IMAPS - OAuth.	Seleccionar protocolos de seguridad de acuerdo al caso de estudio Implementar protocolos de seguridad seleccionados	Autodidacta Analítico Confiable Razonamiento Deductivo Ético Honesto Responsable
Integridad de la Información	Identificar la aplicación de firmas digitales Describir las características de los certificados digitales Identificar conceptos y características de blockchain para la seguridad	Demostrar el uso de las firmas y certificados digitales Desarrollar aplicación utilizando blockchain	Autodidacta Disciplinado Analítico Confiable Razonamiento Deductivo Ético Honesto Responsable

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: - Protocolos de seguridad - Firmas y certificados digitales - Principios de blockchain	1. Identificar los protocolos de seguridad 2. Comprender el uso de las firmas y certificados digitales 3. Identificar los principios de blockchain 4. Relacionar los mecanismos de seguridad al desarrollo de software	- Ejercicios prácticos - Lista de cotejo

SEGURIDAD INFORMÁTICA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
- Prácticas en laboratorios dirigidas y no dirigidas - Solución de problemas - Tareas de investigación	- Equipos de cómputo - Proyector - Internet - Pizarrón y marcadores - Plataformas virtuales - IDE de desarrollo

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	x	

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	1. Entrega un documento que incluya:- Justificación de las herramientas a utilizar para los modelos de datos. - Modelos de datos. - Descripción de metadatos. 2. Entrega archivos, credenciales de registro y secuencia de configuración para la creación de los modelos de datos.
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	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. 2. Entrega archivos de código fuente y configuración de los esquemas de seguridad.
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.	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.
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.	1. Entrega un plan de desarrollo e integración que incluya: - Planteamiento del problema - Definición de necesidades de información. - Descripción de la ubicación y características de los datos. - Justificación de la normativa aplicable. - Justificación de las herramientas y procesos a utilizar.

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 Última revisión 2018	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	London	England	