Programa de asignatura
por competencias de educación superior

Sección I. Identificación del Curso

Tabla 1. Identificación de la Planificación del Curso.

Actualización:	Mayo 18, 2022				
Carrera:	Ingeniería en Tecnologías de Software		**Asignatura:**	Seguridad Informática	
Academia:	Ciencias Computacionales Avanzadas /		**Clave:**	19SCATS0602	
Módulo formativo:	Cómputo de Alto Desempeño		**Seriación:**	- -	
Tipo de curso:	Modalidad mixta		**Prerrequisito:**	19SICTS0406 - Programación Orientada a Objetos	
Semestre:	Sexto	**Créditos:** 5.63	**Horas semestre:**	90 horas	
Teoría:	2 horas	**Práctica:** 1 hora	**Trabajo indpt.:**	2 horas	**Total x semana:** 5 horas

Sección II. Objetivos educacionales

Tabla 2. Objetivos educacionales

Objetivos educacionales		Criterios de desempeño	Indicadores
OE1	Solucionará problemas con sólidas bases científicas y fundamentos tecnológicos que le permitirán comprender, analizar, diseñar, organizar, producir, operar y dar soluciones prácticas a problemas relacionados con las áreas de Organización de Sistemas Computacionales e Ingeniería en Software para el sector productivo y social, promoviendo los principios de ética, responsabilidad y trabajo colaborativo.	El egresado implementará las diferentes etapas del ciclo de vida del software contemplando la protección de datos y prevención de desastres, salvaguardando con ética la seguridad de la información.	50 % Egresados trabajarán en cualquier proceso del desarrollo de software o áreas afines a los sistemas computacionales, promoviendo los principios de ética, responsabilidad y trabajo colaborativo.
OE2	Aportará soluciones innovadoras y sustentables en el área de la electrónica en el que establezca el análisis, diseño, implementación, selección de componentes de hardware de uso específico, el software asociado y su conectividad a través de redes de comunicación para el sector productivo y social.	El egresado implementará las diferentes técnicas de análisis y diseño de circuitos electrónicos que den una solución innovadora sustentable a problemas con el hardware.	20% Egresados trabajarán en cualquier proceso de creación y aplicación de hardware o áreas afines en el sector productivo y social.
OE3	Implementará soluciones innovadoras y sustentables con tecnologías de información que sean acordes a las necesidades, a las tecnologías disponibles y emergentes, para lograr un aprovechamiento óptimo de los recursos humanos y financieros en el sector productivo y social.	El egresado implementará las diferentes tecnologías emergentes en equipos multidisciplinarios que den una solución innovadora y sustentable a las necesidades que se presenten en el ámbito productivo y social.	20 % Egresados trabajarán en la aplicación de Tecnologías de la información o áreas afines en el sector productivo o social.

Atributos de egreso de plan de estudios		Criterios de desempeño	Componentes
AE3	Aplicar una experimentación adecuada con apoyo de metodologías y juicio ingenieril quepermitan interpretar datos para obtener conclusiones que den solución a problemáticas en un contexto determinado.	- Identificará la naturaleza de un ataque informático, así como la importancia de la fortaleza de los passwords. - Será capaz de construir un proceso de seguridad de operaciones.	2. Seguridad de passwords. 2.1 Fases de un ataque informático. 2.2 Hash. 2.3 Ataque de Fuerza Bruta por frecuencia de variaciones. 2.4 Ataque de Diccionario por permutaciones de transformaciones. 2.5 Práctica de vulneración de passwords. 4. Seguridad de operaciones. 4.1. Familia de estándares ISO 27000. 4.2. FIPS 200 y NIST 800-53. 4.3. Revisión de ejemplos de procesos de seguridad de operaciones. 4.4. Elaboración en equipo de un proceso de seguridad de operaciones.
AE6	Identificar la necesidad de actualizarse constantemente para innovar y desarrollar la tecnología de software que sea amigable con el medio ambiente.	- Comprenderá los conceptos básicos de la seguridad informática, desde los enfoques de ciencias de la seguridad y como una cualidad. - Conocerá los diferentes tipos de criptografía y certificados digitales.	1. Introducción a la seguridad informática. 1.1 Importancia, definición y objetivos de la seguridad informática. 1.2 Ciencias de la Seguridad. 1.3 La seguridad como una cualidad de software (ISO 25000). 1.4 Servicios de seguridad. 1.5 Hackers y Hacktivismos. 3. Criptografía. 3.1 Criptografía simétrica. 3.2 Criptografía asimétrica. 3.3 Certificados digitales.

Continuación: Tabla 2. Objetivos educacionales (continuación			
No.	Atributos de egreso de plan de estudios	Criterios de desempeño	Componentes
			3.4 Firma digital. 3.5 Protocolos. 3.6 Prácticas Criptográficas en Java.

Sección III. Atributos de la asignatura

Tabla 3. Atributos de la asignatura

<table>
<tr><th colspan="3">Problema a resolver</th></tr>
<tr><td colspan="3">Ser capaz de incorporar requerimientos de seguridad informática a sus desarrollos; también ser capaz de implantar procesos con prácticas más robustas en las organizaciones en las cuales interactúe, incorporar requerimientos de seguridad informática a sus desarrollos e implantar procesos con prácticas más robustas en las organizaciones donde intervenga.</td></tr>
<tr><th colspan="3">Atributos (competencia específica) de la asignatura</th></tr>
<tr><td colspan="3">- Ser capaz de robustecer la seguridad de los passwords en una organización, así como de usar criptografía en los desarrollos del Ingeniero en Tecnologías de Software, trabajar con modelos y estándares de buenas prácticas de Seguridad Informática e implantar procesos en una organización.</td></tr>
<tr><th colspan="2">Aportación a la competencia específica</th><th>Aportación a las competencias transversales</th></tr>
<tr><td>Saber</td><td>Saber hacer</td><td>Saber Ser</td></tr>
<tr><td>- Conocer los ataques actuales de fuerza bruta y diccionario, hash, características de passwords resistentes a ataques.
- Conocer las características de la criptografía simétrica y asimétrica, certificados digitales, firma digital y protocolos criptográficos.
- Conocer los estándares ISO 27000, FIPS 200 y NIST 800-53, procesos de seguridad de operaciones.</td><td>- Ser capaz de programar ataques de passwords para poder operar procesos de passwords seguros.
- Ser capaz de programar aplicaciones que hagan uso de prácticas criptográficas robustas.
- Ser capaz de escribir procesos de seguridad de operaciones alineados con estándares internacionales.</td><td>- Aporta puntos de vista con apertura a aprender de los otros y considera los de otras personas de manera reflexiva y respetuosa.
- Participa activamente en la construcción de su aprendizaje y en la resolución de problemas, colaborando de manera productiva en espacios y equipos de trabajo.
- Cumple en tiempo y forma en sus obligaciones como estudiante, siguiendo las indicaciones y considerando los criterios de evaluación.</td></tr>
<tr><th colspan="3">Producto integrador de la asignatura, considerando los avances por unidad</th></tr>
<tr><td colspan="3">Portafolio de las prácticas realizadas en la unidad de aprendizaje.</td></tr>
</table>

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.1. Desglose específico de la unidad "Introducción a la Seguridad Informática."

Número y nombre de la unidad:	1. Introducción a la Seguridad Informática.					
Tiempo y porcentaje para esta unidad:	Teoría:	12 horas	Práctica:	5 horas	Porcentaje del programa:	18.89%
Aprendizajes esperados:	Conocer los conceptos fundamentales de la seguridad informática, para aplicarlos durante el desarrollo profesional de proyectos que requieren una seguridad confiable.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
1.1 Importancia, definición y objetivos de la seguridad informática. 1.2 Ciencias de la Seguridad. 1.3 La seguridad como una cualidad de software (ISO 25000). 1.4 Servicios de seguridad. 1.5 Hackers y Hacktivismos.	Saber: - Conocer los conceptos fundamentales de la seguridad informática. Saber hacer: - Identificar y aplicar los conceptos fundamentales de la seguridad informática. Ser: - Aporta puntos de vista con apertura a aprender de los otros y considera los de otras personas de manera reflexiva y respetuosa. - Participa activamente en la construcción de su aprendizaje y en la resolución de	- Identificación de conocimientos previos. - Exposición didáctica. - Debates. - Mapas conceptuales.	Evaluación diagnóstica: - Cuestionario de conocimientos previos. Evaluación formativa: - Debates y actividades en clase. Evaluación sumativa: - Examen.	Portafolio de evidencias: Examen de conocimientos de los temas de esta unidad.

Continuación: Tabla 4.1. Desglose específico de la unidad "Introducción a la Seguridad Informática."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	problemas, colaborando de manera productiva en espacios y equipos de trabajo. - Cumple en tiempo y forma en sus obligaciones como estudiante, siguiendo las indicaciones y considerando los criterios de evaluación. - Utiliza la tecnología para apoyar su aprendizaje y para el desarrollo de habilidades metacognitivas, el aprendizaje autónomo y el longlife learning.			

Bibliografía

- Anderson, R. (2008). Security Engineering. A Guide to Building Dependable Distributed Systems. Second Edition. Wiley.
- Caballero, P. (2003). Introducción a la criptografía. Segunda edición. México, Distrito Federal: Alfaomega.
- Cervantes, P. y Tauste, O. (2016). Internet negro. El lado oscuro de la red. Cd. de México, Paidós.
- Daltabuit, E.; Hernández, L.; Mallén, G. y Vázquez, J.J. (2007). La seguridad de la información. Ciudad de México:Limusa.
- Greenwald, G. (2014). Snowden. Sin un lugar donde esconderse. Ciudad de México: Ediciones B.
- Hook, D. (2005). Beginning Cryptography in Java. Indianapolis: Wiley.
- Kahn, D. (1973). The codebreakers. The story of secret writing. Chicago: New American Library.
- Knudsen, J. (2008). Java Cryptography. O'Reilly.
- Maiorano, A. (2009). Criptografía. Técnicas de desarrollo para profesionales. Ciudad de México: Alfaomega.
- Pfleeger, C. P.; Pfleeger, S. L.; & Margulies, J. (2015). Security in computing (5a ed.). EUA: Pearson / Prentice Hall.
- Snowden, E. (2019). Vigilancia permanente. Ciudad de México: Planeta.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.2. Desglose específico de la unidad "Seguridad de passwords."

Número y nombre de la unidad:	2. Seguridad de passwords.					
Tiempo y porcentaje para esta unidad:	Teoría:	12 horas	Práctica:	5 horas	Porcentaje del programa:	18.89%
Aprendizajes esperados:	Conocer los ataques actuales de fuerza bruta y diccionario, hash, características de passwords resistentes a ataques, para prevenir estos incidentes y desarrollar proyectos que requieren una seguridad confiable.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
2.1 Fases de un ataque informático. 2.2 Hash. 2.3 Ataque de Fuerza Bruta por frecuencia de variaciones. 2.4 Ataque de Diccionario por permutaciones de transformaciones. 2.5 Práctica de vulneración de passwords.	Saber: - Comprender las características de los ataques de password realizados en la actualidad. Saber hacer: - Realizar un minúsculo fragmento de un ataque de password, en un entorno controlado. Ser: - Aporta puntos de vista con apertura a aprender de los otros y considera los de otras personas de manera reflexiva y	- Aprendizaje basado en estudio de casos.	Evaluación formativa: - Análisis de estudios de caso. - Actividades realizadas en clase. Instrumento: Lista de cotejo. Evaluación sumativa: - Práctica y su reporte.	Codificación y ejecución individual de una de las miles de transformaciones posibles en un ataque de diccionario. El reporte de la práctica debe incluir: 1.- El código C++ de la transformación de un diccionario. 2.- El archivo con password vulnerados utilizando la transformación del diccionario.

Continuación: Tabla 4.2. Desglose específico de la unidad "Seguridad de passwords."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	respetuosa. - Participa activamente en la construcción de su aprendizaje y en la resolución de problemas, colaborando de manera productiva en espacios y equipos de trabajo. - Cumple en tiempo y forma en sus obligaciones como estudiante, siguiendo las indicaciones y considerando los criterios de evaluación. - Utiliza la tecnología para apoyar su aprendizaje y para el desarrollo de habilidades metacognitivas, el aprendizaje autónomo y el longlife learning			

Bibliografía

- Anderson, R. (2008). Security Engineering. A Guide to Building Dependable Distributed Systems. Second Edition. Wiley.
- Caballero, P. (2003). Introducción a la criptografía. Segunda edición. México, Distrito Federal: Alfaomega.
- Cervantes, P. y Tauste, O. (2016). Internet negro. El lado oscuro de la red. Cd. de México, Paidós.
- Daltabuit, E.; Hernández, L.; Mallén, G. y Vázquez, J.J. (2007). La seguridad de la información. Ciudad de México:Limusa.
- Greenwald, G. (2014). Snowden. Sin un lugar donde esconderse. Ciudad de México: Ediciones B.
- Hook, D. (2005). Beginning Cryptography in Java. Indianapolis: Wiley.
- Kahn, D. (1973). The codebreakers. The story of secret writing. Chicago: New American Library.
- Knudsen, J. (2008). Java Cryptography. O'Reilly.
- Maiorano, A. (2009). Criptografía. Técnicas de desarrollo para profesionales. Ciudad de México: Alfaomega.
- Pfleeger, C. P.; Pfleeger, S. L.; & Margulies, J. (2015). Security in computing (5a ed.). EUA: Pearson / Prentice Hall.
- Snowden, E. (2019). Vigilancia permanente. Ciudad de México: Planeta.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.3. Desglose específico de la unidad "Criptografía."

Número y nombre de la unidad:	3. Criptografía.					
Tiempo y porcentaje para esta unidad:	Teoría:	10 horas	Práctica:	10 horas	Porcentaje del programa:	22.22%
Aprendizajes esperados:	Conocer las características de la criptografía simétrica y asimétrica, certificados digitales, firma digital y protocolos criptográficos, para aplicarlos durante el desarrollo profesional de proyectos que requieren una seguridad confiable.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
3. Criptografía. 3.1 Criptografía simétrica. 3.2 Criptografía asimétrica. 3.3 Certificados digitales. 3.4 Firma digital. 3.5 Hash. 3.6 Protocolos. 3.7 Prácticas Criptográficas en Java.	Saber: - Conocer de manera integral, las técnicas de criptografía simétrica, criptografía asimétrica, hash, firma digital, certificados digitales y protocolos criptográficos. Saber hacer: - Manejar el protocolo de paso de llave simétricas por medio de criptografía asimétrica, garantizando autenticación, confidencialidad e integridad, y posterior establecimiento de sesiones criptográficas simétricas.	- Aplicación integrada de tecnologías complejas. - Actividades en clase como estudios de caso y prácticas.	Evaluación formativa: - Avance de prácticas. Evaluación sumativa: -Práctica de aplicación integrada de tecnologías complejas y su respectivo reporte. Instrumento : Lista de cotejo.	El reporte de la práctica debe incluir evidencia de: 1. Paso de una llave simétrica AES encriptada con llaves públicas RSA, garantizando confidencialidad, autenticación e integridad. 2. Mensajes encriptados y desencriptados por medio de AES siguiendo el protocolo entre duplas de estudiantes.

Continuación: Tabla 4.3. Desglose específico de la unidad "Criptografía."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	Ser: - Aporta puntos de vista con apertura a aprender de los otros y considera los de otras personas de manera reflexiva y respetuosa. - Participa activamente en la construcción de su aprendizaje y en la resolución de problemas, colaborando de manera productiva en espacios y equipos de trabajo. - Cumple en tiempo y forma en sus obligaciones como estudiante, siguiendo las indicaciones y considerando los criterios de evaluación. - Utiliza la tecnología para apoyar su aprendizaje y para el desarrollo de habilidades metacognitivas, el aprendizaje autónomo y el longlife learning.			

Bibliografía

- Anderson, R. (2008). Security Engineering. A Guide to Building Dependable Distributed Systems. Second Edition. Wiley.
- Caballero, P. (2003). Introducción a la criptografía. Segunda edición. México, Distrito Federal: Alfaomega.
- Cervantes, P. y Tauste, O. (2016). Internet negro. El lado oscuro de la red. Cd. de México, Paidós.
- Daltabuit, E.; Hernández, L.; Mallén, G. y Vázquez, J.J. (2007). La seguridad de la información. Ciudad de México:Limusa.
- Greenwald, G. (2014). Snowden. Sin un lugar donde esconderse. Ciudad de México: Ediciones B.
- Hook, D. (2005). Beginning Cryptography in Java. Indianapolis: Wiley.
- Kahn, D. (1973). The codebreakers. The story of secret writing. Chicago: New American Library.
- Knudsen, J. (2008). Java Cryptography. O'Reilly.
- Maiorano, A. (2009). Criptografía. Técnicas de desarrollo para profesionales. Ciudad de México: Alfaomega.

Continuación: Tabla 4.3. Desglose específico de la unidad "Criptografía."
Bibliografía
- Pfleeger, C. P.; Pfleeger, S. L.; & Margulies, J. (2015). Security in computing (5a ed.). EUA: Pearson / Prentice Hall. - Snowden, E. (2019). Vigilancia permanente. Ciudad de México: Planeta.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.4. Desglose específico de la unidad "Seguridad de operaciones."

Número y nombre de la unidad:	4. Seguridad de operaciones.					
Tiempo y porcentaje para esta unidad:	Teoría:	10 horas	Práctica:	10 horas	Porcentaje del programa:	22.22%
Aprendizajes esperados:	Conocer los estándares ISO 27000, FIPS 200 y NIST 800-53, y los procesos de seguridad de operaciones, para desarrollar proyectos de software con una seguridad confiable garantizada.					

Temas y subtemas (secuencia)	**Criterios de desempeño**	**Estrategias didácticas**	**Estrategias de evaluación**	**Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)**
4.1. Familia de estándares ISO 27000. 4.2. FIPS 200 y NIST 800-53. 4.3. Revisión de ejemplos de procesos de seguridad de operaciones. 4.4. Elaboración en equipo de un proceso de seguridad de operaciones.	Saber: - Conocer la familia de estándares ISO 27000, así como otros modelos de buenas prácticas de seguridad. Saber hacer: - Practicar la elaboración de un proceso de seguridad de operaciones en duplas. Ser: - Aporta puntos de vista con apertura a aprender de los otros y considera los de otras personas de manera reflexiva y respetuosa.	- Aprendizaje basado en estudio de casos. - Trabajo colaborativo.	Evaluación formativa: - Estudio de casos. Instrumento: Lista de cotejo. Evaluación sumativa: - Prácticas y su reporte. Instrumento: Lista de cotejo.	El proceso elaborado en equipo debe incluir: Prácticas alineadas con un estándar internacional de seguridad. Cumplimiento de requerimientos de un estándar internacional de seguridad.

Continuación: Tabla 4.4. Desglose específico de la unidad "Seguridad de operaciones."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	- Participa activamente en la construcción de su aprendizaje y en la resolución de problemas, colaborando de manera productiva en espacios y equipos de trabajo. - Cumple en tiempo y forma en sus obligaciones como estudiante, siguiendo las indicaciones y considerando los criterios de evaluación. - Utiliza la tecnología para apoyar su aprendizaje y para el desarrollo de habilidades metacognitivas, el aprendizaje autónomo y el longlife learning.			

Bibliografía

- Anderson, R. (2008). Security Engineering. A Guide to Building Dependable Distributed Systems. Second Edition. Wiley.
- Caballero, P. (2003). Introducción a la criptografía. Segunda edición. México, Distrito Federal: Alfaomega.
- Cervantes, P. y Tauste, O. (2016). Internet negro. El lado oscuro de la red. Cd. de México, Paidós.
- Daltabuit, E.; Hernández, L.; Mallén, G. y Vázquez, J.J. (2007). La seguridad de la información. Ciudad de México:Limusa.
- Greenwald, G. (2014). Snowden. Sin un lugar donde esconderse. Ciudad de México: Ediciones B.
- Hook, D. (2005). Beginning Cryptography in Java. Indianapolis: Wiley.
- Kahn, D. (1973). The codebreakers. The story of secret writing. Chicago: New American Library.
- Knudsen, J. (2008). Java Cryptography. O'Reilly.
- Maiorano, A. (2009). Criptografía. Técnicas de desarrollo para profesionales. Ciudad de México: Alfaomega.
- Pfleeger, C. P.; Pfleeger, S. L.; & Margulies, J. (2015). Security in computing (5a ed.). EUA: Pearson / Prentice Hall.
- Snowden, E. (2019). Vigilancia permanente. Ciudad de México: Planeta.

V. Perfil docente

Tabla 5. Descripción del perfil docente

Perfil deseable docente para impartir la asignatura
Carrera(s): - Ingeniería en Tecnologías de software. - Ingeniería en Informática. - Ingeniería o Licenciatura en Computación, o carrera afín. - Licenciatura en Informática o Sistemas Computacionales o Maestría relacionada con el área de conocimiento. o carrera afín - Experiencia profesional relacionada con la materia. - Experiencia mínima de dos años - Licenciatura o Ingeniería en Informática o Sistemas Computacionales o Maestría relacionada con el área de conocimiento.