Desarrollo de Software
8º Semestre

Programa de la unidad didáctica:
Seguridad de la informática

Información general de la unidad didáctica

Clave:
15144844

Ciudad de México, febrero de 2025

Universidad Abierta y a Distancia de México

DCEIT

Índice

I. Información general de la unidad didáctica 3
a. Ficha de identificación 3
b. Descripción de la unidad didáctica 3
c. Propósitos 4
d. Competencias a desarrollar 6
e. Contenidos nucleares 6
f. Metodología de trabajo 8
g. Evaluación 8
h. Fuentes de consulta básica 10

I. Información general de la unidad didáctica

a. Ficha de identificación

Carrera:	Ingeniería en Desarrollo de Software
Nombre del curso o unidad didáctica:	Seguridad de la informática
Semestre:	Octavo
Horas contempladas:	72 horas

b. Descripción de la unidad didáctica

Ante las grandes ventajas del uso de internet y de sistemas de comunicación en red, así como a su cada vez más variada capacidad de acceso a la información, las organizaciones hoy cuentan con diversas posibilidades de acceso a sus sistemas de información. Por ello es fundamental analizar sus necesidades de seguridad tanto para el acceso como para la manipulación y administración de información, con el fin de implementar sistemas de protección y control de acceso a la información por parte de los usuarios del sistema de información.

Esta unidad didáctica aporta al perfil de ingeniero de Desarrollo de Software las capacidades para identificar necesidades de seguridad en un sistema de información, además de seleccionar y utilizar de manera óptima técnicas y herramientas más eficaces de protección de la información.

La unidad didáctica se ubica en el octavo semestre de la ingeniería en Desarrollo de software y guarda una estrecha relación con las unidades didácticas *Programación net I*, *II* y *III* e *Interconectividad de redes*, en las cuales revisaste conceptos como encapsulación, Criptología y esteganografía, mecanismos de seguridad, firmas y certificados digitales, criptografía, políticas de seguridad, etcétera, todos éstos dirigidos a intensificar las medidas de seguridad. Asimismo, esta unidad didáctica se relaciona con *Programación web II*, donde revisaste lo correspondiente al acceso seguro a bases de datos mediante la web.

Son recurrentes las fallas en los sistemas de protección de los servidores más utilizados, por ejemplo Apache o IIS. Es posible afirmar que la mayoría de los problemas de seguridad en los sitios web se encuentran a nivel de aplicación y, por tanto, son el resultado de la escritura defectuosa de código. Para asegurar la información en un sistema de información es necesario que el programador visualice una concepción

general de los riesgos que puede correr la información contenida, solicitada y recibida por el sistema. Ante tales riesgos puntos, la unidad didáctica *Seguridad de la informática*, ofrece al desarrollador de software las herramientas más importantes para poder analizar, diseñar, gestionar e implementar protocolos y planes de seguridad de protección de información, puesto que el propósito de la seguridad de la informática es proteger información, independientemente del lugar en el que se localice, así como los equipos que la albergan y las personas que las utilizan; es decir, proteger a todo el sistema informático.

Esta unidad didáctica está conformada por tres unidades, en la *Unidad 1. Principios básicos de la seguridad de la informática,* se revisará la situación actual de la información que es el objeto de mayor valor en las organizaciones, por tanto, su seguridad afecta directamente a las empresas, e incluso a las personas individualmente. En el transcurso de esta unidad, identificarás los conceptos relacionados con la seguridad en los sistemas de información, la clasificación de la seguridad informática y el malware. Además, revisarás información acerca de la informática forense y la legislación de la seguridad informática en México.

Por su parte, en la *Unidad 2. Mecanismos criptográficos en los sistemas informáticos* se abordarán los mecanismos de seguridad en los sistemas informáticos, redes, sistemas operativos y bases de datos. Mediante la criptografía es posible restringir el acceso a emisores y/o receptores potenciales de un mensaje. Durante esta unidad conocerás con mayor profundidad la criptografía, los certificados y firmas digitales. Por último, en la *unidad 3. Gestión y aplicación de protocolos de seguridad informática* se explicarán los protocolos de seguridad en los cuales se definen los lineamientos que gobiernan las comunicaciones para que el sistema pueda soportar ataques. Estos protocolos están diseñados con ciertas premisas con respecto a los riesgos a los que está expuesto un sistema de información. En esta unidad también se abordarán el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación de desastre (DRP), así como las nuevas tecnologías de seguridad de la informática.

c. Propósitos

Al finalizar la unidad didáctica, el alumno será capaz de:

- Identificar los conceptos básicos relacionados con la seguridad de la informática.
- Identificar el código malicioso, así como posibles soluciones para contrarrestarlo.
- Aplicar estándares y políticas de seguridad informática en los ámbitos relacionados a una organización o personales en el marco legal nacional e internacional.
- Identificar los elementos que intervienen en la seguridad de la información para comprender cómo se relacionan con los diversos campos de la informática, analizando

su criptografía y certificación, en base a los estándares y protocolos de certificación digital.

- Determinar la vulnerabilidad de un sistema de información y los mecanismos de seguridad pertinentes.
- Aplicar los planes de Continuidad de Negocio (BCP) y de Recuperación de desastre (DRP) en el desarrollo de un proyecto.

d. Competencias a desarrollar

Competencia general:

- Aplicar arquitecturas criptográficas para implementar sistemas de seguridad informática en una organización contribuyendo al fomento de la cultura de la seguridad informática mediante la metodología de análisis y gestión de riesgos BCP y DRP.

Competencias específicas:

- Identificar las características de un código malicioso para prevenir posibles riesgos en los sistemas de información mediante la aplicación de la triada de la seguridad informática con base en el marco legal de seguridad de la informática nacional e internacional.
- Desarrollar código criptográfico para implementar mecanismos de seguridad de acuerdo a las necesidades de la organización o del usuario en un sistema informático mediante estándares, protocolos de certificación y firmas digitales.
- Evaluar los tipos de amenazas y riesgos en los sistemas informáticos para gestionar la protección de información de acuerdo con las necesidades de la organización o del usuario utilizando la metodología para el desarrollo de proyectos de seguridad informática.

e. Contenidos nucleares

Unidad 1. Principios básicos de la seguridad informática

1.1. La seguridad en los sistemas de información
- 1.1.1. Triada de la seguridad: confidencialidad, integridad, disponibilidad
- 1.1.2. Niveles de seguridad
- 1.1.3. Análisis de riesgos y amenazas

1.2. Clasificación de la seguridad informática
- 1.2.1. Seguridad física
- 1.2.2. Seguridad lógica

1.3. Malware
- 1.3.1. Tipos de malware
- 1.3.2. Prevención y desinfección de malware
- 1.3.3. Marco legal de seguridad de la informática nacional e internacional

Unidad 2. Mecanismos criptográficos en los sistemas informáticos

2.1. Criptografía
2.1.1. Clasificación de los algoritmos criptográficos
2.1.1.1. Algoritmos criptográficos de clave privada
2.1.1.2. Algoritmos criptográficos de clave pública
2.1.1.3. Aplicaciones de la criptografía
2.2. Certificados y firmas digitales
2.2.1. Infraestructuras de clave pública PKI
2.2.2. Estándares y protocolos de certificación digital
2.2.3. Configuración de aplicaciones para el reconocimiento de certificados digitales
2.2.4. Configuración de aplicaciones para el reconocimiento de firmas digitales

Unidad 3. Gestión y aplicación de protocolos de seguridad informática

3.1. Mecanismos de seguridad en los sistemas informáticos: redes, sistemas operativos, bases de datos.

- Vulnerabilidades en TCP/IP
- Aplicaciones de software en la seguridad de los sistemas informáticos

3.2. Metodología para el desarrollo de proyectos de seguridad informática
3.2.1. Plan de Continuidad de Negocio (BCP)
3.2.2. Plan de Recuperación de desastre (DRP)
3.3. Nuevas tecnologías de seguridad de la informática

f. Metodología de trabajo

La metodología de trabajo para el estudio de esta unidad didáctica pretende relacionar los conceptos de un sistema de seguridad, especialmente la determinación de las necesidades de protección, el análisis y la gestión de los riesgos de los sistemas informáticos y los protocolos para implementar los controles, que incluyen políticas, procedimientos y funciones de seguridad que requieren ser mejorados para asegurar que cumplan los objetivos de seguridad.

Las actividades contenidas en esta unidad didáctica tienen como propósito determinar y analizar la efectividad de la seguridad informática de una organización mediante los elementos básicos para aplicar las medidas correctivas necesarias. Dichas actividades estarán apoyadas con Java para la aplicación de código de criptografía.

En la Unidad 1, realizarás un análisis sobre la importancia de la seguridad informática y como evidencia de aprendizaje plantearás la primera fase de un proyecto de seguridad informática que desarrollarás en el transcurso de la unidad didáctica.

En la Unidad 2, realizarás la segunda fase de tu proyecto de seguridad informática incluyendo estándares, protocolos y técnicas criptográficas, para implementar mecanismos de seguridad en tu proyecto de seguridad informática.

En la Unidad 3, evaluarás los tipos de amenazas y riesgos en los sistemas informáticos para gestionar la protección de información realizando la tercera y última fase de tu proyecto de seguridad informática.

g. Evaluación

La evaluación del aprendizaje es un proceso, a través del cual se observa, recoge y analiza información relevante del proceso de aprendizaje de los estudiantes, con la finalidad de reflexionar, emitir juicios de valor, así como tomar decisiones pertinentes y oportunas para optimizarlo (Díaz Barriga A.F. & Hernández R.G., 2005). Orienta la toma de decisiones, da pauta a determinar acciones en términos de valoración de conocimientos, nivel del desempeño, reorientaciones de aprendizaje, mejora del proceso educativo y adecuación de actividades, entre otras acciones.

De acuerdo con lo anterior, mediante la evaluación te brindaremos apoyo y seguimiento para identificar las dificultades en el desarrollo de conocimientos, habilidades y actitudes del proceso integral de aprendizaje.
En el marco del Modelo educativo de la UnADM, la evaluación de la unidad didáctica se realiza en los siguientes momentos:1) formativa y 2) sumativa.

EVALUACIÓN FORMATIVA

Se realiza en paralelo al desarrollo del proceso de enseñanza-aprendizaje de cada unidad, y sirve para localizar dificultades cuando aún estás en posibilidad de remediarlas.

En este primer momento de evaluación, se aplican estrategias asociadas a las:

- Actividades individuales (tareas). Se trata de un primer momento de aprendizaje, en el cual se consideran tus perspectivas, experiencias, intereses, capacidades y necesidades.
- Actividades colaborativas (foros). El trabajo colaborativo fomenta y promueve el aprendizaje en contribución con otros compañeros, ya que eres responsable no sólo de tu aprendizaje, sino de contribuir a que los demás aprendan en equipo y se fomente un ambiente de confianza; por ende, que se logren las metas de aprendizaje.

EVALUACIÓN SUMATIVA

Se aplica al final del proceso de tu experiencia de aprendizaje, su propósito es verificar los resultados alcanzados y el grado de aprendizaje o nivel de conocimientos, habilidades y actitudes que hayas adquirido.

Este segundo y último momento de evaluación, se mide y valora a través de las siguientes actividades:

- Evidencias de aprendizaje. Son actividades que tienen como objetivo integrar el proceso de construcción de tu aprendizaje, la evaluación, la retroalimentación y la planeación de la nueva ruta de aprendizaje que seguirás de acuerdo con los resultados individuales obtenidos.
- Actividad complementaria. Esta actividad es planeada por la figura académica considerando las competencias y logros de la unidad didáctica, toda vez que identifica los conocimientos, habilidades y actitudes que te hizo falta desarrollar o potenciar (se realiza en una ocasión al finalizar la última unidad).
- Actividad de reflexión. Es un ejercicio de metacognición que permite que tomes conciencia de tu proceso de aprendizaje, el punto de partida son las experiencias del contexto académico y la reflexión sobre tu desempeño. Se trata de una acción

formativa que parte de tu persona y no del saber teórico, que considera tu experiencia de aprendizaje (se realiza en una ocasión al finalizar la última unidad).

A continuación, se presenta el esquema general de evaluación correspondiente a esta unidad didáctica:

Esquema general de evaluación		
Tipo de evaluación	**Actividades**	**Puntaje**
Formativa	Actividades individuales	20%
	Actividades colaborativas	20%
Sumativa	Evidencias de aprendizaje	40%
	Actividad complementaria	10%
	Actividad de reflexión	10%
Total		**100%**

Recuerda que la calificación final que te permitirá acreditar, se asigna de acuerdo con los criterios e instrumentos de evaluación establecidos para cada actividad, los cuales son diseñados con base en las competencias y logros de esta unidad didáctica.

h. Fuentes de consulta básica

- Ángel, A. J. J. (2005). *AES Advanced Encryption Standard*. https://xdoc.mx/documents/aes-advanced-encryption-standard-5f2c67e7409e3
- Anónimo (2000). *Linux máxima seguridad: edición especial*. Tr. José Arroyo. Madrid: Prentice Hall.
- Areitio, J. (2008). *Seguridad de la informática, redes, informática y sistemas de información*. Madrid: Paraninfo. ISBN 8497325028, 9788497325028
- Aguirre, J. R. (1999). *Aplicaciones criptográficas*. 2ª Ed. Madrid: Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid. ISBN 83-87238-57-2.

- Aguirre, J. R. (2003). *Libro electrónico de seguridad informática y criptografía*. ISBN 84-86451-69-8. https://n9.cl/j91bd

- Aguilera, P. (2011). *Seguridad del software (Seguridad informática).* Madrid: Editex ISBN 8490031118, 9788490031117

- Baéz R., y Mina P. (2013). *Metodología para el desarrollo de firewalls de software mediante Java*. Capítulo 2. Seguridad de una red. En: Universidad Técnica del Norte. http://repositorio.utn.edu.ec/bitstream/123456789/1106/2/04%20ISC%20010%20Cap%C3%ADtulo%202.pdf

- Bustamante, S. R. (2013). *Seguridad en redes*. México: Universidad Autónoma del Estado de Hidalgo Instituto de Ciencias Básicas e ingeniería.

- Cámara de diputados H. Congreso de la Unión. (2023). *Código Penal Federal*. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

- Cámara de diputados H. Congreso de la Unión. (2022). *Constitución Política de los Estados Unidos Mexicanos*. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

- Cámara de diputados H. Congreso de la Unión. (2013). *Gaceta Parlamentaria Número 3749-VII*. http://gaceta.diputados.gob.mx/Gaceta/62/2013/abr/20130416-VII.html

- Cano-Barrón, J. E., Martínez-Peláez, R., Soriano, M. (octubre, 2007). Current problems and challenges in developing a standard digital rights management system. En: *5th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods (incorporating the 3rd International ODRL Workshop).* Alemania: Koblenz.

- Cassou, R. J. E. (Julio 2009). Delitos Informáticos en México. En *Revista del Instituto de la Judicatura Federal*. No. 28. México: Poder Judicial de la Federación.

- CNN CERT(s/f) .*EAR / PILAR-Entorno de análisis de riesgos*. Disponible en https://n9.cl/certear

- Corleti, A. (2011). *Seguridad por niveles*. Madrid: Learning Consulting S.L. Licencia Creative Commons CC. Disponible en https://www.academia.edu/10480379/Seguridad_por_niveles

- Corrales, A.L., Beltrán, M., Guzmán, A. (2006). *Diseño e implantación de arquitecturas informáticas seguras. Una aproximación práctica*. Madrid: Universidad Rey Juan Carlos, Dikinson.
ISBN 8499823475, 9788499823478

- Cuenca, D. L. (2012). *Análisis de riesgos dinámicos en sistemas de información.* Madrid: Universidad Complutense de Madrid: Facultad de Informática. Disponible en http://eprints.ucm.es/16931/1/PFM_2012_-_David_L%C3%B3pez_Cuenca_-_An%C3%A1lisis_de_Riesgos_Din%C3%A1micos_en_Sistemas_de_Informaci%C3%B3n.pdf

- Gómez L.O.D. (2011). *Administración de sistemas operativos. Ciclos formativos de grado superior.* Madrid: RA-MA

- Gómez, V.A. (2011). *Enciclopedia de la seguridad informática*. 2ª Edición. México: Alfaomega-Ra-Ma.

- Gutiérrez, A. H. C. (30 de julio, 2014). Lo que no debes pasar por alto para gestionar la seguridad de la información. En *Revista Seguridad defensa digital*. *Protección de datos.* No. 22., pp. 4-6.

- IFAI Instituto Federal de Acceso a la Información y Protección de Datos. (2014). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* México: Secretaría de Protección de Datos Personales.

- Jara, H. y Pacheco F. G. (2012). *Ethical Hacking 2.0.* 1ª. Ed. Buenos Aires: Sevagraf.

- López, P. A. (2011). *Seguridad Informática*. Madrid: Editex.

- Lucena, M. J. (2007*). Criptografía y seguridad en computadores*. 4ª E. Jaén: Universidad de Jaen. https://www.u-cursos.cl/ingenieria/2010/2/EL65C/1/material_docente/bajar?id_material=311979

- Ministerio de Educación, Cultura y Deporte. (2012). *Seguridad de la información / Seguridad informática.* Madrid: Observatorio Tecnológico

- Moragues, F. J.; Peñarrubia, C. J. P., Rosell, T.J. M. (2014). *Seguridad para todos en la sociedad de la información.* Valencia: COIICV Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana.

- Rifà, P. H., Serra, R. J. y Rivas L. J. L. (2009). *Análisis forenses de sistemas informáticos*. 1ª Edición. Barcelona: UOC Universitat Oberta de Catalunya

- SEGOB (2014). Código Penal Federal. *Última Reforma DOF 14-07-2014.*

- SEGOB (2014). *Gaceta Parlamentaria*. Número 3749-VII.

- Singh, S. (2000). *Los códigos secretos. El arte y la ciencia de la criptografía desde el antiguo Egipto a la era de internet*. Madrid: Editorial Debate.
  ISBN: 84-8306-278-X.

- Stallings, W. (2003). *Fundamentos de seguridad en redes: aplicaciones y estándares*. Madrid: Pearson Educación-Prentice Hall.
  ISBN 8420540021, 9788420540023

- Téllez V. J. (2004). *Derecho informático.* 3ª. Ed. México: McGraw-Hill.

- UAH Universidad de Alcalá de Henares (n.d. 1). *Niveles de seguridad*.

- UAH Universidad de Alcalá de Henares (n.d. 2). P*rotección de datos de carácter personal*.

- Villalón, A. H. (2000). *Seguridad en Unix y Redes.* Valencia: UPV Universidad Politécnica de Valencia. https://www.rediris.es/cert/doc/unixsec/unixsec.pdf

- Voutssas, M.J. (2010). *Preservación documental digital y seguridad informática*. México: Centro Universitario de Investigaciones Bibliotecológicas UNAM.

- Zahumenszky, C. (2013) *Así se programaron los virus más destructivos de la historia*. http://es.gizmodo.com/asi-se-programaron-los-virus-mas-destructivos-de-la-his-678700816