PROGRAMA ANALÍTICO

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
Facultad de Contaduría Pública y Administración

LICENCIATURA EN TECNOLOGÍAS DE INFORMACIÓN

1. DATOS DE IDENTIFICACIÓN

Nombre de la Unidad de Aprendizaje	ACFP IV (Tecnologías de Información VII)
Horas de Trabajo Presenciales	**3**
Horas de Trabajo Extra – Aula	**3**
Modalidad	**Presencial**
Período Académico	Séptimo semestre
Área Curricular	Formación Básica Profesional
Unidad de Aprendizaje	Obligatoria
Créditos	**3**
Fecha de Elaboración	Diciembre 2014
Fecha de la Última Actualización	Noviembre 2019
Responsable del Diseño	M.T.I. Ahelí De Alba Guerra
Responsable de Actualización	M.T.I. Ahelí De Alba Guerra

2. PRESENTACION

Esta unidad de aprendizaje contribuye al desarrollo de una formación integral del estudiante a través de algunos aspectos como:

- Contribuir en el desarrollo de la formación del estudiante a través del trabajo individual y por equipo que le permita un mejor desenvolvimiento en el contexto de la seguridad informática, específicamente en analizar y gestionar los riesgos de un sistema informático.
- Capacitar a los alumnos en elaborar planes y procedimientos de seguridad informática así como la detección de amenazas y vulnerabilidades de los sistemas informáticos.
- Facultar a los alumnos en el ejercicio práctico del proceso de la identificación de los delitos informáticos y su tratamiento.

3. PROPÓSITO(S)

1. Aplicar los principios básicos de la seguridad informática
2. Analizar y gestionar los riesgos de un sistema informático
3. Elaborar planes y procedimientos de seguridad informática
4. Identificar las amenazas y vulnerabilidades de los sistemas informáticos
5. Comprender los conceptos relacionados con la seguridad informática:
    a. Autenticación y autorización de usuarios
    b. Sistemas biométricos

c. Criptografía
d. Marcas de agua
e. Firma electrónica

6. Identificar la seguridad en redes:
   a. Privadas
   b. Virtuales
   c. Inalámbricas

7. Identificar los delitos informáticos y su tratamiento

4. COMPETENCIAS DEL PERFIL DE EGRESO

COMPETENCIAS GENERALES

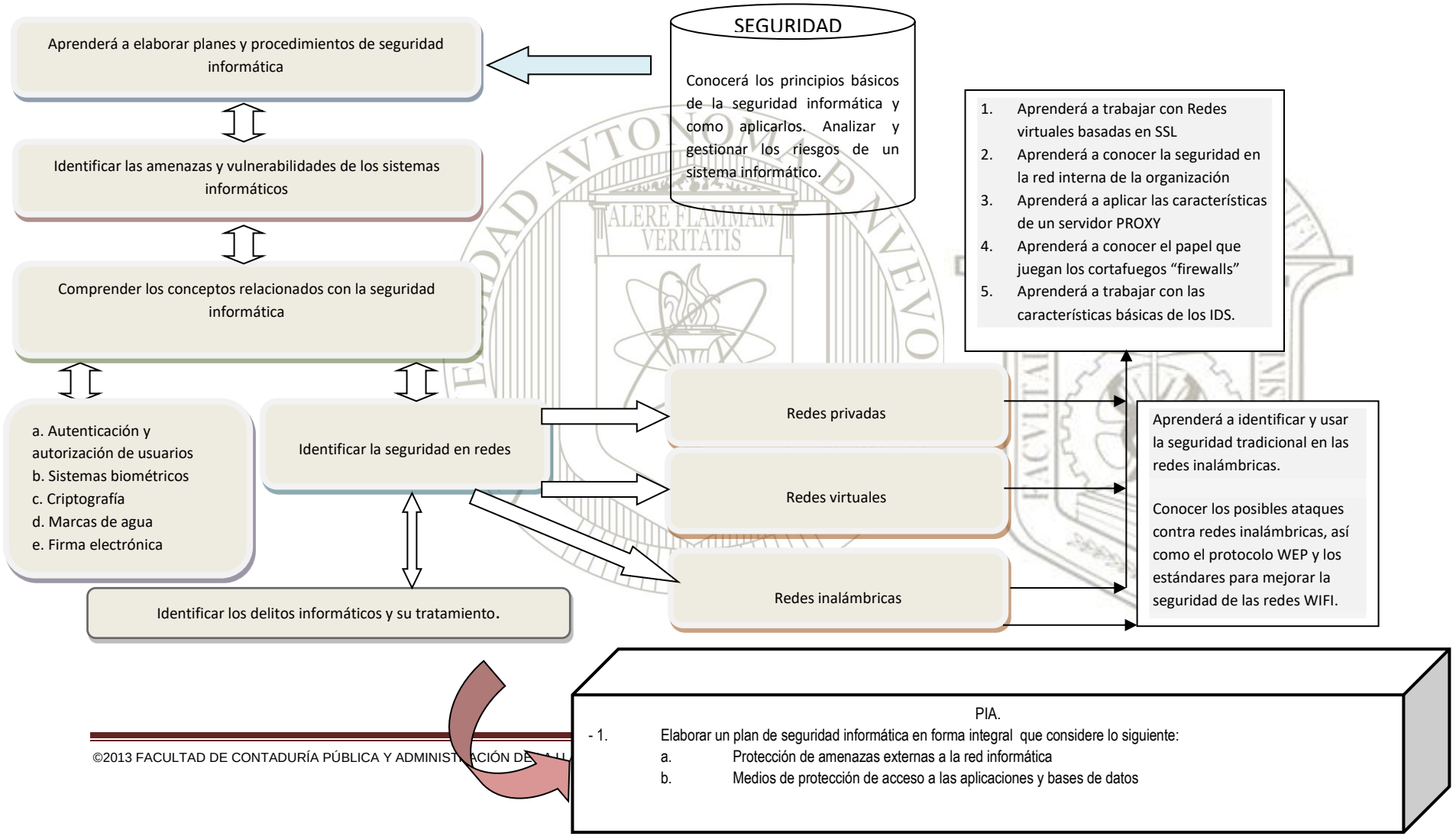
Esta unidad de aprendizaje se vincula con las competencias generales de formación universitaria que corresponden :

1. Capacidad para un aprendizaje autónomo y continuo.
2. Compromiso profesional y humano frente a los retos de la sociedad contemporánea en lo local y global.
3. Práctica de reflexión ética y ejercicio de los valores promovidos por la UANL, tales como verdad, solidaridad, responsabilidad, libertad, justicia, equidad y respeto a la vida.
4. Capacidad de trabajo inter, multi y transdisciplinario.
5. Habilidad para la generación y aplicación del conocimiento.
6. Capacidad para integrarse en situaciones sociales, cambiantes y profesionales.
7. Capacidad de ejercicio de un liderazgo comprometido con las necesidades sociales y profesionales.
8. Capacidad para la solución de problemas y la adecuada toma de decisiones.
9. Comunicar mensajes en forma apropiada en lengua materna para interactuar de manera eficiente en contextos pluridimensionales: emocional, intelectual y social.
10. Desarrollar diversas expresiones del pensamiento: lógico, crítico y creativo, a partir de la selección de información relevante en torno a diversos materiales con el fin de sintetizarla y analizarla.
11. Utilizar las tecnologías de la información y comunicación de manera ética y pertinente para realizar investigaciones temáticas que complementen la información sobre la unidad de aprendizaje.
12. Utilizar diversos lenguajes: lógico, formal, icónico, verbal y no verbal con miras a desarrollar el trabajo colaborativo e interdisciplinario, tanto en el aula como en el contexto profesional.
13. Explicar y argumentar de manera oral y escrita su propia opinión respetando y valorando la opinión de los demás.
14. Desarrollar una actitud analítica y crítica para orientarla a la generación de ideas.

COMPETENCIAS ESPECÍFICAS

1. Aplicar los principios de seguridad informática
2. Elaborar planes de seguridad informática
3. Desarrollar una estrategia de seguridad informática

5. REPRESENTACIÓN GRÁFICA



6. ESTRUCTURA EN CAPÍTULOS, ETAPAS, O FASES DE LA UNIDAD DE APRENDIZAJE.

Elementos de competencia: Seguridad Informática

- Conocerá los principios básicos de la seguridad informática y como aplicarlos.
- Analizar y gestionar los riesgos de un sistema informático

Evidencias de aprendizaje (2)	Criterios de desempeño (3)	Actividades de aprendizaje (4)	Contenidos (5)	Recursos (6)
Evidencia No. 1: Elaboración de material que evidencie el conocimiento, el análisis y la gestión de la seguridad informática	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, una síntesis, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada. -. Otros a elección.

Elementos de competencia: Seguridad Informática

- Elaborar planes y procedimientos de seguridad informática

Evidencias de aprendizaje (2)	**Criterios de desempeño (3)**	**Actividades de aprendizaje (4)**	**Contenidos (5)**	**Recursos (6)**
Evidencia No. 2: Elaboración de material que evidencie el conocimiento, y aplicación en la elaboración de planes y procedimientos de seguridad informática.	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, un esquema, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada. -. Otros a elección.

Elementos de competencia: Seguridad Informática

- Identificar las amenazas y vulnerabilidades de los sistemas informáticos

Evidencias de aprendizaje (2)	**Criterios de desempeño (3)**	**Actividades de aprendizaje (4)**	**Contenidos (5)**	**Recursos (6)**
Evidencia No. 3: Elaboración de material que evidencie el conocimiento de las amenazas y vulnerabilidades de los sistemas informáticos.	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, un esquema, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada. -. Otros a elección.

Elementos de competencia: Seguridad Informática

- Comprender los conceptos relacionados con la seguridad informática
- a. Autenticación y autorización de usuarios
- b. Sistemas biométricos
- c. Criptografía
- d. Marcas de agua
- e. Firma electrónica

Evidencias de aprendizaje (2)	**Criterios de desempeño (3)**	**Actividades de aprendizaje (4)**	**Contenidos (5)**	**Recursos (6)**
Evidencia No. 4: Elaboración de material que evidencie el conocimiento y aplicación de: a. Autenticación y autorización de usuarios b. Sistemas biométricos c. Criptografía d. Marcas de agua e. Firma electrónica	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, un esquema, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada. -. Otros a elección.

Elementos de competencia: Identificar la seguridad en redes

- Privadas
- Virtuales
- Inalámbricas

Evidencias de aprendizaje (2)	**Criterios de desempeño (3)**	**Actividades de aprendizaje (4)**	**Contenidos (5)**	**Recursos (6)**
Evidencia No. 5: Elaboración de material que evidencie el conocimiento y aplicación de la seguridad en redes privadas, virtuales e inalámbricas.	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, un esquema, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada.

				-. Otros a elección.

Elementos de competencia: Identificar la seguridad en redes

- Identificar los delitos informáticos y su tratamiento

Evidencias de aprendizaje (2)	Criterios de desempeño (3)	Actividades de aprendizaje (4)	Contenidos (5)	Recursos (6)

Evidencia No. 6: Elaboración de material que evidencie el conocimiento de los delitos informáticos y su tratamiento.	Se deja a libre definición por parte del maestro lo que habrá de solicitar como evidencia, podría ser: un mapa conceptual, un video, un esquema, entre otros	Consultar en internet, libros de texto. Analizar la información consultada y recopilada y seleccionar por lo menos dos alternativas. Elaborar material a entregar como evidencia	Serán definidos por el maestro, acorde al tipo de material que haya solicitado	Internet: - Videos, blogs y/o algún material electrónico. Plataforma NEXUS. - Enciclopedia de la Seguridad Informática, 2ª edición actualizada. -. Otros a elección.

7. FACTORES A CONSIDERAR EN LA EVALUACIÓN DE LA UNIDAD

Evidencia	**Porcentaje**
Evidencias (Tareas, exposición, etc.)	20%
Examen Parcial	30%

Examen Final	30%
PIA	20%
Total	**100%**
Porcentaje Teoría	**40%**
Porcentaje Práctica	**60%**

8. PRODUCTO INTEGRADOR DE APRENDIZAJE

1. Elaborar un plan de seguridad informática en forma integral que considere lo siguiente:
   a. Protección de amenazas externas a la red informática
   b. Medios de protección de acceso a las aplicaciones y bases de datos
   c. Control de acceso a edificios por medio de dispositivos diseñados para tal efecto

9. FUENTES DE APOYO Y CONSULTA BIBLIOGRÁFICA

AUTOR	TÍTULO	EDICIÓN	EDITORIAL	PAÍS	AÑO	PÁGS	ISBN
	Informática		Ma				81-5
Purificación Aguilera López	Seguridad Informática		Editext				
Alfonso García-Cervigón Hurtado y María del Pilar Alegre Ramos	Seguridad Informática		Informática y Comunicaciones				
ACISSI	Seguridad Informática Ethical Hacking		Ediciones ENI				
Jean-Marc Royer	Seguridad en la Informática de Empresa		Ediciones ENI				

FUENTES DE APOYO Y CONSULTA HEMEROGRÁFICA

TÍTULO	PAÍS	EDITORIAL

FUENTES DE APOYO Y CONSULTA ELECTRÓNICA

TÍTULO	URL

PERFIL DEL DOCENTE

Los profesores que impartan esta asignatura deberán realizar la tarea de formar de manera integral a sus estudiantes, para lo cual deberán demostrar los siguientes rasgos mínimos:

- Poseer Licenciatura y Maestría de la carrera de Tecnologías o afines.
- Permanecer en constante renovación de su conocimiento y tiene capacidad de innovar en la enseñanza.
- Tener capacidad en el uso de las tecnologías de información, para actualizarse, para el aprendizaje autónomo. Para desarrollar competencias comunicativas.
- Domina técnicas y herramientas pedagógicas que promuevan el aprendizaje.
- Tiene capacidad para aprovechar la información disponible y generar la propia, involucrando a los estudiantes en sus tareas académicas.
- Es flexible para aceptar ideas, opiniones y propuestas de los demás, a fin de mejorar su desempeño y trabajar en equipo con espíritu de cooperación.
- Promueve y es modelo de los valores y atributos universitarios; está comprometido con la institución y sus procesos, así como con su entorno.

Anexo.

Producto integrador de aprendizaje: Plan de seguridad de TI	
Instrucciones:	Elaborar un plan de seguridad informática en forma integral para una organización que considere lo siguiente: 1. Protección de amenazas externas a la red informática 2. Medios de protección de acceso a las aplicaciones y bases de datos 3. Control de acceso a edificios por medio de dispositivos diseñados para tal efecto
Valor:	20
Criterios de evaluación:	a) Introducción en inglés y en español (Presentar caso y antecedentes) — a) 5% b) Propósito (Especificación de los beneficios esperados) (ANECA 2.2) — b) 10% c) Identificar los requerimientos funcionales de acuerdo a los criterios establecidos de seguridad esperada (ANECA 2.2) — c) 15% d) Enunciar y justificar las selecciones de algoritmos criptográficos aplicados en la solución propuesta (ANECA 2.4) — d) 5%, e) 46% e) Establecer prácticas y técnicas vigentes de seguridad informática y ciberseguridad aplicables al caso (ANECA 2.1) f) Índice congruente con el contenido — f) 3% g) Conclusiones individuales y general (Concisas y pertinentes) — g) 3% h) Competencia Comunicativa (Ortografía, Redacción y legibilidad) — h) 5% i) Fuentes y referencias — i) 3% j) Valores UANL — j) 5%
Modalidad:	Presencial y/o en línea
Subresultados ANECA	2.1. Utilizar una serie de técnicas con las que identificar las necesidades de problemas reales, analizar su complejidad y evaluar la viabilidad de las posibles soluciones mediante técnicas informáticas. 2.2 Describir un determinado problema y su solución a varios niveles de abstracción. 2.4. Escoger los patrones de solución, algoritmos y estructuras de datos apropiados.