

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA  
COORDINACIÓN DE FORMACIÓN BÁSICA  
COORDINACIÓN DE FORMACIÓN PROFESIONAL Y VINCULACIÓN  
PROGRAMA DE UNIDAD DE APRENDIZAJE

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA  
DEPARTAMENTO DE FORMACIÓN PROFESIONAL Y VINCULACIÓN  
CA-POSTULANTE  
DEC 01 2015  
E C I B

I. DATOS DE IDENTIFICACIÓN

1. Unidad Académica: Facultad de Contaduría y Administración
2. Programa (s) de estudio: Lic. en Informática 3. Vigencia del plan: 2009-2
4. Nombre de la Unidad de aprendizaje: SEGURIDAD INFORMÁTICA 5. Clave: 20646
6. HC: 2 HL 2 HT HPC HCL HE 2 CR 6
7. Ciclo Escolar: 2016-2
8. Etapa de formación a la que pertenece: TERMINAL
9. Carácter de la Unidad de aprendizaje: Obligatoria Optativa X

10. Requisitos para cursar la unidad de aprendizaje:

Formuló: Dr. Ricardo Fernando Rosales Cisneros  
Dra. Maria Del Consuelo Salgado Sotelo  
M.C. Rafael Vital Vergara

Vo.Bo. Dr. Daniel Muñoz Zapata  
Cargo: Subdirector FCA, Tijuana

Fecha: 02 Septiembre 2015

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA



FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN  
TIJUANA, B. C.

## II. PROPÓSITO GENERAL DEL CURSO

Esta unidad de aprendizaje pertenece al área de ciencias computacionales y es de carácter optativo, su propósito es que el alumno tenga bases teóricas y prácticas de la seguridad informática, con el objetivo de diseñar e implementar una estrategia de seguridad dentro de una organización. Ayudando al alumno el saber cómo conservar la integridad de la información y recursos informáticos.

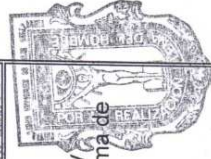
Para cursar esta materia se requiere de preferencia haber cursado las materias de redes y administración de redes del plan de estudios de Licenciado en informática, 2009-2

## III. COMPETENCIA DEL CURSO

Aplicar los conceptos teóricos prácticos (protección, identificación, autenticación, control, acceso, criptografía, seguridad), como elementos a considerar para diseñar e implementar la seguridad informática que garantice la privacidad de la información, continuidad del servicio, tratando de minimizar la vulnerabilidad de sistemas información, redes privadas y recursos informáticos, aplicando las herramientas de seguridad informática de forma ética y responsable.

## IV. EVIDENCIA (S) DE DESEMPEÑO

Resolver a través de un caso práctico una problemática específica de seguridad informática utilizando herramientas que eliminen y minimicen la vulnerabilidad de los sistemas informáticos en una organización, diseñando, desarrollando e implementando un sistema de seguridad informática.



UNIVERSIDAD AUTÓNOMA DE B.C.  
C I B I D  
DEC 01 2015  
TANTO DE FORMACION  
CAMPUS TULUM  
UNIVERSIDAD AUTÓNOMA DE B.C.  
C I B I D  
DEC 01 2015  
TANTO DE FORMACION  
CAMPUS TULUM

**V. DESARROLLO POR UNIDADES**

**Competencia:**

Explicar los aspectos generales de la seguridad informática, a través de la comprensión de las definiciones básicas (protección, identificación, autenticación, control, acceso, seguridad, ataque), para analizar soluciones de problemas de inseguridad en redes computacionales y sistema de información, con actitud crítica y actitud proactiva.

**Contenido**

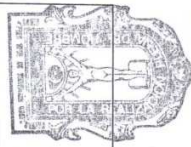
Duración 10 horas

**UNIDAD I: Introducción a la seguridad informática.**

- 1.1. Conceptos y principios de la administración de la seguridad
- 1.2. Mecanismos de protección
- 1.3. Técnicas de identificación y autenticación
- 1.4. Control de acceso
- 1.5. Administración del control de acceso
- 1.6. Mecanismos de autenticación y control de acceso
- 1.7. Métodos de ataque
- 1.8. Hackers, crackers y sus variantes

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA  
E C I B I D  
01 DIC 2015  
DEPARTAMENTO DE SERVICIOS ESTUDIANTILES Y GESTIÓN ESCOLAR

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA



FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN TULUMANA, B. C.

**V. DESARROLLO POR UNIDADES**

**Competencia:**

Identificar los principales algoritmos criptográficos y el manejo de aspectos de una llave PKI a través del criptoanálisis para identificar los algoritmos diseñados para ataques cibernéticos, con actitud crítica y actitud proactiva.

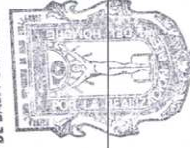
**Contenido**

**Duración 12 horas**

**Unidad II. Criptografía, Algoritmos y Mecanismos de Seguridad.**

- 2.1 Definición y usos de la Criptografía
- 2.2 Conceptos Metodologías y Prácticas criptográficas
- 2.3 Algoritmos de llaves privadas
- 2.4 Algoritmos de llave pública e infraestructura de llave publica PKI
- 2.5 Introducción al criptoanálisis
- 2.6 Uso de la criptografía dentro de los protocolos de autenticación
- 2.7 Practica de cifrado de correo electrónico

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA



FACULTAD DE CONTABILÍA  
Y ADMINISTRACIÓN  
TIJUANA, B. C.

## V. DESARROLLO POR UNIDADES

### Competencia:

Diseñar un sistema de comunicación seguro a través de la evaluación de los principales aspectos vulnerables y de protección en redes de telecomunicaciones para evitar y contrarrestar un ataque cibernético, de forma ética y responsable.

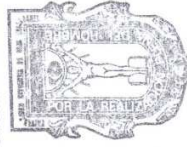
### Contenido

Duración 16 horas

#### Unidad III. Seguridad en redes y telecomunicaciones

- 3.1 Vulnerabilidades en TCP/IP
- 3.2 Internet/Intranet/Extranet
- 3.3 Traducción de direcciones de red (NAT)
- 3.4 Redes virtuales privadas (VPN)
- 3.5 Seguridad nivel red (Firewalls)
- 3.6 Seguridad nivel transporte (SSL)
- 3.7 Protocolos seguridad nivel aplicación
- 3.8 Ataques de redes y medidas preventivas
- 3.9 Monitores de redes y sniffers de paquetes
- 3.10 Seguridad en redes inalámbricas
- 3.11 Seguridad nodal
- 3.12 Seguridad Física

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA



FACULTAD DE CONTABILIDAD  
Y ADMINISTRACIÓN  
TIJUANA, B. C.

**V. DESARROLLO POR UNIDADES**

**Competencia:**

Formular un plan de administración de riesgos, por medio de la aplicación de herramientas y técnicas de seguridad informática para evitar ataques cibernéticos en redes computacionales y sistemas de información, de forma ética y responsable.

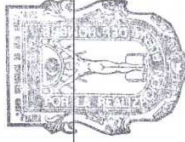
**Contenido**

**Duración 12 horas**

**Unidad IV. Análisis de riesgos en seguridad Informática**

- 4.1. Administración de riesgos.
- 4.2. Amenazas y vulnerabilidades
- 4.3. Determinación de probabilidades
- 4.4. Valuación de activos
- 4.5. Herramientas y técnicas de evaluación de riesgos
- 4.6. Metodologías de evaluación de riesgo (cualitativas y cuantitativas)

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA



FACULTAD DE CONTABILIDAD  
Y ADMINISTRACIÓN  
MEXICALTI, B. C.

**V. DESARROLLO POR UNIDADES**

**Competencia:**

Implementar un sistema de seguridad Informática adecuado, a través de análisis de las vulnerabilidades detectadas, apoyado en el plan de administración de riesgos así como de técnicas y herramientas idóneas para la estabilidad del sistema informático de una organización, de forma ética y responsable.

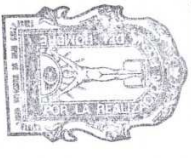
**Contenido**

**Duración 14 horas**

**Unidad V. Implementación de sistemas y herramientas de Seguridad Informática.**

- 5.1. Desarrollo de la implementación de sistemas confiables.
- 5.2. Métodos de evaluación de sistemas confiables
- 5.3. Normativa relacionada con seguridad informática
- 5.4. Herramientas de seguridad informática
- 5.5. Caso práctico: Implantación de un sistema de seguridad informática

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA  
DEPARTAMENTO DE SERVICIOS ADMINISTRATIVOS  
C I B I D U M  
01 DIC 2011



FACULTAD DE CONTABILÍA Y ADMINISTRACIÓN  
TIJUANA, B. C.

VI. ESTRUCTURA DE LAS PRÁCTICAS

No. de Práctica	Competencia(s)	Descripción	Material de Apoyo	Duración
1	<p>Conocer y utilizar el programa 1st Security Agent para proteger y asegurar computadoras basadas en Sistema Operativo Windows. Con compromiso y responsabilidad.</p>	<p>Realizar y completar la instalación del programa 1st. Security Agent, cambiar la contraseña como lo señala el profesor, establecer las restricciones de usuario señaladas, realizar las pruebas de desempeño correspondientes verificando que las restricciones apliquen adecuadamente, quitar las restricciones y restablecer el equipo a su estado original, elaborar y entregar reporte de la práctica en la fecha indicada por el Maestro</p>	<p>Software 1st. Security Agent. Computadora. Bibliografía Equipo de cómputo</p>	<p>3 horas</p>
2	<p>Conocer y utilizar el programa Access Lock para proteger y asegurar una computadora cuando el usuario se encuentre fuera. Con compromiso y responsabilidad.</p>	<p>Realizar y completar la instalación del programa Access Lock, cambiar las diferentes opciones como lo señala el profesor, realizar las pruebas de desempeño correspondientes verificando que las restricciones apliquen adecuadamente, quitar las restricciones y restablecer el equipo a su estado original, elaborar y entregar reporte de la práctica en la fecha indicada por el Maestro.</p>	<p>Software Access Lock Computadora. Bibliografía Equipo de cómputo.</p>	<p>3 horas</p>
3	<p>Conocer y utilizar el programa Lock Down Plus PC para prevenir a usuarios no autorizados contra el borrado de archivos y aplicaciones críticos, cambios no deseados en el escritorio, prevención contra instalación de programas no autorizados, así como descargas no permitidas desde Internet. Con compromiso y responsabilidad.</p>	<p>Realizar y completar la instalación la instalación del programa Lock Down Plus PC, cambiar las diferentes opciones como lo señala el profesor, realizar las pruebas de desempeño correspondientes verificando que las restricciones apliquen adecuadamente, quitar las restricciones y restablecer el equipo a su estado original, elaborar y entregar su reporte de la práctica en la fecha indicada por el Maestro.</p>	<p>Software Lock Down Plus PC. Computadora. Bibliografía Equipo de cómputo.</p>	<p>4 horas</p>

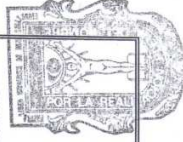




<p>4</p>	<p>Conocer y utilizar el programa de Auditoria de Seguridad en la Red: Nsauiditor, para auditar y monitorear la red de computadoras de posibles vulnerabilidades, revisar y detectar posibles brechas de seguridad que podrían ser utilizados por los hackers para atacar la red y crear un reporte de problemas potenciales de seguridad encontrados. Con compromiso y responsabilidad.</p>	<p>Realizar y completar basado en las instrucciones del maestro la instalación del programa Nsauiditor, realizar las diferentes funciones como lo señala Maestro, realizar las pruebas de desempeño correspondientes verificando que las funciones apliquen adecuadamente, elaborar y entregar su reporte de la práctica en la fecha indicada por el Maestro.</p>	<p>Software Nsauiditor Computadora. Bibliografía de Equipo de cómputo.</p>	<p>6 horas</p>
----------	--	---	--	----------------

<p style="text-align: center;"><b>VII. METODOLOGÍA DE TRABAJO</b></p> <ul style="list-style-type: none"> <li>• Exposición por parte del profesor (material didáctico, herramientas de seguridad, ejemplificaciones de escenarios de seguridad informática, diseño de red, formulación de plan de riesgos, ejemplificación de implementación de sistemas y herramientas de Seguridad Informática).</li> <li>• Exposición por parte del alumno (Prácticas con uso de herramientas, diseño de red, implementación de sistema de seguridad informática aplicado en caso práctico, exposición de caso práctico).</li> <li>• Incentivar al alumno a investigar.</li> <li>• Investigación por parte del alumno.</li> <li>• Resolución de problemas en clase.</li> <li>• Prácticas en clase y extra clase.</li> <li>• Elaboración de Caso Práctico.</li> </ul>
--

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA



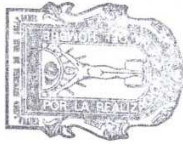
FACULTAD DE CONTABILIDAD Y ADMINISTRACIÓN Tijuana, B. C.

VIII. CRITERIOS DE EVALUACIÓN

- Evaluación parcial de las unidades 30%
- Prácticas 30%
- Resolución de caso práctico 30%
- Exposición de caso práctico 10%

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA  
E C I B I D  
9 1 Dic 2015  
E C I B I D  
SECRETARÍA DE INVESTIGACIONES  
E C I B I D

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA



FACULTAD DE CIENCIAS  
Y ADMINISTRACIÓN  
TELICANA, B. C.

IX. BIBLIOGRAFÍA	
Básica	Complementaria
<p><b>Auditoría de seguridad informática.</b> Gómez Vieites, Alvaro. Ed. StarBook, 2013. ISBN: 9789587620856</p> <p><b>Inseguridad de la información: una visión estratégica</b> Cano Martínez, Jeimy José. Ed. Alfaomega, 2013. ISBN: 9789586828444.</p> <p><b>Enciclopedia de la seguridad informática</b> Gómez Vieites, Alvaro. Ed. Alfaomega, 2011. ISBN: 9786077071815.</p> <p><b>Seguridad informática.</b> María del Pilar Alegre Ramos, Alfonso García-Cervigón Hurtado Ed. Paraninfo, 2011. ISBN: 9788497328128.</p>	<p><b>Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones,</b> Jean-Marc Royer Ed. Eni ediciones. ISBN: 2746023040.</p> <p><b>Computer Security Basics</b> Rick Lehtinen, G. T., Sr. Gangemi Ed. O'Reilly, 2006. ISBN: 9780596006693.</p> <p><b>Practical cryptography</b> Niels Ferguson, Bruce Schneier Ed. Wiley, 2003. ISBN: 9780471223573.</p> <p><b>Ingeniería de proyectos informáticos: actividades y procedimientos</b> Ed. José Salvador Sánchez Garreta Universitas, 2003. ISBN: 8480214082.</p> <p><b>Network Security Tools, Writing, Hacking</b> Nitesh Dhanjani, Justin Clarke, Ed. O'Reilly, 2003. ISBN: 0596007949.</p>

UNIVERSIDAD AUTÓNOMA  
DE BAJA CALIFORNIA



FACULTAD DE CONTABILIDAD  
Y ADMINISTRACIÓN  
TIJUANA, B. C.