Programa de estudio

Datos generales

0. Área Académica

Económico Administrativa

1. Programa educativo

Maestría en Sistemas Interactivos Centrados en el Usuario MSICU

2. Facultad

Estadística e Informática

3. Código

SSIS 30003

Datos experiencia Educativa

4. Nombre de la experiencia educativa

Fundamentos de Seguridad

5. Área curricular

5.1 Base	5.2. Especialidad

6. Proyecto integrador	7. Academia(s)
Optimización y Seguridad de Sistemas Operativos	

8. Requisito(s)

8.a. Prerrequisito(s):	8.b. Correquisito(s):

9. Modalidad

Curso-Taller

10. Características del proceso de enseñanza aprendizaje

10.1 Individual	10.2 Grupal	10.2.1 Número mínimo: 10
		10.2.2 Número máximo: 25

11. Número de horas de la experiencia educativa

11.1 Teóricas: 15	11.2 Prácticas: 45

12. Total de créditos	13. Total de horas	14. Equivalencias
5	60	

15. Fecha de elaboración/modificación		16. Fecha de aprobación
15.a Mayo 2011	15.b. Febrero 2014	

17. Nombre de los académicos que participaron en la elaboración y/o modificación.

MCC Gerardo Contreras Vega MCA. Luis Gerardo Montané Jiménez

18. Perfil del docente

Licenciado en Informática con maestría en Ciencias de la Computación o afín, con experiencia demostrable en el área de seguridad en cómputo y preferiblemente con alguna certificación en el área de seguridad en cómputo.

19. Espacio	20. Relación disciplinar
Aula y laboratorio de cómputo	Multidisciplinario

21. Descripción mínima

Esta EE desarrolla aspectos teóricos y prácticos especializados en materia de seguridad de cómputo, necesarios para la actividad de un profesional en computación. El estudiante aplica, de manera integrada y armónica, conocimientos de seguridad en sistemas de cómputo autónomos, de red y en la nube, a través de exposiciones en el aula, desarrollo de prácticas y solución de problemas, cuyas especificaciones le proporciona el maestro. La realización de los proyectos se evalúa a lo largo del curso y sirve de práctica de lo visto en el curso de modo que el estudiante evidencie su desarrollo mediante la demostración práctica y atendiendo a criterios básicos de pertinencia, claridad y coherencia.

22. Justificación

La seguridad de la información es un tema que debe ocupar a todo profesional de la computación, ya que, muchas veces determina el grado de confianza que tendrá un usuario para utilizar o no un sistema. Existen mucho riesgos latentes con el manejo de datos en un sistema individual y aislado de usuarios externos, estos riesgos se incrementan de manera considerable al contar con un sistema en red, ya que usuarios maliciosos podrían tratar de obtener información confidencial o hacer uso de los recursos de la organización o empresa de una manera no autorizada. Es por ello que se requiere conocer las técnicas y procedimientos que utilizan los atacantes para prevenir posibles ataques y robos de información y así trata de mantener con bajo riesgo los datos.

23. Unidad de Competencia

El alumno identifica los principales conceptos relacionados con la seguridad en sistemas de cómputo y en especial en sistemas conectados en red, así mismo el usuario conoce y se ayuda de herramientas que utiliza un atacante para hacer una intrusión a una red o sistema o provocar un incidente. Todo esto con énfasis en el desarrollo sustentable y con actitud responsable, de cooperación, discrecionalidad y honestidad.

24. Articulación con los ejes

El estudiante aplica los conocimientos adquiridos sobre seguridad de cómputo (eje teórico), mediante la resolución de problemas basados en casos reales (eje heurístico) a partir de una serie de prácticas y retos de manera individual y en equipo que le desarrollen la capacidad de colaboración con creatividad, responsabilidad, constancia, discreción, compromiso y paciencia (eje axiológico).

Detalles experiencia educativa

25. Saberes por unidad

25.1 Teóricos	25.2 Heurísticos	25.3 Axiológicos
I. Servicios de Red para Sistemas Interactivos 1. Definición 2. Características 3. Servicios de red 4. Escenarios donde se emplean servicios de red 5. Implementación de Servicios de Red II. Sistemas distribuidos 1. Fundamentos 2. Comunicación entre procesos 3. Cómputo concurrente y paralelo 4. Comunicación en red 5. Paradigmas de programación distribuida III. Análisis de seguridad en redes y sistemas informáticos 1. Herramientas de evaluación 2. Pruebas de Penetración 3. Escaneo de redes y servicios IV. Buenas Prácticas en los sistema informáticos 1. Vulnerabilidades y errores	• Identificación de los principales conceptos de seguridad. • Análisis de estándares de seguridad. • Conocimiento de métodos y técnicas de la seguridad física • Conocer y utilizar las herramientas de penetración así el cómo protegerse de ellas. • Utilizar sistemas de cifrado, implementar dentro de un sistema. • Estudiar las vulnerabilidades de la información al circular por una red y los métodos para protegerla. • Utilizar las técnicas y herramientas para minimizar	• Responsabilidad • Honestidad • Compromiso • Discreción • Trabajo colaborativo • Conciencia medio ambiente • Paciencia

comunes 2. Gestión de recurso humano y tecnológico V. Software malintencionado 1. Troyanos 2. Puertas traseras 3. Virus y gusanos VI. Cómputo forense 1. Identificación 2. Preservación 3. Evaluación 4. Reportes 5. Herramientas	riesgos en bases de datos, servidores web y en la nube • Utilizar técnicas de programación segura. • Analizar y utilizar técnicas de análisis forense después de una intrusión.	

26. Estrategias metodológicas por unidad

26.1 De aprendizaje:	26.2 De enseñanza:
Se promueve en el estudiante la investigación de temas a través de libros, revistas y sitios especializados en seguridad de cómputo. Se realizan prácticas en el laboratorio de cómputo o con equipo propio donde aplican los conceptos aprendidos en clase. El estudiante elabora reseñas críticas de lecturas y las presenta en clase ante sus compañeros para su discusión y análisis.	Organización de grupo colaborativos. Estudio de casos donde es básico el aseguramiento de la información y de los datos. Dirección de prácticas de laboratorio y casos de estudio. Exposiciones con equipo de cómputo variado. Enseñanza tutorial. Orientación en la solución de problemas. Tareas para estudio independiente.

27. Apoyos educativos por unidad

27.1 Materiales didácticos	27.2 Recursos didácticos
1. Material de apoyo en línea desarrollado para el curso. 2. Libros impresos y electrónicos. 3. Sitios de Internet. 4. Laboratorio de cómputo.	1. Pizarrón. 2. Proyector. 3. Equipo de cómputo. 4. Laboratorio con software especializado. 5. Equipo de conexión de redes (switch, router, Access point)

29. Evaluación del desempeño por unidad

1 Evidencia(s) de desempeño	2 Criterios de desempeño	3 Campo(s) de aplicación	4 Porcentaje
Proyecto final	Funcionando	Empresa	40%

	correctamente y entregado en tiempo y forma	Aula Laboratorio	
Prácticas de laboratorio	Completas, funcionando correctamente, entregadas en tiempo y forma.	Laboratorio	30%
Exposición	Ordenadas y originales	Aula Laboratorio de cómputo	10%
Examen	Calificación mayor a 80	Aula	20%

30. Acreditación

Para acreditar esta experiencia el alumno deberá demostrar sus conocimientos teóricos y prácticos de los temas, mediante la elaboración de un proyecto integrador que le permitirá aplicar lo aprendido en clase. Dicho proyecto se le entrega al estudiante en el sitio de la EE. Deberá acreditar el examen parcial que incluye todo el curso con calificación mayor o igual a 80, así mismo deberá entregar los reportes de las prácticas en tiempo y forma.

31. Fuentes de información

31.1. Básicas

Winkler , J. R. (2011);Securing the Cloud: Cloud Computer Security Techniques and Tactics; Syngress

Fowley, D.(2000); Firewalls y la Seguridad en Internet, 2ª Edición; New Riders

Kaeo, M.(2002), Diseño de Seguridad en Redes". Cisco Press

Johansson, J.(2005), Protect your Windows Network; Addison Wesley

Stanger, J.(2001); "Hack Proofing Linux"; Syngress

MCClure, Stuard; Scambray, Joel; Kurtz, Goerge(2009); Hacking Expose 6: Network Security Secrets & Solutions; MCGrawHill

Morris R.(2007); A Weakness in the 4.2BSD Unix TCP/IP Software; Bell Labs Computer Science Technical

Mogollón, Manuel(2007); Cryptgraphy and Security Services; Cybertech Publushing

Josyula V., Orr M.,Page G. (2009); Cloud Computing: Automating the Virtualized Data Center; Cisco Press.

Jones, A., Valli C. (2008); Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility; Edit. Butterworth-Heineman.

SSL 3.0 Specification; http://www.freesoft.org/CIE/Topics/ssl-draft/3-SPEC.HTM

SSL Introduction; http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html

URIs, Addresability and the use of HTTP GET and POST;

Nmap – Free Security Scanner for Network Exploration & Security Audits; http://nmap.org

Wireshark: Go deep; http://www.wireshark.org/

RFC 2196 Site Security Handbook; http://tools.ietf.org/html/rfc2196

31.2. Complementarias

Anónimo(2001); Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and WorkstationWeb; Ed. SAMS 2da edición.
Cannings, Rich; Dwivedi, Himanshu; Lackey Zane(2007); Hacking Expose Web 2.0 Security Secrets and Solutions; MCGrawHill.
The WWW Security FAQ; http://www.w3.org/Security/Faq/
Hypertext Transfer Protocol – HTTP/1.1; http://www.ietf.org/rfc/rfc2616.txt
Apache Tomcat 4, SSL Configuration Howto; http://tomcat.apache.org/tomcat-4.1-doc/ssl-howto.html