1. Datos Generales de la asignatura

Nombre de la asignatura:	**Planes y Respuesta a Contingencias**
Clave de la asignatura:	**TED-1805**
SATCA[1]:	**2 – 3 – 5**
Carrera:	**Ingeniería en Sistemas Computacionales** **Ingeniería en Tecnologías de la Información y Comunicaciones**

2. Presentación

Caracterización de la asignatura
La administración de servicios de red no solo implica el mantenerlos a punto para el uso diario. Los servicios, como cualquier sistema de cómputo que descansa en una infraestructura, están propensos a sufrir los embates de usuarios malintencionados o administradores de sistemas ingenuos. Es por esto que es de vital importancia proveer al estudiante del área de sistemas y computación, del conocimiento, habilidades y destrezas para detectar contingencias en servicios como lo son DNS, DHCP, FTP, servidor web y correo electrónico; y de igual manera, que se encuentre en posibilidad de generar respuesta a ellas.
Intención didáctica
El estudiante conocerá elementos de peritaje informático, así como metodologías de seguridad y será capaz de instrumentar planes de respuesta a contingencias en los principales servicios de red como lo son DNS, DHCP, FTP, servidor web y correo electrónico.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Piedras Negras, del 13 de Febrero al 31 de Marzo de 2017.	Academias de Ingeniería en Sistemas Computacionales y de Ingeniería en Tecnologías de la Información y Comunicaciones del Instituto Tecnológico de Piedras Negras.	Diseño y elaboración de la especialidad Tecnologías Emergentes para las carreras de Ingeniería en Sistemas Computacionales e Ingeniería en Tecnologías de la Información y Comunicaciones.

4. Competencias a desarrollar

Competencia específica de la asignatura
El estudiante conocerá metodologías de seguridad y será capaz de instrumentar planes de respuesta a contingencias en los principales servicios de red.

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Observar el escenario problema e identificar oportunidades de desarrollo de proyectos generando ideas innovadoras de la aplicación de la investigación en su área profesional.

6. Temario

No.	Temas	Subtemas
1	Peritaje Informático	1.1 Introducción 1.2 Resguardo de la Información Volátil y No Volátil 1.3 Obstáculos para el Peritaje Informático
2	Metodologías de Seguridad	2.1 ISO/IEC 27001 2.2 OCTAVE 2.3 NIST SP 800-30 2.4 MAGERIT
3	Contingencia en el Servidor DNS	3.1 Monitoreo del Servicio DNS 3.2 Resguardo del Servicio DNS 3.3 Restauración del Servicio DNS
4	Contingencia en el Servidor DHCP	4.1 Monitoreo del Servicio DHCP 4.2 Resguardo del Servicio DHCP 4.3 Restauración del Servicio DHCP
5	Contingencia en el Servidor FTP	4.1 Monitoreo del Servicio FTP 4.2 Resguardo del Servicio FTP 4.3 Restauración del Servicio FTP
6	Contingencia en el Servidor WEB	4.1 Monitoreo del Servicio WEB 4.2 Resguardo del Servicio WEB 4.3 Restauración del Servicio WEB
7	Contingencia en el Servidor CORREO	4.1 Monitoreo del Servicio CORREO 4.2 Resguardo del Servicio CORREO 4.3 Restauración del Servicio CORREO

7. Actividades de aprendizaje de los temas

Tema 1.- Peritaje Informático.	
Competencias	Actividades de aprendizaje
Identificar los elementos esenciales del peritaje informático.	• Contrastar entre información volátil y no volátil para su resguardo. • Identificar los problemas más comunes para el peritaje informático.
Tema 2: Metodologías de Seguridad.	
Competencias	Actividades de aprendizaje
Revisar las metodologías de seguridad de mayor uso en la industria.	• Analizar y discutir metodologías de seguridad como ISO/IEC 27001, OCTAVE, NIST SP 800-30 y MAGERIT
Tema 3: Contingencia en el Servidor DNS.	
Competencias	Actividades de aprendizaje
El estudiante será capaz de elaborar un plan de respuesta a una contingencia en el Servidor DNS.	• Identificar los elementos de monitoreo del servicio DNS. • Resguardar el servicio DNS. • Restaurar el servicio DNS a partir de una contingencia.
Tema 4: Contingencia en el Servidor DHCP.	
Competencias	Actividades de aprendizaje
El estudiante será capaz de elaborar un plan de respuesta a una contingencia en el Servidor DHCP.	• Identificar los elementos de monitoreo del servicio DHCP. • Resguardar el servicio DHCP. • Restaurar el servicio DHCP a partir de una contingencia.
Tema 5: Contingencia en el Servidor FTP.	
Competencias	Actividades de aprendizaje
El estudiante será capaz de elaborar un plan de respuesta a una contingencia en el Servidor FTP.	• Identificar los elementos de monitoreo del servicio FTP. • Resguardar el servicio FTP. • Restaurar el servicio FTP a partir de una contingencia.
Tema 6: Contingencia en el Servidor WEB.	
Competencias	Actividades de aprendizaje
El estudiante será capaz de elaborar un plan de respuesta a una contingencia en el Servidor WEB.	• Identificar los elementos de monitoreo del servicio WEB. • Resguardar el servicio WEB. • Restaurar el servicio WEB a partir de una contingencia.
Tema 7: Contingencia en el Servidor de CORREO	
Competencias	Actividades de aprendizaje
El estudiante será capaz de elaborar un plan de respuesta a una contingencia en el Servidor CORREO.	• Identificar los elementos de monitoreo del servicio CORREO. • Resguardar el servicio CORREO. • Restaurar el servicio CORREO a partir de una contingencia.

8. Práctica(s)

1. En un laboratorio de especialidad, preferentemente con Linux Distro Red Hat, configurar los servicios de DNS, DHCP, FTP, WEB y CORREO.
2. Elaborar los planes de respuesta a contingencia para cada uno de los servicios.
3. Resguardar cada uno de los servicios.
4. Recuperar cada uno de los servicios después de haber experimentado una contingencia.

9. Proyecto de asignatura

El objetivo del proyecto que plantee el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la competencia de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y especificas a desarrollar.

- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Establecer la planeación de un sitio web como proyecto final de la asignatura.
- Bitácora de proyectos.
- Ponderar tareas
- Participación y desempeño en el aula y el laboratorio.
- Dar seguimiento al desempeño en el desarrollo del programa (dominio de los conceptos, capacidad de la aplicación de los conocimientos en problemas reales, transferencia del conocimiento).
- Cumplimiento de los objetivos y desempeño en las prácticas
- Exámenes escritos para comprobar el manejo de aspectos teóricos.
- Reportes escritos de las observaciones hechas durante las actividades realizadas en el laboratorio, así como de las conclusiones obtenidas de dichas observaciones.
- Reportes escritos de la Información obtenida durante las investigaciones solicitadas.
- Valorar la inclusión del contenido temático de cada unidad de aprendizaje y el seguimiento de la planeación del desarrollo de proyecto final con un porcentaje del total de las actividades que sumadas evidencien el total de la evaluación del estudiante.

11. Fuentes de información

[1] S.SHAH; W.SOYINKA. “Linux Administration”, McGraw-Hill, 2005.
[2] B.CALKINS. “Solaris 10 System Administration”, SUN Microsystems, 2005.
[3] H.BRELSFORD. “Windows 2000 Server” Arrayan, 2007.
[4] J.RAYA; E.RAYA. “Windows NT Server”, Ra-Ma.
[5] E.NAVARRO; V.PIATTINI. ”Auditoria Informática: Un enfoque practico”, RaMa.
[6] G.MARK “Commands, Editors, and shell Programming ”
[7] TANENBAUM A. (2003). Redes de computadoras. Prentice Hall. 4ta ed. México.
[8] Cert coordination Center, “Análisis de un sistema comprometido”, http://www.cert.org/security-improvement/practices/p046.html
[9] Página dedicada a la seguridad desarrollada por Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx.
[10] Cert Coordination Center, Trabajo sobre el análisis de información en Unix, http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.
[11] Trabajo dedicado a la investigación forense en sistemas informáticos. http://www.loquefaltaba.com/documentacion/forense/.
[12] Trabajo sobre cómo hacer una auditoria informática, http://www.auditoria.com.mx/.
[13] Una colección de herramientas de un investigador forense. Utilidades escritas por Dan y Wietse (trabaja para IBM, y el autor de postfix) http://www.fish.com/tct/.

[14] Benson C., (s.f.), Estrategia de seguridad, Microsoft TechNet. Desde https://www.microsoft.com/latam/technet/articulos/200011/art04/default.asp
[15] Carli F. (2003), Security Issues With DNS. http://www.sans.org/reading room/whitepapers/dns/1069.php.
[16] Red Hat Enterprise Linux (RHEL), (2008), Deployment Guide 5.1, Red Hat Inc, USA. https://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/en-US/RHEL510/Deployment Guide/index.html

[17] Scarfone K., Mell P., (2007) Guide to Intrusion Detection and Prevention Systems (IDPS), NIST. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[18] Wack J., Cutler K., y Pole J. (2002), Guidelines on Firewalls and Firewall Policy, NIST, Computer Security Division. http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
[19] May C., Baker M., y Gabbard D., et. al., (2004), Advanced Information Assurance Hand-book, CERT, Carnegie Mellon University, USA. http://www.cert.org/archive/pdf/aia-handbook.pdf
[20] Ferrer J., Fernández-Sanguino J., (s.f.), El sistema operativo GNU/Linux y sus herramientas libres en el mundo de la seguridad: estudio del estado del arte. http://mmc.igeofcu.unam.mx/LuCAS/Presentaciones/200103hispalinux/ferrer/pdf/seguridad-y-sw-libre v1.0.pdf
[21] Herzog P. (2003), Manual de la Metodología Abierta de Testeo de Seguridad, ISECOM, segunda ed., USA. http://isecom.securenetltd.com/osstmm.en.2.2.pdf
[22] Miles T., Wayne J., McLarnon M., (2002), Guidelines on Securing Public Web Servers, NIST, USA. http://csrc.nist.gov/publications/nistpubs/800-44 ver2/SP800-44v2.pdf
[23] Stoneburner G., Goguen A., Feringa A., (2001), Underlying Technical Models for Information Technology Security, NIST. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[24] Sondeo realizado por Macias Saucedo denominado Encuesta Nacional sobre la Seguridad Informática en México 2007. http://www.acis.org.co/fileadmin/Revista 101/ArticuloEncuestaUNIVA.pdf
[25] Página principal de la metodología iso27000.es http://www.iso27000.es