1.- DATOS DE LA ASIGNATURA

Nombre de la asignatura:	**Planes y Respuesta a Contingencias**
Carrera:	**Ingeniería en Tecnologías de la Información y Comunicaciones e Ingeniería en Sistemas Computacionales**
Clave de la asignatura:	**TED-1405**
Créditos[1]	**2 - 3 - 5**

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, WEB y CORREO; 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, WEB y CORREO.

[1] Sistema de asignación y transferencia de créditos académicos

3.- COMPETENCIAS A DESARROLLAR

El estudiante conocerá metodologías de seguridad y será capaz de instrumentar planes de respuesta a contingencias en los principales servicios de red.	**Competencias instrumentales** • Capacidad de Análisis y Síntesis • Capacidad de Organizar y Planificar • Habilidades de Gestión de Información • Solución de Problemas • Toma de Decisiones **Competencias interpersonales** • Capacidad Crítica y Autocrítica • Trabajo en Equipo • Habilidades Interpersonales • Capacidad de Comunicarse con Profesionales de Otras Áreas • Compromiso Ético **Competencias sistémicas** • Capacidad de Aplicar Conocimientos en la Práctica • Habilidades de Investigación • Capacidad de Aprender • Capacidad de Adaptarse a Nuevas Situaciones • Capacidad de Generar Nuevas Ideas • Liderazgo • Capacidad para Diseñar y Gestionar Proyectos • Preocupación por la Calidad.

4.- HISTORIA DEL PROGRAMA

Lugar y fecha de elaboración o revisión	Participantes	Observaciones (cambios y justificación)
Instituto Tecnológico de Piedras Negras, del 11 de Septiembre al 23 de Octubre de 2013.	Instituto Tecnológico de Piedras Negras Participantes de la Academia de Sistemas y Computación • MAYL. Hilda Patricia Beltrán Hernández • MC. Roberto Espinoza Torres • L.I. Claudia Martha Lozano Longoria • MC. Flor de María Rivera Sánchez • Ing. Filiberto Torres Rábago • MIE. Miguel Arturo Vélez Riojas	Diseño y Elaboración de la especialidad Tecnologías Emergentes para las carreras de Ingeniería en Tecnologías de la Información y Comunicaciones e Ingeniería en Sistemas Computacionales

5.- OBJETIVO(S) GENERAL(ES) DEL CURSO (competencias específicas a desarrollar en el curso)

El estudiante conocerá metodologías de seguridad y será capaz de instrumentar planes de respuesta a contingencias en los principales servicios de red

6.- 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.

7.- TEMARIO

Unidad	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

8.- SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

- Propiciar actividades de búsqueda, selección y análisis de información en distintas asignaturas.
- Fomentar actividades grupales que propicien el intercambio de ideas, reflexión, integración y colaboración entre los alumnos.
- Desarrollar actividades de aprendizaje que propicie la aplicación de las metodologías y planes de respuesta a contingencia que se van presentando en el desarrollo de la asignatura.

9.- SUGERENCIAS DE EVALUACIÓN

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

- Participación en clase.
- Prácticas realizadas en laboratorio de especialidad.
- Información obtenida durante las búsquedas encomendadas.
- Evaluación de unidades de aprendizaje basada en casos.
- Autoevaluación, coevaluación y evaluación de las actividades.

10.- UNIDADES DE APRENDIZAJE

Unidad 1: Peritaje Informático.

Competencia específica a desarrollar	**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.

Unidad 2: Metodologías de Seguridad.

Competencia específica a desarrollar	**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

Unidad 3: Contingencia en el Servidor DNS.

Competencia específica a desarrollar	**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.

Unidad 4: Contingencia en el Servidor DHCP.

Competencia específica a desarrollar	**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.

Unidad 5: Contingencia en el Servidor FTP.

Competencia específica a desarrollar	**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.

Unidad 6: Contingencia en el Servidor WEB.

Competencia específica a desarrollar	**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.

Unidad 7: Contingencia en el Servidor CORREO.

Competencia específica a desarrollar	**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.

11.- FUENTES DE INFORMACIÓN
Fuentes impresas (libros)

[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. Cuarta 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

12.- PRÁCTICAS PROPUESTAS

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