

## 1. Datos Generales de la asignatura

<b>Nombre de la asignatura:</b>	<i>Seguridad en redes.</i>
<b>Clave de la asignatura:</b>	<b>GRD-1803</b>
<b>SATCA<sup>1</sup>:</b>	<b>2-3-5</b>
<b>Carrera:</b>	Ingeniería en Sistema Computacionales ISIC-2010-224 e Ingeniería en Tecnologías de la Información y Comunicaciones. ITIC-2010-225.

## 2. Presentación

<b>Caracterización de la asignatura</b>
<p><b><i>Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales y del Ingeniero en Tecnologías de la Información y Comunicaciones las siguientes habilidades:</i></b></p> <ul style="list-style-type: none"> <li>• Esta asignatura aporta al perfil del egresado las competencias para aplicar los conocimientos científicos y tecnológicos en la solución de problemas de aspectos de seguridad y calidad del servicio de redes de computadoras, aplicando sistemas de seguridad acordes acorde a las políticas internas de las organizaciones basados en estándares establecidos, con la finalidad de garantizar la integridad y consistencia de la información.</li> <li>• Es de suma importancia ya que las habilidades que propicia en el estudiante permite que se involucre en la administración y protección de la información como activo principal de cualquier empresa a nivel mundial.</li> <li>• La asignatura consiste en definir, entender y aplicar los conocimientos para prevenir que alguna entidad no autorizada que intercepte la comunicación pueda acceder de forma inteligible a cierta información, aplicando las técnicas y herramientas para protección y monitoreo con la finalidad de lograr un óptimo desempeño y garantizar la transmisión de la información.</li> <li>• Para el correcto desarrollo de esta asignatura se requieren las competencias adquiridas en las materias de fundamentos de redes, redes de computadoras, en las competencias del control del funcionamiento interno de una computadora, de redes de información y de sistema operativo en la parte de acceder a servicios y recursos de una red de computadoras.</li> </ul>
<b>Intención didáctica</b>

<sup>1</sup> Sistema de Asignación y Transferencia de Créditos Académicos

- Esta asignatura consta de cinco temas relacionados con las funcionalidades y mecanismos de seguridad en una red de computadoras, generalidades y arquitectura en capas del modelo OSI.
- Se sugiere que el docente realice una evaluación diagnóstica a los estudiantes, la cual permitirán saber qué competencias previas se deben reforzar y que son necesarias para el buen desarrollo de esta asignatura.
- En el tema uno el estudiante conocerá el nuevo enfoque de la seguridad de las comunicaciones de extremo a extremo, en la actualidad no es suficiente considerar la seguridad por separado para cada producto o servicio, como las listas de acceso que son una forma de determinar los permisos de acceso apropiados a un determinado objeto. Conocer IPsec como protocolo de seguridad y sus generalidades, autenticando cifrado para cada paquete IP. Estudiando el firewall como una herramienta para controlar los accesos y las VPN como solución de seguridad para una empresa.
- En el tema dos se conocerá la arquitectura en capas para varios casos de uso a fin de proteger usuarios, dispositivos y aplicaciones adaptados a nuevos tipos de amenazas.
- En el tema tres, se conocerán los protocolos de seguridad (nivel aplicación), como el SSL como protocolo seguro para transmitir información de ida y vuelta. El TLS que agrega sistemas criptográficos.
- En el tema cuatro, se analizará el tema de balanceo de cargas que es cuando un router detecta varias rutas a una red específica a través de varios procesos de ruteo o protocolos de ruteo así como mecanismos, solución de problemas, failovers, técnicas de distribución de cargas y otras configuraciones.
- El tema cinco se analizará la redundancia de datos RAID, como una opción de seguridad y tolerancia a fallos así como sus ventajas y desventajas.
- Es necesario e importante que el docente promueva en el estudiante el desarrollo de habilidades para mejorar la seguridad y servicios en las redes de computadoras y la protección de datos.
- El docente deberá promover que el estudiante desarrolle las competencias genéricas para el análisis y solución de problemas reales, así como las discusiones grupales y exposiciones que fomenten la competencia de expresión oral y la capacidad de aplicar los conocimientos en la práctica.

### 3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Villahermosa, junio 2017.	Representantes de la academia de Ingeniería en Sistemas Computacionales e Ingeniería en Tecnologías de la Información y Comunicación del Instituto Tecnológico de Villahermosa.	Reunión de academia de diseño curricular para la elaboración de la especialidad.

### 4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Conocer y comprender los aspectos involucrados en la seguridad de entornos de red para aplicar los mecanismos y técnicas específicos, para la seguridad de los datos.

### 5. Competencias previas

<ul style="list-style-type: none"> <li>• Conocimiento de redes de computadoras.</li> <li>• Bases del funcionamiento del modelo TCP/IP.</li> <li>• Identificar los sistemas básicos de criptografía.</li> <li>• Fundamentos de administración de la función informática.</li> <li>• Conocimiento organización de computadoras.</li> <li>• Bases de sistemas operativos</li> <li>• Conocimientos básicos de administración de servidores.</li> </ul>
--

### 6. Temario

No.	Temas	Subtemas
1	Seguridad en la comunicación.	1.1 Generalidades. 1.2 Listas de control de acceso 1.3 IPsec 1.4 Firewall 1.5 VPN
2.	Arquitectura en capas	2.1 Introducción 2.2 Capa de presentación. 2.3 Capa de negocios.

		2.4. capa de datos: 2.4.1 Componentes de seguridad. 2.4.2 Control de errores 2.4.3 Loggins, instrumentación, seguimiento.
3	Protocolos de seguridad. (Nivel aplicación).	3.1 Introducción. 3.2 SSL 3.3 TLS
4	Balanceo de carga	4.1 Consideraciones. 4.2 Mecanismos: 4.2.1 ECMP 4.2.2 PCC: (Mangle) 4.2.3 NTH 4.3 Soluciones a problemas 4.4 Failover 4.5 Técnica de distribución de carga round robin. 4.6 Configurar balance de carga (NLB) en window server.
5	Redundancia de datos RAID.	5.1 Generalidades. 5.2 Funcionalidad de un RAID 5.3 Almacenamiento en servidores. 5.4 Recuperación de datos.

## 7. Actividades de aprendizaje de los temas

<b>1. Seguridad en la comunicación.</b>	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <p>Identifica las variadas amenazas a la seguridad de comunicaciones y relacionarlas con las técnicas usadas frecuentemente, para mitigar los riesgos subsecuentes.</p> <p>Genéricas:</p>	<ul style="list-style-type: none"> <li>Investiga las generalidades de seguridad en la comunicación de redes de computadoras.</li> <li>Investiga qué es una lista de control de acceso. Realiza prácticas donde se puedan crear ACL, borrar, aplicar sobre puertos.</li> <li>Investiga qué es IPsec, firewall y VPN.</li> </ul>

<ul style="list-style-type: none"> <li>• Conocimientos generales básicos de redes de computadoras.</li> <li>• Habilidades para solución de problemas.</li> <li>• Capacidad de análisis y síntesis.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar conocimientos en la práctica.</li> <li>• Habilidades de investigación.</li> </ul>	<ul style="list-style-type: none"> <li>• Realizar prácticas de tunelización.</li> <li>• Configurar VPN.</li> </ul>
<p><b>2. Arquitectura en capas.</b></p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</p> <p>Identifica los riesgos de seguridad relativos en la distribución de la información y la necesidad de reforzar los controles de seguridad en una arquitectura por capas.</p> <p>Genéricas:</p> <ul style="list-style-type: none"> <li>• Conocimientos generales básicos de redes de computadoras.</li> <li>• Habilidades para solución de problemas.</li> <li>• Capacidad de análisis y síntesis.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar conocimientos en la práctica.</li> <li>• Habilidades de investigación.</li> </ul>	<ul style="list-style-type: none"> <li>• Investiga sobre las diferentes capas del modelo OS Y las vulnerabilidades que presenta en cada una de sus capas.</li> <li>• Identifica las funciones del control de flujo y corrección de errores y en qué capas trabaja.</li> <li>• Investiga loggins, instrumentación y seguimiento.</li> </ul>
<p><b>3. Protocolos de seguridad (nivel aplicación).</b></p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>

<p>Específica(s):</p> <p>Identificar cómo los protocolos de seguridad de la capa de aplicación funcionan y proporcionan vínculos a los documentos de RFC.</p> <p>Genéricas:</p> <ul style="list-style-type: none"> <li>• Conocimientos generales básicos de redes de computadoras.</li> <li>• Habilidades para solución de problemas.</li> <li>• Capacidad de análisis y síntesis.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar conocimientos en la práctica.</li> <li>• Habilidades de investigación.</li> </ul>	<ul style="list-style-type: none"> <li>• Investigar las generalidades de los protocolos de seguridad. (Capa de aplicación).</li> <li>• Investigar el protocolo SSL y su funcionalidad.</li> <li>• Investigar tipos de ataques SSL.</li> <li>• Realizar prácticas con SSL.</li> <li>• Identificar el protocolo TLS y su funcionalidad.</li> <li>• Realizar prácticas con TLS.</li> </ul>
<p><b>4. Balanceo de carga.</b></p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</p> <p>Identificar la técnica del balanceo de cargas, su funcionalidad, los mecanismos, los tipos y el tipo de plataforma en que pueden ser utilizados así como sus ventajas.</p> <p>Genéricas:</p> <ul style="list-style-type: none"> <li>• Conocimientos generales básicos de redes de computadoras.</li> <li>• Habilidades para solución de problemas.</li> <li>• Capacidad de análisis y síntesis.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar conocimientos en la práctica.</li> <li>• Habilidades de investigación.</li> </ul>	<ul style="list-style-type: none"> <li>• Investigar generalidades del balanceo de cargas.</li> <li>• Contextualizar mecanismos: ECMP, PCC, NTH.</li> <li>• Realizar prácticas donde se solucionen problemáticas.</li> <li>• Contextualizar un failover.</li> <li>• Investigar la técnica de distribución de carga Round Robin.</li> <li>• Realizar una práctica de balanceo de cargas en la plataforma Windows.</li> </ul>

<b>5. Redundancia de datos RAID.</b>	
Competencias	Actividades de aprendizaje
<p>Específica(s): Conocer el sistema de almacenamiento de datos RAID, así como su beneficio e implementación así como su alta disponibilidad dentro de un sistema de seguridad.</p> <p>Genéricas:</p> <ul style="list-style-type: none"> <li>• Conocimientos generales básicos de redes de computadoras.</li> <li>• Habilidades para solución de problemas.</li> <li>• Capacidad de análisis y síntesis.</li> <li>• Toma de decisiones.</li> <li>• Trabajo en equipo.</li> <li>• Capacidad de aplicar conocimientos en la práctica.</li> <li>• Habilidades de investigación.</li> </ul>	<ul style="list-style-type: none"> <li>• Identificar las generalidades de un sistema de almacenamiento de datos RAID.</li> <li>• Conocer sus ventajas, desventajas e implementación.</li> <li>• Conocer la funcionalidad de un RAID.</li> <li>• Niveles RAID.</li> <li>• Almacenamiento en servidores.</li> <li>• Conocer la recuperación de datos.</li> </ul>

## 8. Práctica(s)

1. Diseñar una práctica de laboratorio, donde se configure la seguridad básica de red mediante listas de control de acceso. Se aplicarán ACL estándar y ampliadas.
2. Instalar AppServ en Windows y dejar la opción en localhost, una vez instalado probamos abriendo el navegador y la barra de direcciones ponemos <http://localhost>. Se necesita es OpenSSL para Windows. Descargamos la versión 0.97e para windows. Instalado accedemos a una ventana DOS y desde directorio Openssl/bin, realizar lo siguiente:
  1. Creación de la llave  
Generar llave de 1024 bits sin frase de paso  
Openssl genrsa-out server.key 1024
  2. Creación petición del certificado  
Generar petición del certificado digital  
Opensslreq-new-server.key-ouserver.csr
  3. Crear certificado  
Creación de certificado autofirmado

```
Open x509-req-days 365-in server.csr-signkey server.key -out sever.crt
```

Ahora mediante un editor procedemos a buscar el archivo httpd.conf en c:appservapache/conf y editarlo

Hay que comentar la línea del puerto 80

Listen80

Listen 443

Los puertos por donde queremos que escuche.

Reiniciamos el servidor apache.

Se realiza una prueba de conexión a ambos puertos, viéndose una página de prueba satisfactoria.

## 9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) 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 específicas 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

- Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales o mentales, reporte de investigación, reportes de prácticas, tablas comparativas, estudio de casos, exposiciones en clase, portafolio de evidencias, entre otros.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, rúbricas, etc.

## 11. Fuentes de información

Alvaro Gómez Vieites. Enciclopedia de la seguridad informática. Alfaomega. Ra-Ma.

Sheldom Sheldom. Lan times- enciclopedia de redes. Ed. McGraw Hill.

Stallings William. Comunicaciones y redes de computadores. Ed. Prentice Hall.

Tanenbaum Andrew S. Redes de computadoras. Ed. Prentice Hall.

<https://www.netacad.com/>