



PLAN DE TRABAJO

LICENCIATURAS EN QUE SE IMPARTE

1. Informática 7° semestre

DATOS DE LA ASIGNATURA

Nombre:	Seguridad en redes
Clave(s):	0386
Tipo:	Optativa
Plan de Estudios:	Plan 2012 (actualizado 2016)

FECHAS DEL SEMESTRE:

Inicio semestre:	12 de febrero de 2024
Fin del semestre:	21 de junio 2024
Plataforma educativa:	28 de febrero de 2024 Primer día para entrega de actividades en plataforma
Cierre de plataformas:	16 de junio de 2024 a las 23:00 hrs. Último día para entrega de actividades en plataforma
Periodo examen global:	15 y del 17 al 21 de junio 2024
Registro de calificaciones en actas:	
Consulta de calificaciones a partir del:	

DATOS GENERALES

Objetivo general:

El alumno conocerá los aspectos generales de la seguridad en las redes de computadoras en una organización, el análisis de riesgos y vulnerabilidades, las técnicas de identificación, así como la implementación de la seguridad en la red por hardware y software

Contenido temático:

	Tema	Teóricas	Prácticas
1	seguridad física y lineamientos generales de seguridad	8	0
2	identidad	8	0
3	seguridad en la comunicación	8	0
4	monitoreo	8	0
5	seguridad en los servicios	8	0
6	detección de vulnerabilidades e intrusiones	8	0
7	autenticación y autorización de accesos	8	0
8	Recursos de seguridad	8	0
Total		64	0
Suma total de horas		64	

BIENVENIDA

Estimad@s alumn@s de la asignatura Seguridad en Redes:

Seré su maestro de esta asignatura, durante este semestre; por ello, mi labor es apoyarte en tu proceso de aprendizaje, resolviendo tus dudas y sugiriendo cómo aprovechar los contenidos para que puedas obtener un mejor aprendizaje. No dejes de preguntar en las asesorías cuanto sea necesario y las veces que consideres pertinente.

Revisaré tus actividades de aprendizaje en plataforma y tendrás un comentario a cada una de ellas en un lapso que no debe ser mayor a 8 días hábiles después de entregar la actividad, lo cual te permitirá conocer la retroalimentación correspondiente para que puedas analizar y asimilar los comentarios que, sin duda, repercutirán en tu aprendizaje. Asimismo, es recomendable que presentes tus exámenes parciales una vez que hayas entregado las actividades de aprendizaje de esas unidades y consideres que te has preparado lo suficiente para poder acreditarlas.

Será importante mantenerse atento a los comunicados que emitan tanto las autoridades de la Facultad como del sistema abierto (SUA), respecto a las medidas de sanidad, seguridad y control para minimizar o evitar cualquier situación de riesgo de contagio, durante el tiempo que se estime necesario por los efectos del Covid-19, así como de las guías e instrucciones para cumplir los requisitos para la acreditación de la asignatura.

En los días y horarios establecidos para las asesorías, estaré en el cubículo o mesa asignados para facilitar el intercambio de comentarios, dudas y consultas sobre el desarrollo de las actividades y preparación para los exámenes parciales

PRESENTACIÓN DE LA ASIGNATURA

Esta asignatura te permitirá adentrarte, conocer y comprender lo que implica el concepto de seguridad en redes y su importancia y aplicación en el ámbito de las empresas, para reducir significativamente los riesgos de que sean vulneradas.

Debido a que la información es ya un activo en las organizaciones, se vuelve de vital importancia protegerlo como tal y cumplir con la guarda, registro, control y seguridad de nuestra información.

Así mismo, entenderás la relación que tiene con el concepto general de Ciberseguridad, también en redes y la importancia que esto tiene en todas nuestras actividades del día a día.

FORMA EN QUE EL ALUMNO DEBE PREPARAR LA ASIGNATURA

Cada unidad tiene actividades de aprendizaje e instrucciones para que investigues el material a estudiar. Es importante que estes atento al material que se te presenta en la plataforma y que revises el foro general en Moodle, donde se te podrán indicar nuevamente instrucciones generales que debes seguir para desarrollar tu materia adecuadamente, la estructura para la entrega de todos tus trabajos: debe ser considerando portada, índice/contenido, objetivo, introducción/antecedentes, desarrollo del tema, conclusiones personales y bibliografía/mesografía en formato APA., todas tus actividades las deberás presentar en formato PDF. La entrega de tus actividades en plataforma deberás realizarla a más tardar a las 21:00 hr del día anterior a la aplicación del primer día del primer período de exámenes para las actividades 1 a 4 y también a más tardar a las 21:00 hr del día anterior al primer día de aplicación del tercer periodo para las actividades 5 a 8, de lo contrario no serán calificadas, por no cumplir con este requerimiento. Las actividades de aprendizaje se han estructurado de tal forma que te permitan desarrollar habilidades y destrezas, para dar solución a un problema en específico, producto de los aprendizajes significativos derivados de la apropiación de los contenidos temáticos de la asignatura. Cuando la realización de una actividad implique hacer una investigación, deberás buscar fuentes oficiales como libros, revistas, artículos, etcétera, tu trabajo deberá contener al menos dos fuentes mesográficas diferentes a los apuntes electrónicos, deberás hacer la cita en formato APA. <http://normasapa.net/2017-edicion-6/> |

Para la realización de tus actividades deberás cuidar tu **ortografía** y usar **fuentes oficiales** como: libros, revistas, artículos, etcétera. Recuerda hacer la cita en formato APA, ya que, si no lo haces incurrirás en plagio. https://www.revista.unam.mx/wp-content/uploads/3_Normas-APA-7-ed-2019-11-6.pdf .

Las actividades elaboradas con inteligencia artificial serán sancionadas según el criterio que establezca profesor.

ACTIVIDADES POR REALIZAR DURANTE EL SEMESTRE

Estimado alumno, para facilitar el aprendizaje de esta asignatura, en la sección de recursos de tu plataforma encontrarás un archivo llamado Videoclases, que contiene los vínculos a videos que tu profesor ha grabado para ti.

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
Unidad 1: Seguridad física y lineamientos generales de seguridad	Actividad 1	<p>Revisa el video que se te indica en la bibliografía para que tengas una introducción general a la seguridad específica en redes.</p> <p>Estudia la video asesoría que se te presenta en la plataforma relativa a esta unidad, sobre los lineamientos generales de seguridad.</p> <p>Investiga dentro de la clasificación de seguridad física y lógica, las distintas subdivisiones de cada una, define cada concepto y describe en detalle en que consiste en un ensayo donde expongas tu investigación.</p> <p>Recuerda presentar tu trabajo con la estructura solicitada</p>	<p>Revisa, estudia y comprende la siguiente liga: https://www.youtube.com/watch?v=K919npjkbJ4</p> <p>Buscar en fuentes de información varias y confiables</p>	7 pts
Unidad 2: Identidad	Actividad 1 (colaborativa)	<p>Participación en el foro general de la plataforma para profundizar, discutir y exponer tus puntos de vista sobre la identidad en redes o identidad digital y biometría digital respondiendo a lo siguiente : 1) define en tus propias</p>	<p>Revisa, estudia y comprende las siguiente ligas: https://www.bbva.com/es/economia/mercados-financieros/blockchain/ https://www.arimetrics.com/glosario-digital/identidad-digital https://tinyurl.com/2z5e5pu5</p>	3

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
		<p>palabras a la identidad digital, 2) Qué debo hacer para cuidar mi identidad en redes 3) Define en tus propias palabras la biometría digital y sus ventajas de al menos 8 tipos</p> <p>Debes exponer tu opinión informada y comentar al menos dos de las opiniones de tus compañeros, argumentando tus comentarios.</p>	<p>Buscar en fuentes de información varias y confiables</p>	
<p>Unidad 3: Seguridad en la comunicación</p>	<p>Actividad de aprendizaje 1</p>	<p>Revisa, estudia y comprende la información de las ligas de la bibliografía y el video de la plataforma de este tema y realiza un ensayo sobre las medidas, políticas o procedimientos que adoptarías en tu empresa para mitigar estos riesgos en la comunicación.</p> <p>Estudia la video asesoría que se te presenta en la plataforma relativa a esta unidad 3, sobre la seguridad en la comunicación y el cibercrimen.</p> <p>Elabora una infografía donde describas la ingeniería social</p>	<p>Revisa, estudia y comprende la siguiente liga: Impacto del cibercrimen alcanza los 12 mil mdd https://tinyurl.com/2efnjhlp</p> <p>Gota a gota:¿Cómo operan y que hacer ante el fraude? https://tinyurl.com/2gox7acy</p> <p>Estiman que México tuvo 85 mil millones de ciberataques https://tinyurl.com/2qazhzuf</p> <p>Buscar en fuentes de información varias y confiables</p>	<p>7</p>
<p>Unidad 4: monitoreo</p>	<p>Actividad de aprendizaje 1</p>	<p>Dentro de las muchas y distintas herramientas de seguridad, las de monitoreo están diseñadas para analizar la confiabilidad de un sistema y</p>	<p>Revisa, estudia y comprende la siguiente liga: Monitoreo de redes; https://www.youtube.com/watch?v=PdBepa1WXI4</p>	<p>7</p>

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
		seguridad de la red. Elabora una infografía donde incluyas al menos 10 de estas herramientas, donde menciones entre ellas, las siguientes 5; Satan, NTA, NPM, Tiger y SPI. Debes describirlas e indica su creador.	https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/ Buscar en fuentes de información varias y confiables	
Unidad 5: Seguridad en los servicios	Actividad de aprendizaje 1	Para tener una adecuada comprensión de la seguridad en los servicios, estudiaremos de entre todas las que existen, las siguientes 3 herramientas que nos soportan para modificar parámetros en nuestro sistema y con esto minimizar los riesgos que tenemos contra diversos ataques a los servicios. Investiga y describe a detalle en un ensayo que son los firewalls (incluye los distintos tipos que existen), la criptografía y sus llaves secretas y públicas y el sistema kerberos.	Para que inicies tu investigación, estas ligas te ayudarán para iniciar y completar tu búsqueda de información : https://tinyurl.com/2gy4jllk , para criptografía https://tinyurl.com/yabpmc7o , para firewalls https://es.wikipedia.org/wiki/Kerberos , para Kerberos Buscar en fuentes de información varias y confiables	8
Unidad 6: Detección de vulnerabilidades e intrusiones	Actividad de aprendizaje 1	Realiza una investigación para que entiendas que es un pentest (prueba de penetración), los kits que existen, cuánto cuestan y para que sirven. Es deseable que realices el siguiente ejercicio en una máquina con linux o para evitar problemas de acceso, ataque a una computadora en funcionamiento y que tengas que conseguir sw y hw, la	La siguiente liga te ayudará a realizar tu actividad, adicionalmente busca en youtube este procedimiento : https://tinyurl.com/2o9k69r7 Buscar en fuentes de información varias y confiables	8

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
		actividad consistirá en que describas y fotodocumentes /presentes las pantallas a detalle de los pasos necesarios para: Conocer, entender y explicar los pasos para realizar un ataque con la distribución de Kali desde una máquina virtual a un ordenador con Windows. Se debe efectuar el ataque realizando la clonación de la página web de Facebook, utilizando las herramientas SET y Metasploit para cargar un Java Applet en un ordenador con Windows		
Unidad 7: Autenticación y autorización de accesos	Actividad de aprendizaje 1	Realiza una investigación sobre los conceptos de autenticación y autorización de accesos, su importancia y como se implantan en tu organización, sube a plataforma los resultados de tu investigación en un mapa mental conforme a la estructura solicitada	https://www.ibm.com/docs/es/control-desk/7.6.1.2?topic=security https://tinyurl.com/2hz7fwzr Buscar en fuentes de información varias y confiables	5
Unidad 8: Recursos de seguridad	Actividad de aprendizaje 1	Eres el encargado del área informática de una organización, acorde a lo que has estudiado y que complementes con más investigación sobre ciberseguridad, elabora una lista con una breve descripción de sus ventajas al adoptarlos, de consejos/políticas, sugerencias de seguridad que aplicarías en tu empresa, considera desde los más	Buscar en fuentes de información varias y confiables	7

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
		<p>simples o básicos hasta los más sofisticados. Al menos enlista 40 conceptos en una tabla que contenga al menos las siguientes columnas:</p> <p>1)consecutivo de concepto; 2)política/medida/sugerencia; 3) clasificación (física, lógica,subdivisión) 4)ventaja; 5)dirigido a (usuarios, informáticos, todo personal, ejecutivos, etc</p>		
Ponderación total de las actividades				52

EXÁMENES

De acuerdo con los lineamientos del modelo educativo, tienes tres períodos a lo largo del semestre para presentar tus exámenes parciales (consulta las fechas en el calendario de inscripción a parciales y globales en el Portal SUAyED), tú decides el período en el que los realizarás. Si tu asignatura es optativa, deberás consultar los períodos y número de exámenes con tu asesor.

Para esta asignatura están programados de la siguiente manera:

- **Parciales:**
- Deberás entregar las actividades de aprendizaje de las unidades implicadas en cada parcial, **antes de que inicie el periodo de aplicación**. Es importante que te inscribas en cada periodo y cumplas con los lineamientos para su presentación.

NÚMERO	UNIDADES (que lo integran)	VALOR (núm. enteros)
1ro.	1 a 4	24
2do.	5 a 8	24

- Global. Examen único

Valor	Requisitos	Aplicación de global
100%	Ninguno	15 y del 17 al 21 de junio 2024

PORCENTAJES Y ESCALA DE EVALUACIÓN Y ACREDITACIÓN

Porcentajes de evaluación:

Concepto	Porcentajes
Actividades de aprendizaje	49 %
Actividades colaborativas	03 %
Exámenes parciales	48 %
Otro	%
Total	100 %

Escala de evaluación:

Rango	Calificación
1.00 a 5.99	5
6.00 a 6.99	6
7.00 a 7.99	7
8.00 a 8.99	8
9.00 a 9.54	9
9.55 a 10.00	10

FUNCIONES DEL ASESOR

Por ser una modalidad abierta, tu asesor:

1. Será tu apoyo y guía de manera presencial para la resolución de dudas y desarrollo de las actividades; así mismo, por la mensajería de la plataforma educativa para dudas concretas.
2. Calificará y retroalimentará tus actividades de aprendizaje en plataforma educativa en un lapso no mayor a diez días hábiles después de la entrega.
3. Te recomendará recursos didácticos adicionales para ampliar tu conocimiento. No es su obligación facilitarte: copias, archivos digitales o proporcionarte ligas directas de la BIDI.
4. Enviará tu calificación al finalizar el semestre de manera personalizada.

DATOS DEL ASESOR O GRUPO DE ASESORES

Nombre	Correo electrónico
Nombre completo del asesor	Correo electrónico para plataforma
Raúl Salvador Jiménez Ramírez	raclara@yahoo.com

Enseñar no es transferir conocimiento, sino crear las posibilidades para su propia producción o construcción.

Paulo Freire