I. Datos de la institución

Plantel		**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO** **FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN** DIVISIÓN SISTEMA UNIVERSIDAD ABIERTA Y EDUCACIÓN A DISTANCIA Modalidad: A Distancia		**Grado o Licenciatura**	Licenciatura en Informática

II. Datos del asesor

Nombre	HERNANDEZ CERVANTES MARICARMEN	**Correo**	mari_hernandez@cuaed.unam.mx

III. Datos de la asignatura

Nombre	SEGURIDAD EN REDES	**Clave**	0386	**Grupo**	8891
Modalidad	Optativa	**Plan**	2012	**Fecha de inicio del semestre**	28 de enero de 2019
Horas de asesoria semanal	4	**Horario**	Lunes: 08:00 - 10:00 hrs Miércoles: 08:00 - 10:00 hrs	**Fecha de término del semestre**	05 de junio de 2019

IV. Contenido temático

TEMA	**HORAS**		
	Total	**Teoría**	**Práctica**
I. Seguridad física y lineamientos generales de seguridad	8	8	0
II. Identidad	8	8	0
III. Seguridad en la comunicación	8	8	0
IV. Monitoreo	8	8	0

V. Seguridad en los servicios	8	8	0
VI. Detección de vulnerabilidades e intrusiones	8	8	0
VII. Autenticación y autorización de accesos	8	8	0
VIII. Recursos de seguridad	8	8	0

V. Presentación general del programa

¡Bienvenidos! Mi nombre es Maricarmen Hernández Cervantes y les estaré acompañando como asesora a distancia durante el desarrollo de las actividades académicas en la asignatura **Seguridad en Redes**.
Estoy segura que tendremos una estrecha comunicación para que puedan realizar sus estudios y se cumplan los objetivos de la asignaura. Les estaré asesorando y orientando hasta que concluyan satisfactoriamente sus estudios, cumpliendo algunas actividades principales: Resolver tus dudas, revisar y retroalimentar tus actividades y mantener comunicación constante.
Es importante que desde un inicio revisen su correo personal, el que tienen dado de alta en la plataforma, debido a que se les enviarán copias automáticas de nuestras comunicaciones por medio de la plataforma.
En caso de que tengan alguna duda o comentario, me estaré conectando por chat los lunes y miércoles de 8:00 a 10:00 horas. También pueden utilizar los mensajes de la plataforma para comunicar cualquier duda u observación.
Estoy segura que tienen un enorme compromiso con su aprendizaje, así que no duden en contactarme cuando lo requieran.
¡Saludos!

VI. Forma en que el alumno deberá preparar la asignatura

Te sugiero que al iniciar el semestre revises todo el material de la asignatura. Estará disponible en todo momento, pero hay algunas ligas de las cuales no tengo control de su publicación, por si llegara a desaparecer un sitio o si llegaras a detectar algún problema, házmelo saber y de inmediato colocaré algún material reemplazándolo.
En cada unidad están los materiales de estudio que utilizarás, después de leerlos deberás realizar las actividades de aprendizaje indicadas. En los textos de tus actividades, si copias un texto de cualquier otro autor es obligatorio que lo cites; de no ser así se considerará que has cometido un plagio.
Las actividades de aprendizaje están programadas para entregarse en períodos específicos, te recomiendo que cumplas con ellos. En todo el semestre habrá tres periodos de recuperación, en los cuales podrás entregar trabajos retrasados con una penalización de un punto en la calificación. Debido a esto, es necesario que tengas presentes las fechas de entrega y que envíes tus actividades al menos un día antes de que cierren, previniendo fallas en la energía eléctrica, fallas en la conectividad de Internet o cualquier otro inconveniente que no te permitiera enviar de último momento.
Al finalizar el curso, presentarás un examen final de conocimientos.

CALENDARIO DE ACTIVIDADES

Fecha	No. Unidad	No. Actividad	Descripción de la de actividad de acuerdo a la plataforma	Ponderación

25 de febrero de 2019	UNIDAD 1: Seguridad física y lineamientos generales de seguridad	Actividad 1	Para reforzar los conocimientos adquiridos acerca de este tema, revisa todo el material anteriormente proporcionado, y participa en el foro. **1.** Después de ver el video Introducción a seguridad en las redes networking (curso de seguridad informática), participa comentando acerca de un punto de lo que se menciona de la ***seguridad física y lógica***. El primer participante deberá comentar de la Seguridad física de backup / almacenamiento, el segundo de Switch / rosetas, y así sucesivamente según lo que se menciona en el video. Al terminar, envía tu participación y lee los comentarios de otro compañero, y comenta algo más que puedas aportar a su comentario. Quienes vayan participando en el foro deberán ir viendo lo que escriben sus compañeros, porque si alguien ya habló de un tema, deberán hablar de otro distinto! si se acabaron los temas, regresa al primero pero comenta algo distinto. ¡Hay mucha información al respecto! Si no lo hacen así, no contará como respuesta válida y esto se reflejará en su calificación.	8 %
04 de marzo de 2019	UNIDAD 1: Seguridad física y lineamientos generales de seguridad	Actividad 2	Para reforzar los conocimientos adquiridos acerca de este tema, prepara un documento que contenga lo siguiente: **1.** Después de haber leído el libro Procesos y herramientas para la seguridad de redes y de investigar en el manual de OSSTMM la parte de la Seguridad física además de otras fuentes, indica lo solicitado. a. Indica dos acciones que correspondan a cada tipo de revisión, explicando en un párrafo corto a lo que se refiere cada acción: **a.1** Evaluación de controles ***(2 puntos)*** **a.2** Revisión de ubicación ***(2 puntos)*** **a.3** Ubicación de alarmas ***(2 puntos)*** **a.4** Revisión de entorno ***(2 puntos)*** Al final redacta en tus propias palabras una ***conclusión*** de lo aprendido en la actividad. Recuerda mencionar lo que cites en tu trabajo para que no sea considerado un plagio. ***(2 puntos)***	7 %
11 de marzo de 2019	UNIDAD 2: Identidad	Actividad 3	Para reforzar los conocimientos de este tema, revisa el material de esta unidad, ve el video llamado ***Spoofing attacks*** e investiga por tu cuenta, luego realiza lo siguiente: **1.** Graba un video casero, donde tu expliques lo siguiente (debes grabarte y explicarlo con tu voz): **a**) Qué es el robo de identidad de un equipo de cómputo. ***(3 puntos)*** **b**) Qué es el robo de identidad de un usuario. ***(3 puntos)*** **c**) Las diferencias entre el robo de identidad en un equipo de cómputo vs. el robo de identidad de un usuario. ***(4 puntos)*** Al final, súbelo a YouTube o algún otro repositorio de video y comparte la liga con tu asesora, para su calificación.	7 %

25 de marzo de 2019	UNIDAD 3: Seguridad en la comunicación	Actividad 4	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguiente: **1.** Después de leer los dos papers, la presentación en Pretzi de seguridad informática y de investigar por tu cuenta en otras fuentes, revisa los protocolos comunicación e identifica los que proporcionan seguridad adicional. Realiza una ***infografía*** en donde indiques **características** de: **1.** Black hat hackers **2.** White hat hackers **3.** Gray hat hackers **4.** Crackers Puedes revisar los consejos para realizar infografías, y realizarlo con alguna de las herramientas recomendadas en http://www.juancmejia.com/marketing-en-redes-sociales/como-hacer-una-infografia-guia-y-herramientas-para-disenarla/	7 %
01 de abril de 2019	UNIDAD 3: Seguridad en la comunicación	Actividad 5	Para reforzar los conocimientos adquiridos acerca de este tema, realiza la lectura del paper Seguridad en redes y protocolos asociados, aparte de investigar por tu cuenta del tema. Indica ***para qué sirve*** y ***en qué situación usarías*** cada protocolo enlistado abajo: **1**. SSL ***(2 puntos)*** **2.** SSH ***(2 puntos)*** **3.** IPsec ***(2 puntos)*** **4.** PGP ***(2 puntos)*** **5.** TLS ***(2 puntos)*** *Ejemplo:* el protocolo **HTTPS** sirve para hacer el envío de páginas Web de forma más segura de la que tiene HTTP al hacer uso de un certificado de seguridad y lo usaría al hacer el envío de páginas web que requieren de más seguridad en el envío de y hacia cliente-servidor, así como el cifrado de los datos; aunque ahora ya los navegadores como Chrome o Firefox ya marcan como inseguras las páginas que no utilizan este protocolo, desde mediados de 2018.	7 %
08 de abril de 2019	UNIDAD 4: Monitoreo	Actividad 6	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguiente: **1.** Investiga la ***metodología OSSTMM*** y los siguientes conceptos, explicando en tus propias palabras dentro de una ***infografía***, qué es cada uno de ellos, para qué sirve y deberán ilustrarse cada uno con una imagen. Los párrafos que indiques de cada punto ***no deberán ser mayores a 200 caracteres.*** **a.** OSSTMM (2 puntos) **b.** Plantillas OSSTMM (2 puntos) **c.** Test de intrusión o Pentest (2 puntos) **d.** Hacking ético (2 puntos) **e.** Caja negra, gris y blanca (2 puntos)	7 %

22 de abril de 2019	UNIDAD 4: Monitoreo	Actividad 7	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguientes documentos: 1. Investiga el funcionamiento de la herramienta llamada **Wireshark**, descarga la versión más reciente en https://www.wireshark.org (no versiones anteriores, esto se tomará en cuenta para la calificación), instálala y comenta ampliamente en un documento lo siguiente: **a)** Explica paso a paso cómo la instalaste, incluyendo una imagen por cada paso de su instalación en tu equipo, instala WinPcap indicando el sistema operativo en donde lo estás instalando. ***(2 puntos)*** **b)** Escribe en un párrafo corto de no más de 200 caracteres, para qué sirve esta herramienta. ***(1 punto)*** **c)** Indica detaladamente qué tipo de filtros permite hacer el programa. ***(1 punto)*** **d)** ¿Se podría utilizar esta herramienta para revisar contraseñas en la red? Justifica tu respuestal. ***(1 punto)*** **e)** Realiza una prueba utilizando Wireshark en tu equipo, entrando a la página de la plataforma de tu licenciatura, y comprueba si se puede leer tu contraseña. Muestra imágenes, explicando paso a paso lo que hiciste. ***(3 puntos)*** Al final coloca una conclusión de tu entrega completa, utilizando tus propias palabras. Recuerda mencionar lo que cites en tu trabajo para que no sea considerado un plagio. ***(2 puntos)***	8 %
29 de abril de 2019	UNIDAD 4: Monitoreo	Actividad 8	Para reforzar los conocimientos adquiridos acerca de este tema, participa en el foro comentando acerca de lo siguiente: **1.** Después de haber leído acerca de la criptografía y de investigar por tu cuenta en otras fuentes, sube un **audio** en donde indiques los conceptos siguientes: **a)** Cifrado simétrico (**3.5 puntos**) **b)** Cifrado asimétrico (**3.5 puntos**) Finaliza concluyendo **cuál de ellos consideras es más seguro** para realizar una comunicación en la red.	7 %
06 de mayo de 2019	UNIDAD 5: Seguridad en los servicios	Actividad 9	Para reforzar los conocimientos adquiridos acerca de este tema, participa en el foro de la siguiente manera: **1.** Investiga el ataque realizado el 21 de octubre de 2016 y contesta lo siguiente de forma puntual y en tus propias palabras cualquiera de estos conceptos. Si alguien más ya opino del tema, ¡proporciona datos nuevos! a) Qué es una botnet y qué es DoS b) Qué es un dispositivo IoT y qué es DDoS c) Qué tipo de ataque se realizó el 21 de octubre de 2016 y cómo se efectuó.	8 %
13 de mayo de 2019	UNIDAD 6: Detección de vulnerabilidades e intrusiones	Actividad 10	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguiente: Después de leer el paper Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red, en la página 44 aparece una tabla con las etapas de un Pentest. Toma la información de esa tabla y crea una infografía, muy gráfica y con poco o nada de texto, donde representes cada etapa con una imagen alusiva a lo que significa cada una de ellas. Las imágenes no se deben repetir.	6 %

20 de mayo de 2019	UNIDAD 7: Autenticación y autorización de accesos	Actividad 11	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguiente: **1.** Lee acerca de la ***autenticación multi-factor*** e investiga por tu cuenta en otras fuentes, para contestar lo siguiente: **a)** Indica en tus propias palabras qué es la autenticación multi-factor y en qué beneficia su uso. ***(1 punto)*** **b)** De la autenticación que toma en cuenta lo que se, lo que soy, lo que tengo y dónde estoy ubicado, indica un ejemplo de cada uno de ellos (qué se puede utilizar). Agrega una imagen en cada uno de los puntos. **b.1** Lo que se ***(2 puntos)*** **b.2** Lo que soy ***(2 puntos)*** **b.3** Lo que tengo ***(2 puntos)*** **b.4** Dónde estoy ubicado ***(2 puntos)*** **c)** ¿Considerarías útil que se implementara en esta plataforma educativa? Indica qué problemas consideras resolvería. ***(1 punto)***	7 %
27 de mayo de 2019	UNIDAD 8: Recursos de seguridad	Actividad 12	Para reforzar los conocimientos adquiridos acerca de este tema, realiza lo siguiente: **1.** Investiga qué es el ***ransomware***. **a)** Explica en tus propias palabras qué es y cómo se produce. ***(2 puntos)*** **b)** Indica medidas preventivas ante el ransomware ***(2 puntos)*** **c)** ¿Qué tipo de dispositivos puede afectar? (Servidores, equipos de escritorio, dispositivos móviles, dispositivos de salida, equipos de telecomunicaciones, etcétera) ***(1 punto)*** **2.** Investiga acerca de la ***Deep web***: **a)** Indica sus características ***(1 punto)*** **b)** Menciona ventajas y desventajas de entrar en ella ***(2 puntos)*** **c)** ¿Está relacionada en algo con Blockchain? ***(1 punto)*** **f)** ¿Cuál es la forma de pago habitual en la DW? ***(1 punto)***	7 %

VII. Sistema de evaluación

FACTORES	DESCRIPCIÓN	
Requisitos	Al finalizar el semestre, presentarás un examen que contempla todos los temas de la asignatura (programa de la asignatura Plan 2012) y sobre todo lo realizado en las actividades. Debes tener presente que sólo tienes un intento con 110 minutos para contestarlo; al terminar ese tiempo se cerrará automáticamente, enviando la calificación obtenida.	
Porcentajes	Act. de aprendizaje Examen Final Foros TOTAL	70 % 14 % 16 % 100 %
La calificación final de la asignatura está en función de la ponderación del asesor, no de la que se visualiza en la plataforma. Es necesario solicitar por correo electónico la calificación final al asesor.		

VIII. Recursos y estratégias didácticas

Lecturas Obligatorias	(X)
Trabajos de Investigación	(X)
Clases Virtuales (PPT)	(X)
Elaboración de Actividades de Aprendizaje	(X)
Software Específico	(X)
Procesadores de Texto, Hojas de Cálculo y Editores de Presentación	(X)
Videos	(X)
Plataforma Educativa	(X)
Foro Electrónico	(X)
Chat	(X)
Tablero de Anuncios	(X)
Sitios de Internet	(X)
Plan de Trabajo	(X)