PLAN DE TRABAJO

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	RAMIREZ CHAVERO ESTHER	**Correo**	echavero@comunidad.unam.mx

III. Datos de la asignatura

Nombre	SEGURIDAD EN INFORMATICA	**Clave**	1767	**Grupo**	8791
Modalidad	Obligatoria	**Plan**	2012	**Fecha de inicio del semestre**	04 de febrero de 2025
Horas de asesoria semanal	4	**Horario**	Martes: 11:00 - 13:00 hrs Jueves: 11:00 - 13:00 hrs	**Fecha de término del semestre**	13 de junio de 2025

IV. Contenido temático

TEMA	HORAS		
	Total	**Teoría**	**Práctica**
I. Introducción a la Seguridad Informática (conceptos y definiciones)	6	6	0
II. Análisis de Riesgos	6	6	0

III. Arquitectura y diseño de seguridad	4	4	0
IV. Criptografía	10	10	0
V. Seguridad Física	4	4	0
VI. Seguridad de la red y las telecomunicaciones	14	14	0
VII. Seguridad de aplicaciones	12	12	0
VIII. Planeación de la continuidad del negocio y de la recuperación en caso de desastre (BCP/DRP)	4	4	0
IX. Legislación, regulaciones, cumplimiento e investigación	4	4	0

V. Presentación general del programa

Seré tu asesora durante el presente semestre, la forma en que trabajaremos será por medio de la plataforma, por tal motivo te solicito que para conocer de manera pertinente las actividades que debes realizar por unidad descargues el plan de trabajo desde: http://fcaenlinea1.unam.mx/planes_distancia/grupos.php?sem=7

Están establecidas 2 sesiones por semana de 2 horas de chat con (4 horas por semana), en caso de que te surja alguna duda puedes conectarte, esta conexión no es obligatoria para ti, sin embargo yo estaré a lo largo del semestre en los días y horarios establecidos. También nos podemos comunicar por la mensajería de la plataforma.

Contaremos con las siguientes sesiones de videoconferencia:

Sesión 1: 6 de febrero / 11:00 a 13:00 h. /dudas de la unidad 1, 2 y 3

Sesión 2: 27 de marzo / 11:00 a 13:00 h. /dudas de la unidad 4 y 5

Sesión 3: 24 de abril / 11:00 a 13:00 h. /dudas de la unidad 6 y 7

Sesión 4: 20 de mayo / 11:00 a 13:00 h. /dudas de la unidad 8 y 9

VI. Forma en que el alumno deberá preparar la asignatura

Revisaré tus actividades de aprendizaje y tendrás una retroalimentación a cada una de ellas en un tiempo no mayor a 72 horas hábiles. En caso de que sean entregadas de forma extemporánea, es muy probable que tarde más en revisarlas. No dejes de preguntar cuanto sea necesario y las veces que consideres pertinentes vía correo, mensajería o chat. En caso de que necesites volver a elaborar una actividad, ésta se evaluará sobre 9 (nueve).

Puedes entregar tus actividades fuera de la fecha indicada, revisaré tus actividades, solo que las que se entregan de forma extemporánea, es posible que me tarde un poco más en calificarlas.

No debes copiar y pegar información de Internet, en caso de que lo hagas tu calificación será 0 (cero).

CALENDARIO DE ACTIVIDADES

Fecha de entrega	No. Unidad	No. Actividad	Descripción de la de actividad de acuerdo a la plataforma	Ponderación
20 de febrero de 2025	UNIDAD 1: Introducción a la Seguridad Informática (conceptos y definiciones)	Act. complementaria 1	Investiga los diferentes tipos de amenazas a la seguridad informática (virus, malware, phishing, ransomware, etc.).	5 %
27 de febrero de 2025	UNIDAD 1: Introducción a la Seguridad Informática (conceptos y definiciones)	Act. complementaria 2	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un virus y un gusano? 2. ¿Qué es un firewall y cómo funciona? 3. ¿Qué es la ingeniería social y cómo se puede prevenir? 4. ¿Cuáles son las mejores prácticas para crear contraseñas seguras? 5. ¿Qué es un ataque de denegación de servicio (DoS)?	5 %
06 de marzo de 2025	UNIDAD 2: Análisis de Riesgos	Act. complementaria 1	Investiga las diferentes metodologías de análisis de riesgos (cualitativo, cuantitativo, semi-cuantitativo).	5 %
13 de marzo de 2025	UNIDAD 2: Análisis de Riesgos	Act. complementaria 2	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un riesgo y una amenaza? 2. ¿Qué es una matriz de riesgos y cómo se construye? 3. ¿Cuáles son las principales técnicas de mitigación de riesgos? 4. ¿Cómo se puede medir la efectividad de los controles de seguridad? 5. ¿Qué es el análisis de riesgos cuantitativo y cuál es su utilidad?	5 %
20 de marzo de 2025	UNIDAD 3: Arquitectura y diseño de seguridad	Act. complementaria 1	Investiga diferentes modelos de seguridad (ISO 27001, NIST Cybersecurity Framework, etc.).	5 %
25 de marzo de 2025	UNIDAD 3: Arquitectura y diseño de seguridad	Act. complementaria 2	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre una política de seguridad y una arquitectura de seguridad? 2. ¿Qué es una zona desmilitarizada (DMZ) y cuál es su función? 3. ¿Cuáles son los principales principios de diseño de una arquitectura de seguridad? 4. ¿Cómo se puede evaluar la efectividad de una arquitectura de seguridad? 5. ¿Qué es el principio de menor privilegio y por qué es importante?	5 %
27 de marzo de 2025	UNIDAD 4: Criptografía	Act. complementaria 1	Investiga algoritmos como AES, RSA, SHA-256, y sus aplicaciones.	5 %
03 de abril de 2025	UNIDAD 4: Criptografía	Act. complementaria 2	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un cifrado simétrico y uno asimétrico? 2. ¿Qué es una función hash y cuáles son sus aplicaciones? 3. ¿Cuáles son los principales tipos de ataques criptográficos? 4. ¿Cómo se puede garantizar la seguridad de las claves criptográficas? 5. ¿Qué es la criptografía post-cuántica y por qué es importante?	5 %

10 de abril de 2025	UNIDAD 5: Seguridad Física	Act. complementaria 1	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre seguridad física y seguridad lógica? 2. ¿Qué es un sistema de control de acceso y cómo funciona? 3. ¿Cuáles son los principales componentes de un sistema de videovigilancia? 4. ¿Cómo se elabora un plan de respuesta a emergencias? 5. ¿Qué es la seguridad perimetral y por qué es importante?	5 %
22 de abril de 2025	UNIDAD 6: Seguridad de la red y las telecomunicaciones	Act. complementaria 1	Analiza protocolos como IPsec, SSL/TLS, VPNs y sus funciones.	5 %
24 de abril de 2025	UNIDAD 6: Seguridad de la red y las telecomunicaciones	Act. complementaria 2	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un firewall y un IDS? 2. ¿Qué es un ataque de denegación de servicio (DDoS) y cómo se puede mitigar? 3. ¿Cuáles son los principales protocolos de autenticación utilizados en las redes? 4. ¿Cómo se puede proteger una red inalámbrica de intrusos? 5. ¿Qué es el cifrado de extremo a extremo y cómo funciona?	5 %
06 de mayo de 2025	UNIDAD 7: Seguridad de aplicaciones	Act. complementaria 1	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un ataque de inyección SQL y un ataque XSS? 2. ¿Qué es un firewall de aplicaciones web (WAF) y cómo funciona? 3. ¿Cuáles son las mejores prácticas para el manejo seguro de contraseñas? 4. ¿Cómo se puede proteger una aplicación web de ataques de denegación de servicio (DDoS)? 5. ¿Qué es el análisis de código estático y cuáles son sus ventajas?	5 %
13 de mayo de 2025	UNIDAD 8: Planeación de la continuidad del negocio y de la recuperación en caso de desastre (BCP/DRP)	Act. complementaria 1	Responde las siguientes preguntas: 1. Cuál es la diferencia entre un BCP y un DRP? 2. ¿Qué es un RPO y un RTO y cómo se determinan? 3. ¿Cuáles son los componentes clave de un BCP/DRP? 4. ¿Cómo se realiza una prueba de restauración? 5. ¿Qué papel juega la comunicación en la gestión de un desastre?	5 %
20 de mayo de 2025	UNIDAD 9: Legislación, regulaciones, cumplimiento e investigación	Act. complementaria 1	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre ética y cumplimiento? 2. ¿Cuáles son los principales riesgos legales a los que se enfrentan las empresas? 3. ¿Cómo se puede fomentar una cultura de cumplimiento dentro de una organización? 4. ¿Qué es un programa de denuncias anónimas y cómo funciona? 5. ¿Cuáles son las últimas tendencias en materia de cumplimiento?	5 %

VII. Sistema de evaluación

FACTORES	DESCRIPCIÓN

Requisitos	Deberás elaborar las actividades solicitadas en el plan de trabajo, así como realizar un examen final al finalizar el semestre, si no realizas el examen, no puedes acreditar la asignatura	
Porcentajes	Act. complementaria	70 %
	Examen(es)	30 %
	TOTAL	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)
Elaboración de Actividades de Aprendizaje	(X)
Videos	(X)
Plataforma Educativa	(X)
Chat	(X)
Sitios de Internet	(X)
Plan de Trabajo	(X)