

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	08 de febrero de 2022
Horas de asesoría semanal	4	Horario	Martes: 11:00 - 13:00 hrs Jueves: 11:00 - 13:00 hrs	Fecha de término del semestre	16 de junio de 2022

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: correo y mensajería de la plataforma.

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

Las fechas de entrega son propuestas, revisaré todas tus actividades sin importar cuando las hayas subido y no afecta en nada las entregas extemporáneas.

CALENDARIO DE ACTIVIDADES

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

17 de febrero de 2022	UNIDAD 1: Introducción a la Seguridad Informática (conceptos y definiciones)	Act. complementaria 1	Actividad complementaria 1 Después de leer: " Seguridad Informática Conceptos generales" (lo encontrarás en la siguiente liga: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf), investiga tres víctimas de alguno de los ataque en la seguridad informática e indica que tipo de ataque que sufrió.	5 %
24 de febrero de 2022	UNIDAD 2: Análisis de Riesgos	Act. de aprendizaje 2	Describe un caso real o ficticio de transferencia de riesgo. Redacta tu actividad en al menos una página completa	5 %
03 de marzo de 2022	UNIDAD 2: Análisis de Riesgos	Act. de aprendizaje 4	Realiza una lista de chequeo para determinar la seguridad en el área de informática de una empresa, incluye al menos 10 preguntas	5 %
10 de marzo de 2022	UNIDAD 3: Arquitectura y diseño de seguridad	Act. de aprendizaje 3	Realiza una tabla donde indiques las diferencias entre la acreditación y la certificación.	5 %
17 de marzo de 2022	UNIDAD 4: Criptografía	Act. complementaria 1	Actividad Complementaria 1. Investiga que son los algoritmos Hash y da por lo menos 3 ejemplos de uso.	5 %
24 de marzo de 2022	UNIDAD 5: Seguridad Física	Act. complementaria 1	Actividad complementaria 1. Indique cuales son las ventajas y desventajas de utilizar sistemas biométricos para la seguridad física de una empresa, indique por lo menos 3 aparatos que se pueden utilizar en una empresa e indique las áreas en las cuales los colocaría.	5 %
31 de marzo de 2022	UNIDAD 5: Seguridad Física	Act. complementaria 2	Actividad Complementaria 2 Elabora un documento Word en donde explique con sus propias palabras los objetivos de la seguridad física, ambiental y el control de acceso indicando las consideraciones para su implementación, según describe el Estándar ISO -17799.	5 %
07 de abril de 2022	UNIDAD 6: Seguridad de la red y las telecomunicaciones	Act. complementaria 1	Actividad complementaria 1. Responde las siguientes preguntas: <ul style="list-style-type: none"> • ¿Contra qué protege el snooping de DHCP? • ¿Contra qué protege la inspección de ARP dinámicas? • ¿Contra qué protege la protección de fuente de IP? 	3 %

21 de abril de 2022	UNIDAD 6: Seguridad de la red y las telecomunicaciones	Act. complementaria 2	Actividad complementaria 2. Responde las siguientes preguntas: <ul style="list-style-type: none"> • ¿Qué es la regla de firewall de denegación implícita? • ¿En que consiste la protección contra saturación? • ¿Qué es proxy inverso? • ¿Qué es un ataque de tabla de arco iris? • ¿Qué es el modo promiscuo? 	10 %
28 de abril de 2022	UNIDAD 7: Seguridad de aplicaciones	Act. de aprendizaje 1	Investiga qué herramientas utilizan frecuentemente los administradores de servidores para realizar la monitorización del correcto funcionamiento de UNIX y Windows; explicando detalladamente una de ellas para cada sistema.	5 %
05 de mayo de 2022	UNIDAD 8: Planeación de la continuidad del negocio y de la recuperación en caso de desastre (BCP/DRP)	Act. de aprendizaje 2	Coloca todos los riesgos físicos (internos y externos), riesgos lógicos y desastres naturales que están en los apuntes. Haz una lista con ellos y resalta los que consideras que son más comunes en una empresa de la Ciudad de México, Guadalajara o Monterrey. Puedes dar ejemplos de alguna experiencia que tengas o algunos casos que se hayan difundido en las noticias. Al final, indica la razón por la que has elegido esos riesgos y finaliza con una conclusión, si tuvieras que elegir riesgos para empresas ubicadas en Los Cabos, Puerto Vallarta o Cancún.	5 %
12 de mayo de 2022	UNIDAD 8: Planeación de la continuidad del negocio y de la recuperación en caso de desastre (BCP/DRP)	Act. de aprendizaje 3	Investiga acerca del RFC 1244 y elabora una infografía en donde presentes sus puntos más relevantes. No coloques mucho texto, explica de forma concreta cada punto.	5 %
19 de mayo de 2022	UNIDAD 9: Legislación, regulaciones, cumplimiento e investigación	Act. de aprendizaje 1	Un estudiante al estar haciendo una tarea en su computadora de pronto ve el siguiente mensaje en la pantalla: “Tu computadora ha sido asegurada por el Departamento de Justicia y el FBI, dado que se encontró una violación a las leyes federales en el uso de este equipo de cómputo. Se ha detectado que su dirección IP ha visitado sitios de pornografía y abuso de menores. Para desbloquear su computadora necesita pagar una multa de \$4,000.00 Tiene 48 horas para realizar el pago, en caso contrario será arrestado.” 1. Indica cómo se llama el ataque del que está siendo objeto. 2. Indica cómo debería catalogar este ataque (Delito relacionado con el contenido, Delito informático, Delito relacionados con infracciones de la propiedad intelectual y derechos de autor o Delito contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos), y justifica tu respuesta.	4 %

26 de mayo de 2022	UNIDAD 9: Legislación, regulaciones, cumplimiento e investigación	Act. de aprendizaje 2	<p>Imagina que eres parte del equipo de Seguridad de una empresa y se presenta un ataque de Phishing que ha estado robando las cuentas de los usuarios. Todo el equipo ha investigado y se ha dado aviso a los usuarios de este ataque que inició por correo electrónico dirigiendo a los usuarios a una liga en donde debían escribir sus datos de ingreso al sistema empresarial.</p> <p>Al momento se han cambiado las contraseñas de todos los usuarios y bloqueado la cuenta de donde provenían los correos, así como se ha bloqueado el acceso a la URL a donde dirigía el correo.</p>	3 %
--------------------	---	--------------------------	--	-----

VII. Sistema de evaluación

FACTORES	DESCRIPCIÓN								
Requisitos	Deberas elaborar las actividades solicitadas en el plan de trabajo, así como realizar un examen global al finalizar el semestre.								
Porcentajes	<table border="0"> <tr> <td data-bbox="725 707 1599 738">Act. de aprendizaje</td> <td data-bbox="1610 707 2067 738">37 %</td> </tr> <tr> <td data-bbox="725 738 1599 770">Examen Final</td> <td data-bbox="1610 738 2067 770">30 %</td> </tr> <tr> <td data-bbox="725 770 1599 802">Act. complementaria</td> <td data-bbox="1610 770 2067 802">33 %</td> </tr> <tr> <td data-bbox="725 802 1599 834">TOTAL</td> <td data-bbox="1610 802 2067 834">100 %</td> </tr> </table>	Act. de aprendizaje	37 %	Examen Final	30 %	Act. complementaria	33 %	TOTAL	100 %
Act. de aprendizaje	37 %								
Examen Final	30 %								
Act. complementaria	33 %								
TOTAL	100 %								
<p>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 electrónico la calificación final al asesor.</p>									

VIII. Recursos y estrategias didácticas

Lecturas Obligatorias	(X)
Trabajos de Investigación	(X)
Elaboración de Actividades de Aprendizaje	(X)
Procesadores de Texto, Hojas de Cálculo y Editores de Presentación	(X)
Plataforma Educativa	(X)
Foro Electrónico	(X)
Chat	(X)

Correo Electrónico	(X)
Sitios de Internet	(X)
Plan de Trabajo	(X)