UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE MEDICINA
PLAN DE ESTUDIOS DE LA LICENCIATURA DE MÉDICO CIRUJANO
Programa de las asignaturas optativas

Facultad de Medicina

Denominación: **SEGURIDAD EN INFORMÁTICA BIOMÉDICA**	**Secretaría, División, Coordinación o Departamento responsable:** Informática Biomédica **Nombre del Profesor:** Alejandro Alayola Sansores, German Domínguez Montes **Horario propuesto (día y hora):** Jueves 14:00 a 16:00 hrs.			
Clave:	**Área:** Nuevas Tecnologías de la Información y la Comunicación			**No. Créditos:** 4
Carácter: optativo	**Horas**		**Horas por semana**	**Horas por semestre**
Tipo: Teórica	**Teoría:** 34	**Práctica:** 0	2	34
Modalidad: (x)curso presencial **Infraestructura:** Aulas de IB, Basamento del Edificio A, Facultad de Medicina **( ) taller** **( ) laboratorio** **( ) otro** _____	**Duración del programa:** Semestral. **El alumno podrá cursarla desde:** quinto semestre de la carrera.			

Objetivo general:
Integrar los conocimientos sobre seguridad informática de los sistemas médicos digitales en la práctica médica, mediante la revisión de casos de amenazas, metodologías y buenas prácticas que contribuyan a la prevención de ataques cibernéticos a datos y sistemas hospitalarios; así como, a la propuesta de acciones destinadas a conseguir un sistema de información seguro y confiable.

Justificación:
Google, redes sociales, Smartphone o el Big Data son ejemplo de desarrollos y tecnologías que están revolucionando nuestra forma de vida, incluyendo la salud, estos compiten por la adaptación digital acrecentando las brechas digitales entre las generaciones XYZ de la población; con esto surge la necesidad de formar al personal de salud en el uso las nuevas tecnologías que evolucionan a un ritmo irrefrenable y a las que habrá que sumarles las transformaciones de la inteligencia artificial o la robótica.

Lo anterior, no solo implica la adaptación y la adopción de las nuevas tecnologías sino que involucra la gestión del cambio al requerir nuevas habilidades por parte de los médicos, ya que no basta con poder realizar un buen diagnóstico o tratamiento, es necesario contar con profesionales que posean las competencias digitales para hacer frente a estos retos y ser competitivos en áreas en las que antes no se tenían contempladas, por ejemplo, en la implementación de planes de seguridad informática en los sistemas de salud.

Competencias con las que se relaciona en orden de importancia:

(1) Pensamiento crítico, juicio clínico, toma de decisiones y manejo de información.
(5) Aprendizaje autorregulado y permanente.
( ) Comunicación efectiva.
(3) Conocimiento y aplicación de las ciencias biomédicas, sociomédicas y clínicas en el ejercicio de la medicina.
( ) Habilidades clínicas de diagnóstico, pronóstico, tratamiento y rehabilitación.
(2) Profesionalismo, aspectos éticos y responsabilidades legales.
( ) Salud poblacional y sistemas de salud: promoción de la salud y prevención de la enfermedad.
(4) Desarrollo y crecimiento personal.

Índice Temático				Horas
Unidad	**Tema**	**Objetivo temático**	**Subtema(s)**	**Teóricas**
1	Conceptos básicos de la Seguridad informática.	Identificar conceptos básicos de la Seguridad Informática.	1.1. Definición de seguridad informática. 1.2. Cualidades de la seguridad informática. 1.3. Aspectos legales que rigen la seguridad. informática. 1.4. Seguridad informática en los sistemas de salud institucionales e individuales. 1.5. Implicaciones de los fallos en seguridad en los sistemas informáticos dedicados a salud. 1.6. ¿Qué debemos proteger?: Datos, información y sistemas.	**3**
2	Seguridad de la Información y protección de datos en salud.	Identificar formas seguras para la protección de información y datos en salud.	2.1. Introducción a técnicas de protección de datos. 2.2. Codificación de datos e información. 2.3. Comunicaciones electrónicas seguras (codificación de archivos y correos electrónicos).	**4**
3	Vulnerabilidades más comunes en sistemas de cómputo en salud.	Identificar las vulnerabilidades más comunes de los sistemas de cómputo en salud.	3.1. Tipos y características de riesgos en los sistemas de cómputo en salud. 3.2. Top10 de Vulnerabilidades Open Web Application Security Project (OWASP).	**4**

Índice Temático				Horas
Unidad	**Tema**	**Objetivo temático**	**Subtema(s)**	**Teóricas**
4	Análisis, prevención y mitigación de riesgos de seguridad informática en sistemas de cómputo en salud.	Analizar los factores físicos y de sistema que ponen en riesgo la seguridad informática; así como las formas de prevención y mitigación.	4.1. Análisis y prevención de riesgos. 4.2. Mitigación de riesgos. 4.3. Metodologías de análisis de riesgos aplicadas a los sistemas de salud.	**4**
5	Seguridad en dispositivos médicos digitales.	Analizar la utilizad de los dispositivos médicos digitales y su seguridad.	5.1. Definición de dispositivo médico digital. 5.2. Seguridad en dispositivos médicos digitales IoT (Internet of Things). 5.3. Seguridad en dispositivos médicos implantables. 5.4. Vulnerabilidades en dispositivos médicos digitales.	**4**
6	Seguridad en ecosistemas y en Sistemas de Información Hospitalaria.	Analizar la seguridad en sistemas de información hospitalaria.	6.1. Seguridad en redes de datos. 6.2. Normas de seguridad para Sistemas de Información Hospitalario y Expediente Clínico Electrónico. 6.3. Comunicaciones seguras en Sistemas de Información Hospitalario y Expediente Clínico Electrónico con Internet Protocol security (IPSEC), versión 6 del Protocolo de Internet (IPv6) y por red privada virtual VPN). 6.4. Aseguramiento de Sistemas de Información Hospitalario y Expediente Clínico Electrónico.	**6**
7	La seguridad informática en la vida diaria del médico: amenazas más comunes.	Aplicar la prevención de daños a la seguridad informática en medicina	7.1. Seguridad en bases de datos. 7.2. Seguridad en la infraestructura médica. 7.3. Arquitectura de seguridad en el sistema de salud. 7.4. Cómputo forense. 7.5. Ética y seguridad informática.	**5**

Índice Temático				Horas
Unidad	**Tema**	**Objetivo temático**	**Subtema(s)**	**Teóricas**
8	Buenas prácticas de seguridad informática en Sistemas de salud.	Integrar los conocimientos sobre prácticas seguras en la práctica médica.	8.1. Navegación segura. 8.2. Gestores de contraseñas. 8.3. Doble autenticación. 8.4. Protocolo HTTPS, PCI, TLS, SSL.	**4**
			Total de horas:	**34**

Bibliografía Básica:

- Costas, J. Seguridad informática. España: Ra-Ma. 2014.
- Dordoigne, J. Redes informáticas: Nociones fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6). España: ENI ediciones. 2015
- Gómez, A. Seguridad informática: básica. Bogotá: Ecoe Ediciones. 2011
- Gómez, Á. Auditoría de seguridad informática. España: Starbook. 2014
- Gómez, A. Enciclopedia de la seguridad informática. España: Ra-Ma. 2014
- Roa, J. F. Seguridad informática. Madrid: McGraw-Hill. 2013.
- Sanders, C., & Smith, J. Applied network security monitoring: collection, detection, and analysis. Países Bajos: Syngress. 2014
- Katz, M. Redes y seguridad. México: Alfaomega. . 2013

Bibliografía complementaria:

- RODRIGUEZ, R. J. , GATTINI, C., ALMEIDA, G. Et col. El establecimiento de Sistemas de información en servicios de atención de salud. Guía para el análisis de requisitos, especificación de las aplicaciones y adquisición. Pan American Health Organization. Washington, D.C.: PAHO, 1999. ISBN 92 75 12266 0. 1999. Sección A1. p.8
- Vidal L, M. Cazes, G. Seguridad, datos y salud. CD Tecnología de Salud. Información Informática y Estadística de Salud. CDS. ISBN 959-7158-08-6. 2004.
- García P, G. Seguridad Informática. Folleto docente. Tema 1. Introducción a la Seguridad Informática. CD Tecnología de Salud. Información Informática y Estadística de Salud. CDS. ISBN 959-7158-08-6. 2004. p. 1-26.
- Vidal L, M. Seguridad Informática. Términos relacionados. Folleto docente. Tema 1. Introducción a la Seguridad Informática. CD Tecnología de Salud. Información Informática y Estadística de Salud. CDS. ISBN 959-7158-08-6. 2004. p. 1-11.
- Gost G, J. Gestión Sanitaria y Tecnologías de la Información. Servicio de Medicina Preventiva. Hospital de Navarra, España. CD Biblioteca Virtual para formación postgraduada de directivos del Sector Salud. ISBN 959-7158-13-2 V.2004. p.14
- Journal of the American Medical Informatics Association
- Revista Cubana de Informática Médica

Sugerencias didácticas:

Aprendizaje basado en la solución de problemas (ambientes reales).	( )
Aprendizaje Basado en Problemas	(x)
Aprendizaje basado en simulación.	( )
Aprendizaje basado en tareas.	(x)
Aprendizaje colaborativo.	( )
Aprendizaje reflexivo.	( )
Ejercicios dentro de clase	( )
Ejercicios fuera del aula	( )
e-learning	(x)
Enseñanza en pequeños grupos.	( )
Exposición audiovisual	( )
Exposición oral	( )
Lecturas obligatorias	(x)
Portafolios y documentación de avances	( )
Prácticas de campo	( )
Prácticas de taller o laboratorio	( )
Seminarios	( )
Trabajo de investigación	(x)
Trabajo en equipo.	(x)
Tutorías (tutoría entre pares (alumnos), experto-novato, y multitutoría.	( )
Otras	( )

Mecanismos de evaluación del aprendizaje de los alumnos:

Análisis crítico de artículos	(x)
Análisis de caso	(x)
Asistencia	( )
Ensayo	(x)
Exposición de seminarios por los alumnos	( )
Informe de prácticas	(x)
Lista de cotejo	( )
Mapas conceptuales	( )
Mapas mentales	( )
Participación en clase	( )
Portafolios	( )
Preguntas y respuestas en clase	( )
Presentación en clase	( )
Seminario	( )
Solución de problemas	( )
Trabajos y tareas fuera del aula	( )
Otros	( )

Perfil profesiográfico:

Requeridos:
Título de Médico Cirujano - Licenciado en informática o materias afines. Experiencia clínica de un mínimo de 3 años. Experiencia docente mínima de 1 año. Experiencia clínico-administrativa en unidades médicas de primero, segundo o tercer nivel de atención mínima de 1 año.

Deseables:
Formación y experiencia en Seguridad informática. Análisis de vulnerabilidades. Hacking Ético. Cómputo forense.