FASE 1

1. DATOS GENERALES DEL CURSO	
Nombre del curso	**Gestión de Seguridad Informática**
Programa al que pertenece	Licenciatura en Tecnologías de la Información
Experto disciplinar	Enrique Everardo Lara Gómez
Asesor pedagógico	Aida Araceli Martinez Jimenez
Créditos y horas	8 créditos / 105 horas
Eje de formación	Sistemas de información
Fecha de elaboración	12/08/16

2. COMPETENCIA

El estudiante aplica herramientas de la gestión de seguridad informática, para generar estrategias integrales de la gestión de seguridad informática orientadas al cumplimiento de los objetivos de una organización.

3. ATRIBUTOS DE LA COMPETENCIA	
Conocimientos	Conceptos básicos sobre gestión de la seguridad informática Estándares Internacionales de gestión de la seguridad informática Riesgos en las vulnerabilidades y amenazas

	Gestión de riesgos Ataques de malware Control de accesos Firewall Sistemas de detección de intrusos Criptografía Redes privadas virtuales BCP y DRP
Habilidades	Identificar metodologías y controles de tecnologías de la información para la gestión de la seguridad informática Analizar los riesgos y amenazas en seguridad informática Gestionar riesgos y controles de accesos Detectar intrusos Utilizar recursos y estrategias que eviten ataques cibernéticos Análisis de los riesgos y amenazas que existen en los espacios cibernéticos
Actitudes	Análisis, paciencia, observación visión a futuro en la identificación de alternativas para mejorar las estrategias de la Gestión de Seguridad Informática
Valores[1]	Honesta ante el pronóstico de las amenazas Ética, compromiso, responsabilidad y conciencia en la importancia de la Gestión de Seguridad Informática

[1]Aludir no sólo a valores universales, sino de postura ante los problemas y alternativas de atención.

4. COMPETENCIA GENERAL DEL PERFIL DE EGRESO CON QUE SE VINCULA O A LA QUE APOYA

Evaluar las necesidades informáticas de una organización, realizar análisis de sistemas, diseñar, desarrollar, integrar, operar y evaluar soluciones tecnológicas, así como optimizar el uso y la gestión de la infraestructura tecnológica en colaboración con equipos interdisciplinarios

5. PRODUCTO INTEGRADOR

Descripción	El estudiante aplica herramientas de la Gestión de Seguridad Informática, para generar estrategias

	integrales de Gestión de Seguridad Informática que ayudaran a mitigar los riesgos identificados en casos reales.

6. RECORTE DE CONTENIDO (unidades y contenidos).[1]		
	Unidad 1	**Unidad 2**
Título	Seguridad de las Tecnologías de la Información	Herramientas de Gestión de Seguridad Informática
Objetivo	Identificar los conceptos básicos de seguridad de la información y la Gestión de Seguridad Informática, así como las buenas prácticas sugeridas por los marcos de referencia internacionales.	Identificar las herramientas principales de la Gestión de Seguridad Informática
Contenido	• Seguridad de las Tecnologías de la Información • Marcos de Referencia de la Gestión de Seguridad Informática • Casos de estudio	• Vulnerabilidades • Amenazas • Ataques de Malware • Control de Acceso • Criptografía • Firewall • Sistemas de Detección de Intrusos • Redes Privadas Virtuales • Plan de Recuperación de Desastres • Continuidad del Negocio • Políticas • Gestión de la Seguridad Informática
Producto de la unidad	Se divide en dos: **1.** Organizador gráfico para integrar la A1 y	Desarrollar una política de Gestión de Seguridad Informática

	A2 **2.** Identificación de casos reales donde la Gestión de Seguridad Informática se vio vulnerada	
Duración	24 días	66 días

[1] Se pueden insertar o eliminar unidades (subcompetencias) dependiendo de las necesidades de cada curso

7. PRODUCTO INTEGRADOR	
Título	Estrategias Integrales de Gestión de Seguridad Informática, aplicadas en casos reales.
Objetivo	Proponer medidas de Gestión de Seguridad Informática en casos reales
Caracterización	Video no mayor a 10 minutos, donde describa las estrategias de Gestión de Seguridad Informática que considere hubiesen ayudado a mitigar las vulneraciones en cada caso de estudio. El video debe contener al menos los temas: • Vulnerabilidades • Amenazas • Vector de Ataques • Políticas • Control de Acceso • Criptografía • Firewall • Sistemas de Detección de Intrusos • Plan de Recuperación de Desastres • Políticas

9. BIBLIOGRAFÍA	
Básica	Albright. (2002). The Basic of an IT Security Policy. 09/09/2016, de 2002 Sitio web: https://www.giac.org/paper/gsec/1863/basics-security-policy/103278
	Recurso: INTECO. (2014). Cortafuegos (Firewalls): Qué son Y para qué Sirven. Noviembre 12, 2015, de Instituto Nacional de las Tecnologías de la Información Sitio web: https://www.incibe.es/file/d4f_vt-2kbzM0ex5BxJguQ Recurso: SANS. (2010). Intrusion Detection FAQ. Noviembre 12, 2015, de SANS Sitio web: https://www.sans.org/security-resources/idfaq/
	Andress J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. US: Syngress Media. Recurso: Strahler O. (2003). Network Based VPNs. Noviembre 12, 2015, de SANS Institute Sitio web: https://www.sans.org/reading-room/whitepapers/vpns/network-based-vpns-1047
	Recurso: Easttom, W.. Network Defense and Countermeasures: Principles and Practices, Second Edition. US: Pearson Certification.
	Recurso: Martin B. (2002). Disaster Recovery Plan Strategies and Processes. Noviembre 12, 2015, de SANS Institute Sitio web: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564
	inai. (2005). Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas. Noviembre 12, 2015, de inai Sitio web: http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf.
	http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf
	NMX-I-27002-NYCE-2015: TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - CÓDIGO DE BUENAS PRACTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN