UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

SÍLABO POR COMPETENCIAS

CURSO: SEGURIDAD DE LA INFORMACIÓN

DOCENTE: MG. ANA DORIS MAGDALENA BARRERA LOZA

SÍLABO DE SEGURIDAD DE LA INFORMACIÓN

I. DATOS GENERALES

LINEA DE CARRERA	SEGURIDAD INFORMÁTICA
CURSO	SEGURIDAD DE LA INFORMACIÓN
CÓDIGO	3305403
HORAS	HORA TEORICA: 2 HORA PRACTICA: 3
CICLO	VII

II. SUMILLA Y DESCRIPCIÓN DEL CURSO

SUMILLA.

La asignatura Seguridad de la Información se encuentra dentro de los cursos de especialidad, en la línea de Seguridad Informática. Es de tipo teórico práctico, debido al avance de la tecnología y la ciencia, la gestión de la información y el conocimiento, por lo que el propósito del curso es que los alumnos gestionen la seguridad de la información en cualquier tipo de empresa. Cuenta con 4 unidades didácticas cuyo contenido es el siguiente: Seguridad informática. Objetivos. Áreas. Causas de la inseguridad. Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios. Gestión de la Seguridad de la Información. Serie Norma ISO 27000. ISO 27001. Control de Accesos. Mecanismos de Seguridad. Ataques informáticos. Seguridad en Base de Datos. Seguridad en las redes. Informática forense. Políticas de seguridad.

DESCRIPCIÓN DEL CURSO.

Con la proliferación de la tecnología han aparecido notables riesgos que pueden atentar contra el funcionamiento de los sistemas, sometidos a ataques por una creciente comunidad de delincuentes informáticos. La existencia de estos riesgos y mecanismos para su detección, mitigación o recuperación obligan al profesional informático incorporar a su perfil las competencias que posibiliten evaluar e implementar medidas de seguridad en sus sistemas.

Para un estudiante de **Ingeniería Informática** es necesario y fundamental tener un conocimiento solido sobre la gestión de la seguridad de la información con el fin de desarrollar su capacidad de lógica y racionamiento para solucionar problemas relacionados con la identificación y tratamiento de los riesgos para contribuir en tomas de decisiones en forma eficiente y eficaz dentro de una organización, de tal forma que la puedan aplicar en su desarrollo profesional, una vez que egresen de la Universidad.

En el proceso de la formación del Ingeniero Informático debe incorporarse como diseñar el plan de seguridad que debería adoptar una empresa para prevenir, impedir, reducir controlar los riesgos que soporta un sistema de información y el entorno asociado con él; entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.

III.- CAPACIDADES AL FINALIZAR EL CURSO

UNIDAD DIDACTICA	***UNIDADES DIDACTICAS Y SUS CAPACIDADES RELACIONADAS***		***SEMANAS***
	CAPACIDAD DE LA UNIDAD DIDACTICA	***NOMBRE DE LA UNIDAD DIDACTICA***	
I	Administra los elementos de la gestión de la seguridad de la información dentro de una empresa para asegurar la integridad de la información según ciclo de Deming	INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN	1,2,3,4
II	Gestiona los controles de accesos necesarios en una empresa para el aseguramiento de su información de acuerdo a un sistema de avance tecnológico.	CONTROL DE ACCESOS	5,6,7,8
III	Propone los mecanismos de seguridad que se pueden implementar en una empresa de acuerdo a su realidad para evitar ataques de intrusos siguiendo recomendaciones internacionales	MECANISMOS DE SEGURIDAD	9,10,11,12
IV	Evalúa los diferentes tipos de ataques que pueden sufrir sus sistemas de redes y bases de datos, para implementar políticas de seguridad de las mismas de acuerdo a las recomendaciones de normas.	SEGURIDAD EN REDES Y BASES DE DATOS	13,14,15,16.

IV.- INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

ITEM	*INDICADOR DE CAPACIDAD AL FINAL EL CURSO*
1	Identifica los elementos y la importancia de la seguridad de la información.
2	Identifica correctamente los diferentes activos de información en una empresa.
3	Desarrolla un sistema de Gestión de la Seguridad de la Información en una empresa.
4	Aplica la gestión de riesgos que se debe tener en una organización.
5	Aplica las recomendaciones de la Serie Norma ISO 27000. ISO 27001.
6	Aplica los controles de acceso dentro de una organización.
7	Aplica los diferentes mecanismos de identificación.
8	Implementa los diferentes mecanismos de autentificación.
9	Aplica las principales reglas y políticas para la creación y administración de contraseñas.
10	Implementa los diferentes sistemas biométricos, dentro de una organización.
11	Aplica los diferentes controles criptográficos dentro de las organizaciones.
12	Reconoce los diferentes métodos de ataques informáticos.
13	Implementa adecuadamente controles de seguridad en las bases de datos.
14	Implementa adecuadamente controles de seguridad en las redes.
15	Aplica adecuadamente la informática forense.
16	Diseña e implementa políticas de seguridad dentro de una organización.

V.- DESARROLLO DE LAS UNIDADES DIDACTICAS:

<table>
<tr><td rowspan="6">UNIDAD DIDACTICA I : INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN</td><td colspan="5">CAPACIDAD DE LA UNIDAD DIDACTICA I: Administra los elementos de la gestión de la seguridad de la información dentro de una empresa para asegurar la integridad de la información según ciclo de Deming</td></tr>
<tr><td rowspan="2">SEMANA</td><td colspan="3">CONTENIDOS</td><td rowspan="2">ESTRATEGIA DIDACTICA</td><td rowspan="2">INDICADORES DE LOGRO DE LA CAPACIDAD</td></tr>
<tr><td>CONCEPTUAL</td><td>PROCEDIMENTAL</td><td>ACTITUDINAL</td></tr>
<tr><td>1</td><td>Introducción a la seguridad de la Información. Principios. Seguridad informática. Objetivos. Áreas.</td><td>Analiza los elementos de seguridad de la información y su importancia dentro de las organizaciones.</td><td>Trabajo en equipo para discutir los conceptos de seguridad de la información.</td><td>Clase expositiva y análisis de los elementos de seguridad de la información.</td><td>Identifica los elementos y la importancia de la seguridad de la información.</td></tr>
<tr><td>2</td><td>Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios. Inventario de Activos.</td><td>Analiza y comprende la importancia de los activos de información y sus vulnerabilidades.</td><td>Trabajo en equipo para realizar el inventario de activos de una organización.</td><td>Clase expositiva y análisis de activos, sus amenazas, vulnerabilidades y riesgos.</td><td>Identifica correctamente los diferentes activos de información en una empresa.</td></tr>
<tr><td>3</td><td>Gestión de la Seguridad de la Información. Beneficios. Ciclo de Deming. Planificar y Hacer. Alcance.</td><td>Analiza y comprende el sistema de Gestión de la Seguridad de la Información y sus ventajas.</td><td>Acrecienta el interés sobre el sistema de Gestión de la Seguridad de la Información.</td><td>Clase expositiva y análisis a fin de identificar las ventajas del sistema de Gestión de la Seguridad de la Información.</td><td>Desarrolla un sistema de Gestión de la Seguridad de la Información en una empresa.</td></tr>
<tr><td>4</td><td>Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos. Declaración de aplicabilidad. Implementación del SGSI. Revisar y actuar.</td><td>Comprenderla Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos.</td><td>Trabajo en equipo para acrecentar el interés sobre cómo gestionar los riesgos, su Análisis y Tratamiento de riesgos.</td><td>Clase expositiva y análisis a fin de identificar las ventajas y desventajas de la gestión de riesgos.</td><td>Aplica la gestión de riesgos que se debe tener en una organización.</td></tr>
<tr><td colspan="5">EVALUACIÓN DE LA UNIDAD DIDÁCTICA</td></tr>
<tr><td colspan="2">EVIDENCIA DE CONOCIMIENTO</td><td colspan="2">EVIDENCIA DE PRODUCTO</td><td>EVIDENCIA DE DESEMPEÑO</td></tr>
<tr><td colspan="2">Sustentación oral Argumentación de la importancia de la seguridad de la información.</td><td colspan="2">Informes y exposiciones sobre la implementación de un SGSI.</td><td>Observación en el análisis y el diseño de un SGSI.</td></tr>
</table>

UNIDAD DIDACTICA II : **CONTROL DE ACCESOS**	***CAPACIDAD DE LA UNIDAD DIDACTICA II:*** Gestiona los controles de accesos necesarios en una empresa para el aseguramiento de su información de acuerdo a un sistema de avance tecnológico.					
	SEMANA	**CONTENIDOS**			**ESTRATEGIA DIDACTICA**	**INDICADORES DE LOGRO DE LA CAPACIDAD**
		CONCEPTUAL	**PROCEDIMENTAL**	**ACTITUDINAL**		
	5	Serie Norma ISO 27000. ISO 27001. Beneficios. Implementación. Certificación.	Comprende la Serie Norma ISO 27000, ISO 27001 y sus beneficios.	Trabajo en equipo para discutir cómo implementar las recomendaciones de la Serie Norma ISO 27000. ISO 27001.	Clase expositiva y análisis de las recomendaciones de la Serie Norma ISO 27000. ISO 27001.	Aplica las recomendaciones de la Serie Norma ISO 27000. ISO 27001.
	6	Control de Accesos. Principios. Categorías de control de Acceso.	Analiza y determina que tipos de control de acceso se debe implementar según el tipo de información.	Propicia el trabajo en equipo para analizar y determina que tipos de control de acceso se debe implementar en una organización.	Exposición de ejemplos prácticos de diferentes tipos de control de accesos y sus ventajas.	Aplica los controles de acceso dentro de una organización.
	7	Técnicas de control de accesos. Identificación, Autenticación, Autorización.	Diferencia entre lo que es identificación, autenticación y autorización.	Acrecienta el interés sobre los mecanismos de identificación.	Clase expositiva y análisis de los mecanismos de identificación.	Aplica los diferentes mecanismos de identificación.
	8	Métodos de Autenticación.	Analiza los diferentes métodos de autenticación y autorización.	Propicia el trabajo en equipo para implementar mecanismos de autenticación.	Clase expositiva y análisis de los mecanismos de autentificación.	Implementa los diferentes mecanismos de autentificación.
		EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
		EVIDENCIA DE CONOCIMIENTO		**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**
		Sustentación oral. *Exposición de los informes presentados.*		*Informes escritos de controles de acceso. Informe de aplicación e implementación de controles de accesos dentro de una organización.*		*Observación en la implementación de controles de accesos.*

UNIDAD DIDACTICA III : **MECANISMOS DE SEGURIDAD**	***CAPACIDAD DE LA UNIDAD DIDACTICA III:*** Propone los mecanismos de seguridad que se pueden implementar en una empresa de acuerdo a su realidad para evitar ataques de intrusos siguiendo recomendaciones internacionales					
	SEMANA	**CONTENIDOS**			**ESTRATEGIA DIDACTICA**	**INDICADORES DE LOGRO DE LA CAPACIDAD**
		CONCEPTUAL	**PROCEDIMENTAL**	**ACTITUDINAL**		
	9	Contraseñas. Tipos de contraseñas. Administración de contraseñas de usuarios. Políticas de contraseñas.	Analiza las recomendaciones para la creación y administración de contraseñas.	Acrecienta el interés sobre la seguridad en la creación y administración de contraseñas.	Ejemplos prácticos para la creación y administración de contraseñas.	Aplica las principales reglas y políticas para la creación y administración de contraseñas.
	10	Biometría. Sistemas Biométricos. Huella digital, Verificación de voz, biometría vascular, Ventajas y desventajas. Bondades.	Analizar los diferentes sistemas biométricos que existen y se pueden implementar en las organizaciones según su realidad.	Se propicia en el estudiante el análisis de los diferentes sistemas biométricos, sus ventajas y desventajas.	Exposición de ejemplos prácticos, costos y utilización de los sistemas biométricos según las organizaciones.	Implementa los diferentes sistemas biométricos, dentro de una organización.
	11	Criptografía. Controles criptográficos. Tipos. Certificado digital. Usos y funcionamiento. Ventajas y desventajas. Firma digital. Ventajas y desventajas. Técnicas usadas.	Comprende los diferentes controles criptográficos y su aplicación dentro de las organizaciones.	Se propicia en el estudiante el análisis de los diferentes controles criptográficos y su aplicación dentro de las organizaciones.	Exposición de ejemplos prácticos de los diferentes controles criptográficos y su aplicación dentro de las organizaciones.	Aplica los diferentes controles criptográficos dentro de las organizaciones.
	12	Metodología de ataques informáticos.	Analiza los diferentes métodos de ataques informáticos.	Acrecienta el interés de conocer los diferentes métodos de ataques informáticos.	Exposición de ejemplos prácticos de los diferentes métodos de ataques informáticos.	Reconoce los diferentes métodos de ataques informáticos.
		EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
		EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE CONOCIMIENTO**		**EVIDENCIA DE CONOCIMIENTO**	
		Sustentación oral Exposición de los informes presentados.	*Informe de aplicación de mecanismos de seguridad en una empresa determinada*		*Observación en el análisis e implementación de mecanismos de seguridad.*	

UNIDAD DIDACTICA IV : **SEGURIDAD EN REDES Y BASES DE DATOS**	***CAPACIDAD DE LA UNIDAD DIDACTICA IV:*** Evalúa los diferentes tipos de ataques que pueden sufrir sus sistemas de redes y bases de datos, para implementar políticas de seguridad de las mismas de acuerdo a las recomendaciones de normas.					
	SEMANA	**CONTENIDOS**			**ESTRATEGIA DIDACTICA**	**INDICADORES DE LOGRO DE LA CAPACIDAD**
		CONCEPTUAL	**PROCEDIMENTAL**	**ACTITUDINAL**		
	13	Seguridad en Base de Datos.	Comprende los mecanismos de seguridad dentro de la administración de las bases de datos.	Se propicia en el estudiante el análisis de la importancia de la información que contienen las bases de datos	Clase expositiva y análisis a fin de identificar los mejores mecanismos de seguridad dentro de las bases de datos.	Implementa adecuadamente controles de seguridad en las bases de datos.
	14	Seguridad en las redes	Analiza mecanismos de seguridad dentro de la administración de las redes.	Se propicia en el estudiante el análisis de la importancia y seguridad de las redes.	Clase expositiva y análisis a fin de identificar los mejores mecanismos de seguridad dentro de las redes.	Implementa adecuadamente controles de seguridad en las redes.
	15	Informática forense.	Comprende la importancia y utilización de la informática forense.	Acrecienta el interés sobre el uso de la informática forense.	Clase expositiva y análisis de casos de informática forense.	Aplica adecuadamente la informática forense.
	16	Políticas Informáticas. Ventajas. La ética en la informática. Principios éticos. Los 10 mandamientos de la ética informática.	Comprende la importancia de implementar políticas de seguridad.	Acrecienta el interés sobre el uso de políticas de seguridad.	Clase expositiva y análisis delas políticas de seguridad en diferentes áreas.	Diseña e implementa políticas de seguridad dentro de una organización.
		EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
		EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE CONOCIMIENTO**		**EVIDENCIA DE CONOCIMIENTO**	
		Sustentación oral Argumentación de los informes presentados.	*Informes escritos sobre seguridad en bases de datos y redes. Informe de aplicación de políticas de seguridad.*		*Observación en el análisis y el diseño de políticas de seguridad en diferentes áreas.*	

VI.- MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDACTICOS

1. MEDIOS ESCRITOS:

- Libros
- Revistas
- Separatas

2. MEDIOS VISUALES Y ELECTRÓNICOS:

- Pizarra
- Proyector multimedia
- Ecran
- Internet, página web; www.fiisi-unjfsc.edu.pe.
- Aulas virtuales.
- Plataformas virtuales.

3. MEDIOS INFORMÁTICOS:

- Discos
- Videos
- Computadora

VII.- EVALUACION

1.- EVIDENCIA DE CONOCIMIENTO

- Preguntas escritas.
- Preguntas orales.
- Resolución de casos.
- Incidentes críticos.

2.- EVIDENCIA DE DESEMPEÑO

- Observación directa.
- Lista de chequeo.

3.- EVIDENCIA DE PRODUCTO

- Documentos.
- Proyectos.
- Reportes.

Evaluación mensual por cada unidad didáctica: Todas las unidades didácticas serán evaluadas en las tres componentes con un puntaje del 0 al 20, obteniéndose tres (03) notas:

UNIDA DIDACTICA	***EVIDENCIA DE CONOCIMIENTOS (30%)***	***EVIDENCIA DE PRODUCTO (35%)***	***EVIDENCIA DE DESEMPEÑO (35%)***
I	EC_1	EP_1	ED_1
II	EC_2	EP_2	ED_2
III	EC_3	EP_3	ED3
IV	EC_4	EP_4	ED_4

Donde el PROMEDIO FINAL ES: (PM1 + PM2 + PM3 + PM4)/4

Para aprobar el curso se requiere de una nota mínima de 10,5 puntos.

VIII.- BIBLIOGRAFIA Y REFERENCIAS WEB

UNIDAD DIDACTICA I: INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

- Garcia, A. (2011). *Seguridad Informática.*
- DIRECCION GENERAL DE MODERNIZACION ADMINISTRATIVA, PROCEDIMIENTOS EIMPULSO DE LA ADMINISTRACION ELECTRONICA. (2012). *Metodología de análisis y gestión de riesgos de los sistemas de información versión 3.0*. España: Ministerio de Hacienda y Administraciones Públicas
- Recursos de Seguridad de la Información. http://www.isaca.org - http://www.sans.org - http://www.intypedia.com/ - http://www.welivesecurity.com/la-es
- Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT versión 3.0. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

UNIDAD DIDACTICA II: CONTROL DE ACCESOS

- Piattini, M. y De Peso, E. (2001). *AUDITORIA INFORMATICA – Un enfoque práctico.* RA-MA Editorial.
- Norma Técnica Peruana NTP ISO 17799:2007 EDI. *Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información*. INDECOPI, 2007. http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf
- Norma Técnica Peruana NTP ISO 27001:2014. *Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos*. 2ª Edición. http://portal.indecopi.gob.pe/cidalerta/buscadocdet.aspx?id=21374

UNIDAD DIDACTICA III: MECANISMOS DE SEGURIDAD

- MITNICK, K., SIMON W. (2008). *El Arte de la Intrusion - Como Ser un Hacker o Evitarlos* (Spanish Edition). España:Ra-MA
- MITNICK, K., SIMON W. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. USA: Wiley Publishing.
- MITNICK, K., SIMON W. (2003). *The Art of Deception: Controlling the Human Element of Security.* USA: Wiley Publishing.

UNIDAD DIDÁCTICA IV: SEGURIDAD EN REDES Y BASES DE DATOS

- López, I. (2014). *Gestión de Bases de Datos*
- Raya. *Seguridad de una Red Netware.* (5ta. Ed.) Alfaomega.
- McCarthy. *Seguridad Digital*. Mc. Graw-Hill.

Mg. Ana Doris Magdalena Barrera Loza
CIP N° 98960
Profesor del Curso
e-mail: anadobar@hotmail.com