	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA
Código: FIISI-SI-16		Versión: 01
PROCESO: PLANIFICACION		

SÍLABO POR COMPETENCIAS

CURSO: SEGURIDAD INFORMÁTICA

DOCENTE: Mg. Elvi Renee Bazalar Ganoza

SÍLABO DE SEGURIDAD INFORMÁTICA

I. DATOS GENERALES

Línea de Carrera	Seguridad Informática.
Semestre Académico	2026-2
Código del Curso	501
Créditos	Tres (3)
Horas Semanales	Hrs. Totales: 4 Teóricas: 2 Practicas: 2
Ciclo	IX
Sección	A
Apellidos y Nombres del Docente	BAZALAR GANOZA ELVI R.
Correo Institucional	ebazalar@unjfsc.edu.pe
N° de Celular	960665948

II. SUMILLA Y DESCRIPCIÓN DEL CURSO

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.

III. CAPACIDADES AL FINALIZAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDACTICA	NOMBRE DE LA UNIDAD DIDACTICA	SEMANAS
UNIDAD 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.**	**1-4**
UNIDAD 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.**	**5-8**
UNIDAD 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.**	**9-12**
UNIDAD 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.**	**13-16**

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

NÚMERO	INDICADORES DE CAPACIDAD AL FINALIZAR 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:

Unidad Didáctica I : INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

CAPACIDAD DE LA UNIDAD DIDÁCTICA 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.

Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
	Cognitivos	Procedimental	Actitudinal		
1	Introducción a la seguridad de la Información. Principios. Seguridad informática. Objetivos. Áreas.	Analiza los elementos de seguridad de la información y su importancia dentro de las organizaciones.	Trabajo en equipo para discutir los conceptos de seguridad de la información.	**Expositiva (Docente/Alumno)** **Debate dirigido (Discusiones)** ➢ Foros, Chat **Lecturas** ➢ Uso de repositorios digitales **Lluvia de ideas (Saberes previos)** Foros, Chat	Identifica los elementos y la importancia de la seguridad de la información.
2	Activos. Amenazas. Vulnerabilidad. Riesgo e impacto en los negocios. Inventario de Activos.	Analiza y comprende la importancia de los activos de información y sus vulnerabilidades.	Trabajo en equipo para realizar el inventario de activos de una organización.		Identifica correctamente los diferentes activos de información en una empresa.
3	Gestión de la Seguridad de la Información. Beneficios. Ciclo de Deming. Planificar y Hacer. Alcance.	Analiza y comprende el sistema de Gestión de la Seguridad de la Información y sus ventajas.	Acrecienta el interés sobre el sistema de Gestión de la Seguridad de la Información.		Desarrolla un sistema de Gestión de la Seguridad de la Información en una empresa.
4	Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos. Declaración de aplicabilidad. Implementación del SGSI. Revisar y actuar.	Comprenderla Gestión de riesgos. Análisis de riesgos. Tratamiento de riesgos.	Trabajo en equipo para acrecentar el interés sobre cómo gestionar los riesgos, su Análisis y Tratamiento de riesgos.		Evaluación escrita con preguntas, utilizando los temas desarrollados en la unidad.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTOS	EVIDENCIA DE PRODUCTO	EVIDENCIA DE DESEMPEÑO
Sustentación oral Argumentación de la importancia de la seguridad de la información.	Informes y exposiciones sobre la implementación de un SGSI.	Observación en el análisis y el diseño de un SGSI.

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA	
Código: FIISI-SI-16			Versión: 01
PROCESO: PLANIFICACION			

Unidad Didáctica II : CONTROL DE ACCESOS

CAPACIDAD DE LA UNIDAD DIDÁCTICA 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 didáctica	Indicadores de logro de la capacidad
	Cognitivos	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.	**Expositiva (Docente/Alumno)** **Debate dirigido (Discusiones)** • Foros, Chat **Lecturas** • Uso de repositorios digitales **Lluvia de ideas (Saberesprevios)** Foros, Chat	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.		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.*		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.		Implementa los diferentes mecanismos de autentificación.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTOS	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.

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA	
Código: FIISI-SI-16			Versión: 01
PROCESO: PLANIFICACION			

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

Unidad Didáctica III : MECANISMOS DE SEGURIDAD

CAPACIDAD DE LA UNIDAD DIDÁCTICA 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 didáctica	Indicadores de logro de la capacidad
	Cognitivos	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.*	**Expositiva (Docente/Alumno)** **Debate dirigido (Discusiones)** • **Foros, Chat** **Lecturas** • **Uso de repositorios digitales** **Lluvia de ideas (Saberes previos)** **Foros, Chat**	*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.*		*Identifica los tiempos de acceso a la información y la transmisión un mediode conexión.*
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.*		*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.*		*Evaluación escrita con preguntas, utilizando los temas desarrollados enla unidad.*

	EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
	EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**
	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 Didáctica IV **:** SEGURIDAD EN REDES Y BASES DE DATOS

CAPACIDAD DE LA UNIDAD DIDÁCTICA 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 didáctica	Indicadores de logro de la capacidad
	Cognitivos	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.	**Expositiva (Docente/Alumno)** **Debate dirigido (Discusiones)** • **Foros, Chat** **Lecturas** • **Uso de repositorios digitales** **Lluvia de ideas (Saberesprevios)** **Foros, Chat**	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.	Acrecienta el interés sobre el uso de la informática forense.		Implementa adecuadamente controles de seguridad en las redes.
15	Informática forense.	Comprende la importancia y utilización de la informática forense.	Desarrolla los problemas propuestos.		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.		Diseña e implementa políticas de seguridad dentro de una organización.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTOS	EVIDENCIA DE PRODUCTO	EVIDENCIA DE DESEMPEÑO
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.

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDÁCTICOS

Los materiales educativos y recursos didácticos que se utilizaran en el desarrollo del presente curso:

1. MEDIOS ESCRITOS

- Materiales convencionales como separatas, guías de prácticas y pizarra
- Material de apoyo del curso.

2. MEDIOS VISUALES Y ELECTRÓNICOS

- Materiales audiovisuales como videos.
- Presentaciones multimedia, animaciones y simulaciones interactivas.
- Servicios telemáticos: sitios web, correo electrónico, chats, foros.

3. MEDIOS INFORMÁTICOS

- Laptop con conexión a internet.
- Programas informáticos (CD u on-line) educativos.
- Uso de plataformas virtual con fines educativos.

VII. EVALUACIÓN

La Evaluación es inherente al proceso de enseñanza aprendizaje y será continua y permanente. Los criterios de evaluación son de conocimiento, de desempeño y de producto.

1. Evidencias de Conocimiento.

La Evaluación será a través de pruebas escritas y orales para el análisis y autoevaluación. En cuanto al primer caso, medir la competencia a nivel interpretativo, argumentativo y propositivo, para ello debemos ver como identifica (describe, ejemplifica, relaciona, reconoce, explica, etc.); y la forma en que argumenta (plantea una afirmación, describe las refutaciones en contra de dicha afirmación, expone sus argumentos contra las refutaciones y llega a conclusiones) y la forma en que propone a través de establecer estrategias, valoraciones, generalizaciones, formulación de hipótesis, respuesta a situaciones, etc.

En cuanto a la autoevaluación permite que el estudiante reconozca sus debilidades y fortalezas para corregir o mejorar.

Las evaluaciones de este nivel serán de respuestas simples y otras con preguntas abiertas para su argumentación.

1. EVIDENCIA DE CONOCIMIENTO		PORCENTAJE	PONDERACION	INSTRUMENTOS
1	• Estudios de Casos • Cuestionarios	5%	0.05	Cuestionario
2	• Sustentación oral • Argumentación de la investigación	7%	0.07	Cuestionario
3	• Exposiciones de los trabajos, y argumentación	8%	0.08	Cuestionario
4	• Exposiciones de los trabajos, y argumentación	10%	0.1	Cuestionario/videos
Total Evidencia de Conocimiento		**30%**	**0.3**	

2. Evidencia de Desempeño.

Esta evidencia pone en acción recursos cognitivos, recursos procedimentales y recursos afectivos; todo ello en una integración que evidencia un saber hacer reflexivo; en tanto, se puede verbalizar lo que se hace, fundamentar teóricamente la práctica y evidenciar un pensamiento estratégico, dado en la observación en torno a cómo se actúa en situaciones impredecibles.

La evaluación de desempeño se evalúa ponderando como el estudiante se hace investigador aplicando los procedimientos y técnicas en el desarrollo de las clases a través de su asistencia y participación asertiva.

2. EVIDENCIA DEL DESEMPEÑO	PORCENTAJE	PONDERACION	INSTRUMENTOS
1. Presentación oportuna del trabajo	5%	0.05	Responsabilidad en la entrega de avances de los proyectos formativos
2. Formular un procedimiento para hacer el mejor planteamiento de la solución posibles.	15%	0.15	
3. Discriminar las soluciones posibles y propone una solución la que permite resolver el problema.	10%	0.1	
Total Evidencia del Desempeño	**30%**	**0.3**	

3. Evidencia de Producto.

Están implicadas en las finalidades de la competencia, por tanto, no es simplemente la entrega del producto, sino que tiene que ver con el campo de acción y los requerimientos del contexto de aplicación.

La evaluación de producto de evidencia en la entrega oportuna de sus trabajos parciales y el trabajo final.

Además, se tendrá en cuenta la asistencia como componente del desempeño, el 30% de inasistencia inhabilita el derecho a la evaluación.

3. EVIDENCIA DEL PRODUCTO	PORCENTAJE	PONDERACION	INSTRUMENTOS
1. Presentación del primer avance del proyecto formativo.	5%	0.05	Trabajo impreso de acuerdo al formato establecido
2. Contenido de forma y fondo	20%	0.2	
3. Aportes hechos al trabajo	15%	0.15	
Total Evidencia del Producto	**40%**	**0.4**	

ISO 9001 BUREAU VERITAS Certification
ISO 21001 BUREAU VERITAS Certification

VARIABLES	PONDERACIONES	UNIDADES DIDÁCTICAS DENOMINADAS MÓDULOS
Evaluación de Conocimiento	**30 %**	El ciclo académico comprende 4
Evaluación de Producto	**35%**	
Evaluación de Desempeño	**35 %**	

Siendo el promedio final (PF), el promedio simple de los promedios ponderados de cada módulo (PM1, PM2, PM3, PM4).

$$PF = \frac{PM1 + PM2 + PM3 + PM4}{4}$$

CRONOGRAMA ACADEMICO

CRONOGRAMA DE REGISTRO DE DATOS EN EL SISTEMA

SEMESTRE ACADÉMICO: 2026-2

Descripción del Proceso	Fecha de Inicio	Fecha de Finalizacion
Registro de Evaluaciones del Primer Parcial	12-10-2026	18-10-2026
Registro de Evaluaciones del Segundo Parcial	07-12-2026	13-12-2026
Registro de Evaluación Primer Módulo	14-09-2026	20-09-2026
Registro de Evaluación Segundo Módulo	12-10-2026	18-10-2026
Registro de Evaluación Tercer Módulo	09-11-2026	15-11-2026
Registro de Evaluación Cuarto Módulo	07-12-2026	13-12-2026
Registro de Evaluación Primer Módulo Medicina Ciclo 11/12	20-07-2026	26-07-2026

VIII. BIBLIOGRAFÍA 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 DIDACTICA 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.

Huacho, agosto, 2026

Mg. Elvi R. Bazalar Ganoza
Docente auxiliar