UNIVERSIDAD NACIONAL "JOSÉ FAUSTINO SÁNCHEZ CARRIÓN"

VICERRECTORADO ACADÉMICO

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

MODALIDAD PRESENCIAL
SÍLABO POR COMPETENCIAS

CURSO:

INFORMATION TECHNOLOGY AUDIT

I. DATOS GENERALES

Línea de carrera	GESTIÓN
Semestre académico	2025 – II
Código del curso	3205551
Créditos	4
Horas Semanales	Hras. Totales: 5 Teóricas: 3 Prácticas: 2
Ciclo	X
Sección	A
Apellidos y Nombres del Docentes	Costilla Retuerto Fernando Sósimo
Correo Institucional	fernandocosret@gmail.com
N de Celular	976030410

II. SUMILLA

El curso es teórico-práctico; contribuye a que el estudiante identifique los elementos de como las debilidades y fisuras en la gestión informática o situación que pongan en peligro la integridad del Negocio. Cuenta con 4 unidades didácticas cuyo contenido es el siguiente: Gestión y auditoría de TI. Plan e informe de auditoría de TI. Evaluación administrativa del departamento de informática. Evaluación de los sistemas. Evaluación del proceso de datos y de los equipos de cómputo.

DESCRIPCIÓN DEL CURSO.

La asignatura Information Technology Audit proporcionará al estudiante de Ingeniería de Sistemas los conceptos y metodologías relacionados al proceso de Seguridad de la Información. Le proporcionará las herramientas necesarias para diseñar, planear y ejecutar una Auditoría de Sistemas, comprender el Sistema de Gestión de Seguridad de Información SGSI y comprender los procesos que soportan la entrega y la administración de los sistemas de información dentro de un entorno específico.

De igual manera, la asignatura pretende que los participantes puedan delinear las políticas informáticas de una empresa y entender la importancia de los aspectos éticos de la tecnología de información para una gestión exitosa.

III. CAPACIDADES AL FINALIZAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDACTICA	NOMBRE DE LA UNIDAD DIDACTICA	SEMANAS
UNIDAD I	Realiza un análisis de brechas de Seguridad de Información.	SEGURIDAD DE INFORMACIÓN	1-4
UNIDAD II	Identifica las debilidades, riesgos y problemas inherentes a la Gestión de Seguridad de Información.	GESTIÓN Y ANÁLISIS DE RIESGOS	5-8
UNIDAD III	Planifica el desarrollo de una Auditoría de Sistemas	CONTROL INTERNO	9-12
UNIDAD IV	Proponer y aplicar prácticas para la Implementación del Modelo de Gobierno de Tecnologías de la Información basados en COBIT 2019.	COBIT 2019	13-16

IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

N	INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO
1	Detalla la seguridad de la información para cualquier entidad, empresa u organización.
2	Identifica el Modelo Operativo de TI y los Macroprocesos.
3	Realiza el estudio de controles de la ISO.
4	Realiza el estudio a detalle de los dominios de la ISO para determinar las consideraciones que se tienen en cada uno de ellos.
5	Aplica los conocimientos para una adecuada identificación del riesgo.
6	Desarrollar a gran medida la Gestión de Riesgos, identificando los riesgos.
7	Enfocarse en la seguridad del Ciberespacio.
8	Desarrolla las mejorar y asegura las operaciones de una organización.
9	Aplica la auditoría interna en una organización para el aseguramiento y consultoría objetiva diseñada para agregar valor.
10	Evalúa las herramientas de la auditoría Informática.
11	Plantea los requisitos para desarrollar la Auditoría de la Seguridad.
12	Evalúa la auditoría Informática de la empresa u organización escogida.
13	Desarrolla el Modelo COBIT y plantear casos para su utilización.
14	Identificar y aplicar lo nuevo de COBIT 2019 en el Gobierno y gestión de las organizaciones.
15	Reconoce y analiza la Implementación de COBIT 2019 en las organizaciones.
16	Identifica los procesos de Transformación Digital.

V. DESARROLLO DE LAS UNIDADES DIDACTICAS:

<table>
<tr><td rowspan="8">UNIDAD DIDACTICA I: SEGURIDAD DE INFORMACIÓN</td><td colspan="5">CAPACIDAD DE LA UNIDAD DIDACTICA I: Realiza un análisis de brechas de Seguridad de Información.</td></tr>
<tr><td rowspan="2">SEMANA</td><td colspan="3">CONTENIDOS</td><td rowspan="2">ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL</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>Presentación del curso, Seguridad de Información</td><td>Analiza la importancia de la seguridad de la información para cualquier entidad, empresa u organización.</td><td>Valora el impacto del proceso de la Seguridad en las organizaciones.</td><td rowspan="4">Clase expositiva (Docente/Alumno)
• Uso del Google Meet

Debate dirigido (Discusiones)
• Foros, chat

Lecturas
• Uso de repositorios digitales

Lluvia de ideas (Saberes previos)
• Foros, chat</td><td>Detalla la seguridad de la información para cualquier entidad, empresa u organización.</td></tr>
<tr><td>2</td><td>Modelo Operativo de T.I.</td><td>Desarrollar el Modelo Operativo.
Macroprocesos.</td><td>Propicia el desarrollo con la línea del Modelo Operativo y la estrategia de negocio de la organización.</td><td>Identifica el Modelo Operativo de TI y los Macroprocesos.</td></tr>
<tr><td>3</td><td>Introducción ISO 27001 – 27002.</td><td>Analiza los estándares y controles de la ISO para su entendimiento y comprensión.</td><td>Valora la función que tienen los controles de la ISO.</td><td>Realiza el estudio de controles de la ISO.</td></tr>
<tr><td>4</td><td>Detalle de los dominios 27002

Examen Parcial.</td><td>Analizar a detalle los dominios de la ISO.</td><td>Valorar la importancia de los dominios.</td><td>Realiza el estudio a detalle de los dominios de la ISO para determinar las consideraciones que se tienen en cada uno de ellos.</td></tr>
<tr><td></td><td colspan="4">EVALUACIÓN DE LA UNIDAD DIDÁCTICA</td></tr>
<tr><td></td><td>EVIDENCIA DE CONOCIMIENTO</td><td colspan="2">EVIDENCIA DE PRODUCTO</td><td>EVIDENCIA DE DESEMPEÑO</td></tr>
<tr><td></td><td>• Sustentación oral Argumentación de la importancia de la Seguridad de TI.</td><td colspan="2">• Exposiciones sobre la sobre la seguridad de TI.</td><td>• Comportamiento en clase presencial y observación en el análisis de la seguridad de TI.</td></tr>
</table>

UNIDAD DIDACTICA II: GESTIÓN Y ANÁLISIS DE RIESGOS

CAPACIDAD DE LA UNIDAD DIDACTICA II: Identifica las debilidades, riesgos y problemas inherentes a la Gestión de Seguridad de Información.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
5	Análisis de Riesgos. Magerit.	Identifica y analiza los riesgos.	Acrecienta el interés sobre la identificación y análisis de riesgos.	**Clase expositiva** (Docente/Alumno) • Uso del Google Meet **Debate dirigido** (Discusiones) • Foros, chat **Lecturas** • Uso de repositorios digitales **Lluvia de ideas (Saberes previos)** • Foros, chat	Aplica los conocimientos para una adecuada identificación del riesgo.
6	ISO 27005 – Gestión de Riesgos.	Conocer la gestión de los riesgos relativos a la seguridad de información.	Identificar la gestión de riesgos.		Desarrollar a gran medida la Gestión de Riesgos, identificando los riesgos.
7	Gestión de la Ciberseguridad ISO 27032.	Conocer el marco de orientación para mejorar el estado de la Ciberseguridad.	Identificar la Gestión de la Ciberseguridad.		Enfocarse en la seguridad del Ciberespacio.
8	Introducción a la Auditoría de T.I. Examen Parcial.	Determina los alcances y mejorar en la organización.	Propicia el trabajo en equipo para desarrollar y determinar alcances.		Desarrolla las mejorar y asegura las operaciones de una organización

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTO	EVIDENCIA DE PRODUCTO	EVIDENCIA DE DESEMPEÑO
• Cuestionarios. • Sustentación oral. • Exposición de los informes presentados.	• Trabajos individuales y/o grupales. • Informes de administración de riesgos y desarrollo del Plan de Seguridad de Información.	• Comportamiento en clase presencial y Observación en la elaboración del Plan de Seguridad de Información.

UNIDAD DIDACTICA III: AUDITORÍA DE SISTEMAS

CAPACIDAD DE LA UNIDAD DIDACTICA III: Planifica el desarrollo de una Auditoría de Sistemas

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
9	Auditoría Interna. Ciclo de vida de la Auditoría.	Generar aseguramiento y consultoría objetiva e independiente diseñada para agregar valor y mejorar las operaciones de una organización	Valora el rol de la Auditoría Interna.	**Clase expositiva** (Docente/Alumno) • Uso del Google Meet **Debate dirigido** (Discusiones) • Foros, chat **Lecturas** • Uso de repositorios digitales **Lluvia de ideas (Saberes previos)** • Foros, chat	Aplica la auditoría interna en una organización para el aseguramiento y consultoría objetiva diseñada para agregar valor.
10	Auditoría Informática Herramientas de la Auditoría Informática.	Analiza las herramientas de la Auditoría Informática.	Acrecienta el interés sobre el desarrollo de la auditoría informática.		Evalúa las herramientas de la auditoría Informática.
11	Auditoría de la Seguridad.	Analiza, identifica e incorpora la Auditoría de la Seguridad en el trabajo de investigación.	Participa en el análisis y resolución de trabajos de investigación.		Plantea los requisitos para desarrollar la Auditoría de la Seguridad.
12	Exposición de trabajos.	Analiza y desarrolla la auditoria informática de la empresa escogida.	Participa en el análisis y resolución de trabajos de investigación.		Evalúa la auditoría Informática de la empresa u organización escogida.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE CONOCIMIENTO**	**EVIDENCIA DE CONOCIMIENTO**
• Cuestionarios. • Sustentación oral Exposición de los informes presentados.	• Trabajos individuales y/o grupales. • Informe de planificación y realización de auditorías.	• Comportamiento en clase presencial y Observación en el análisis y desarrollo de auditorías de TI.

UNIDAD DIDACTICA IV: COBIT 2019

CAPACIDAD DE LA UNIDAD DIDACTICA IV: Proponer y aplicar prácticas para la Implementación del Modelo de Gobierno de Tecnologías de la Información basados en COBIT 2019.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
13	Introducción al marco de gobierno y gestión de TI, Principios del sistema de gobierno y del marco, Conceptos Básicos y Componentes del sistema de Gobierno.	Identificar a COBIT 2019 como El Nuevo Modelo De Gobierno Empresarial Para Información Y Tecnología.	Intereses por conocer los principios y procesos de COBIT 2019.	**Clase expositiva** (Docente/Alumno) • Uso del Google Meet **Debate dirigido** (Discusiones) • Foros, chat **Lecturas** • Uso de repositorios digitales **Lluvia de ideas (Saberes previos)** • Foros, chat	Desarrolla el Modelo COBIT y plantear casos para su utilización.
14	Factores de Diseño y Cascada de metas.	Analiza los factores de Diseño de COBIT y desarrolla la Cascada de metas.	Valora los cambios al aplicar COBIT 2019.		Identificar y aplicar lo nuevo de COBIT 2019 en el Gobierno y gestión de las organizaciones.
15	Gestión del desempeño COBIT. Diseño de un sistema de gobierno a medida. Implementation COBIT.	Desarrolla un Sistema de Gobierno a medida con la implementación de COBIT.	Acrecienta el interés por conocer el desempeño de COBIT.		Reconoce y analiza la Implementación de COBIT 2019 en las organizaciones.
16	Transformación Digital con COBIT 2019. Examen Parcial.	Analiza y comprende la Transformación Digital, como necesidad comercial.	Propicia el trabajo en equipo para determinar la importancia de la Transformación Digital con COBIT 2019.		Identifica los procesos de Transformación Digital.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTO	EVIDENCIA DE CONOCIMIENTO	EVIDENCIA DE CONOCIMIENTO
• Sustentación oral Argumentación de los informes presentados. • Cuestionarios.	• Trabajos individuales y/o grupales. • Informes sobre COBIT 2019, El Nuevo Modelo De Gobierno Empresarial.	• Comportamiento en clase presencial Observación en el análisis de los procesos de COBIT.

VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDACTICOS

Se utilizarán todos los materiales y recursos requeridos de acuerdo a la naturaleza de los temas programados. Básicamente serán:

1. MEDIOS Y PLATAFORMAS VIRTUALES:

- Casos prácticos.
- Pizarra interactiva.
- Google Meet.
- Repositorios de datos.

2. MEDIOS INFORMÁTICOS:

- Computadora.
- Tablet.
- Celulares.
- Internet.

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. EVIDENCIA DE CONOCIMIENTO

La avaluación 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.

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.

3. EVIDENCIA DE PRODUCTO

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

La evaluación de producto se evidencia en la entrega oportuna de sus trabajos.

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

VARIABLES	PONDERACIONES	UNIDADES DIDÁCTICAS DENOMINADAS MODULOS
Evaluación de Conocimiento	30 %	El ciclo académico comprende de 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).

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

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

VIII. BIBLIOGRAFIA Y REFERENCIAS WEB

8.1. UNIDAD DIDACTICA I: SEGURIDAD DE INFORMACIÓN

- García, 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.

8.2. UNIDAD DIDACTICA II: GESTIÓN Y ANÁLISIS DE RIESGOS

- Recursos de Seguridad Informática 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/

8.3. UNIDAD DIDACTICA III: AUDITORÍA DE SISTEMAS

- Hernández, E. (1995). Auditoría en Informática: un enfoque metodológico. México: Ed. Continental S.A.
- Océano - Centrum. (1996). Enciclopedia de la Auditoria. Edición española, Tomo1.
- Piattini, M. & De Peso, E. (2008). E. Auditoria de tecnologías y Sistemas de Información. España: RA-MA Editorial.
- Piattini, M. & De Peso, E. (2001). Auditoria Informática: un enfoque práctico. España: RA-MA Editorial.
- Pinilla Forero, José Dagoberto. (1997). Auditoria de Sistemas en funcionamiento. Colombia: Editorial.

8.4. UNIDAD DIDACTICA IV: COBIT 2019

- Marco de referencia COBIT® 2019: Introducción y metodología
- Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión
- Guía de diseño COBIT® 2019 Diseño de una solución de Gobierno de Información y Tecnología.
- Guía de implementación de COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología.

Huacho 05, setiembre del 2025