****

UNIVERSIDAD NACIONAL

“JOSÉ FAUSTINO SÁNCHEZ CARRIÓN”

**VICERRECTORADO ACADÉMICO**

**FACULTAD DE CIENCIA**

**ESCUELA ESTADISTICA**

**MODALIDAD NO PRESENCIAL**

**SÍLABO**

**CURSO:**

**AUDITORÍA Y SEGURIDAD DE SISTEMAS**

1. **DATOS GENERALES**

|  |  |
| --- | --- |
| Semestre académico | 2020 - I |
| Código del curso | 3204503 |
| Créditos | 3 |
| Horas Semanales | Hras. Totales: 4 Teóricas: 2 Prácticas: 2 |
| Ciclo | IX |
| Sección | A |
| Apellidos y Nombres del Docentes | Figueroa Revilla, Jorge Martín |
| Correo Institucional | jfigueroa@unjfsc.edu.pe |
| N de Celular | 999756563 |
| PRE – REQUISITO | 503-504 |
| CONDICIÓN  | OBLIGATORIA  |

1. **SUMILLA**

Sistemas de información. Concepto de auditoria. Tipos de auditoria. Plantación de la auditoria informática. Auditoria de la función informática. Metodología para el desarrollo de una auditoria informática. Documentación de sistemas. Protección de datos, tipos de control y la función.

1. **OBJETIVO GENERAL**
2. Comprender el proceso de seguridad de la información.
3. Aplicar la metodología para el proceso de auditoria en los sistemas de información.
4. Proporcionar a los alumnos las herramientas necesarias para diseñar, planear y ejecutar una Auditoria de Sistemas.
5. Entender las etapas del ciclo de Seguridad.
6. Comprender el SGSI sistema de gestión de seguridad de información.
7. Planificar el desarrollo de un Plan de Seguridad de Información.
8. Planificar el desarrollo de una auditoria de sistemas.
9. **TOPICOS CUBIERTO**
10. **Seguridad de Información**

Analiza la importancia de la seguridad de la información para cualquier entidad, empresa u organización.

1. **Modelo Operativo de T.I.**

Desarrollar el Modelo Operativo. Macroprocesos.

1. **Introducción ISO 27001 – 27002.**

Analiza los estándares y controles de la ISO para su entendimiento y comprensión.

1. **Detalle de los dominios 27002**

Analizar a detalle los dominios de la ISO.

1. **Plan Análisis de Riesgos. Magerit.**

Identifica y analiza los riesgos.

1. **ISO 27005 – Gestión de Riesgos.**

Conocer la gestión de los riesgos relativos a la seguridad de información.

1. **Gestión de la Ciberseguridad ISO 27032.**

Conocer el marco de orientación para mejorar el estado de la Ciberseguridad.

1. **Introducción a la Auditoría de T.I.**

Determina los alcances y mejorar en la organización.

OCTAVA SEMANA: EXAMEN PARCIAL

1. **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.

1. **Auditoria Informática. Herramientas de la auditoría informática.**

Analiza las herramientas de la Auditoría Informática.

1. **Auditoria de la Seguridad**

Analiza, identifica e incorpora la Auditoría de la Seguridad en el trabajo de investigación.

1. **Exposición de trabajos.**

Analiza y desarrolla la auditoria informática de la empresa escogida.

1. **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.

1. **Factores de Diseño y Cascada de metas.**

Analiza los factores de Diseño de COBIT y desarrolla la Cascada de metas.

1. **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.

1. **Transformación Digital con COBIT 2019.**

 Analiza y comprende la Transformación Digital, como necesidad comercial.

**DECIMA SEPTIMA SEMANA: EXAMEN FINAL.**

1. **APORTE DEL CURSO AL LOGRO DE RESULTADOS**

La siguiente escala de medidas es usada para evaluar la relación entre los objetivos del curso y las capacidades seleccionadas del programa.

K=clave R=relacionado vacío= no aplica

|  |  |
| --- | --- |
| a) habilidad para aplicar conocimientos de matemática, ciencia e ingeniería |  |
| b) habilidad para diseñar y conducir experimentos, así como analizar e interpretar los datos obtenidos |  |
| c) habilidad para diseñar sistemas, componentes o procesos que satisfagan las necesidades requeridas | K |
| d) habilidad para trabajar adecuadamente en un equipo multidisciplinario | R |
| e) habilidad para identificar, formular y resolver problemas de ingeniería | R |
| f) comprensión de lo que es la responsabilidad ética y profesional | K |
| g) habilidad para comunicarse con efectividad | R |
| h) una educación amplia necesaria para entender el impacto que tienen las soluciones de la ingeniería dentro de un contexto social y global |  |
| i) reconocer la necesidad y tener la habilidad de seguir aprendiendo y capacitándose a lo largo de su vida |  |
| j) conocimiento de los principales temas contemporáneos | R |
| k) habilidad de usar técnicas, destrezas y herramientas modernas necesarias en la práctica de la ingeniería |  |
| l) Comprensión de los procesos que soportan la entrega y la administración de los sistemas de información dentro de un entorno específico |  |

1. **METODOLOGIA**

EL curso exige la participación activa de los alumnos en el análisis y discusión del material de lectura asignado, así como en el desarrollo de tareas y casos de estudio. Cada equipo de trabajo deberá estar preparados para exponer (15 min. aprox) donde se escogerá al menos un participante para la presentación. Los participantes a los que no les toque la presentación deberán estar preparados interrogantes y consultas. Además del desarrollo de tareas y casos, los participantes deberán estar preparados para controles.

1. **EQUIPOS y MATERIALES**

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.
1. **EVALUACION DEL CURSO**

De acuerdo al art. 127 del Reglamento Académico existirán dos evaluaciones parciales, el promedio de cada evaluación parcial se determina anotando el promedio simple de:

* Evaluación Escrita (con un decimal sin redondeo).
* Evaluación Oral (con un decimal sin redondeo).
* Trabajo académico.

El promedio final (PF) se hará calculando: PF = (P1 + P2)/2

1. **REFERECIAS BIBLIOGRAFICAS**
* PIATTINI, M. – DE PESO, E. “Auditoria de tecnologías y Sistemas de Información”. RA-MA Editorial. España. 2008
* AUDITORIA III; “Control Interno. Áreas específicas de implantación. Procedimiento y control”, tomo 3; Didáctica Multimedia.
* Compendio de Normas Legales
* ECHENIQUE, J. “Auditoria en Informática”. Editorial Mc Graw-Hill 2001
* Enrique Hernández Hernández. “Auditoria en Informática” – Ed. Mc Graw Hill
* HERNÁNDEZ H., Enrique; “Auditoria en informática”; Editorial C.E.C.S.A.; México
* HERNANDEZ, E. “Auditoría en Informática – un enfoque metodológico”. Ed. Continental S.A. México 1995, reimpreso en 1996.
* OCEANO – CENTRUM; “Enciclopedia de la Auditoria”, tomo 1; Edición española 1996.
* PIATTINI, M. - DE PESO, E. “Auditoria Informática – un enfoque práctico” RA-MA Editorial, 2001
* PINILLA FORERO, José Dagoberto; “Auditoria Informática: un enfoque operacional”; Editorial ECOE Ediciones; Segunda Edición, Santa fe de Bogotá noviembre 1997
* PINILLA FORERO, José Dagoberto; “Auditoria de Sistemas en funcionamiento”; Editorial ROESGA, Colombia 1997.
* SOLIVERA, J. “Audit of computer systems”. Ed. Paraninfo. España 1999.

Huacho, Junio del 2020



**Mg. Ing. Jorge Martin Figueroa Revilla
CIP N° 50126
Profesor del Curso****e-mail:** **jfigueroa@unjfsc.edu.pe**