



FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DEPARTAMENTO DE INFORMATICA
SILABO DE LA EXPERIENCIA CURRICULAR
“SEGURIDAD INFORMATICA”

I. DATOS DE IDENTIFICACIÓN

- 1.1. Área : Ciencias Básicas y Tecnológicas
1.2. Facultad : Ciencias Físicas y Matemáticas
1.3. Departamento Académico : Informática
1.4. Programa de Estudios : Informática
1.5. Sede / filial : Trujillo – Valle Jequetepeque
1.6. Año - Semestre académico : 2024 - I
1.7. Ciclo : 9
1.8. Código de curso : 14078
1.9. Sección(es) : A
1.10. Créditos : 4
1.11. Tipo / Régimen : Obligatorio
1.12. Requisito : Redes de Computadoras II.
1.13. Inicio-Termino : 06/05/2024 – 30/08/2024
1.14. Organización semestral del tiempo :

Actividades	Total de Horas	Unidad		
		I	II	III
Teóricas	30	10	10	10
Prácticas	57	19	19	19
Retroalimentación	03	01	01	01
Total de horas	90			

1.15. Docente(s):

Condición	Apellidos y Nombres	Profesión	Correo Institucional
Coordinador	Mg. Mendoza Torres, Edwin Raul	Ing. Informático	emendoza@unitru.edu.pe

II. SUMILLA

- 2.1. Área : Estudios de especialidad.
2.2. Naturaleza : Teórico - Práctico.
2.3. Propósito : Se orienta a desarrollar la unidad de competencia de enseñanza y contribuye directamente al logro de las capacidades terminales CT1.1; CT2.1 y CT2.7 del perfil del egresado.

La experiencia curricular, será útil para que el estudiante demuestre en su práctica profesional conocimientos actualizados sobre cómo se implementa soluciones de redes de diferente complejidad.

- 2.4. Contenidos : Se ha organizado el desarrollo de la experiencia curricular en tres unidades temáticas:

- Unidad I : Introducción, Peligro en la red, Análisis de los principales sistemas operativos.
Unidad II : Protocolos de red, verificación de la conectividad.
Unidad III : Servicios de redes e Infraestructura de la Seguridad Informática.



Visado III. COMPETENCIAS

COMPETENCIA GENERAL:

Demuestra conocimientos teóricos-prácticos del campo de la informática que lo habilitan para desenvolverse como profesionales e investigadores en ciencia computacional, competentes e íntegros con responsabilidad social, capaces de resolver problemas computacionales en diferentes ámbitos de la sociedad, con calidad y rigor científico para lograr el desarrollo sostenible de la región y del país.

COMPETENCIAS ESPECÍFICAS:

Unidad de Competencia 1:

Participa en proyectos multidisciplinarios para resolver problemas computacionales en diferentes ámbitos de la sociedad demostrando su competencia profesional e integridad.

Capacidades Terminales:

CT 1.1 Maneja e integra cuatro habilidades básicas: abstracción, pensamiento sistémico, experimentación y trabajo en equipo.

Unidad de Competencia 2:

Aplica con ética profesional conocimientos computacionales teórico-práctico-aplicación involucrándose como actor principal del desarrollo de la sociedad.

Capacidades Terminales:

CT 2.1 Aplica fundamentos matemáticos, principios algorítmicos y teoría de ciencia de la computación en el modelamiento y diseño de sistemas basados en computadora.

CT 2.7 Reconoce y valora las relaciones entre Informática y Sociedad.

INFORMACIÓN DE CONTENIDOS.

Contenido: Servicios de redes (DNS, DHCP, HTTP, SSH, etc), Amenazas y ataques, seguridad en redes, criptografía, plataformas de seguridad además la implementación de soluciones de red de diferente complejidad.

RESUMIR LOS LOGROS A LOS QUE APORTA LAS CAPACIDADES.

La experiencia curricular, será útil para que el estudiante demuestre en su práctica profesional conocimientos actualizados sobre cómo se implementa soluciones de redes de diferente complejidad.



PROGRAMACIÓN ACADÉMICA

Visado	CAPACIDADES TERMINALES (CT)	RESULTADOS DE APRENDIZAJES	CONTENIDOS	ESTRATEGIAS DIDÁCTICA	EVIDENCIAS DE EVALUACIÓN	INSTRUMENTO DE EVALUACION	SEMANAS (INICIO Y TÉRMINO)
	<p>CT 1.5 Comprende los aspectos y la responsabilidad profesional, ética, legal, de seguridad y social..</p> <p>CT 1.6 Contribuye con los resultados de la investigación a resolver problemas de la comunidad nacional e internacional.</p>	<p>RDA1: : Instalar máquinas virtuales para crear un entorno seguro para la implementación y el análisis de los eventos de amenazas de ciberseguridad</p> <p>RDA2: Explicar el rol del analista de operaciones de ciberseguridad en la empresa.</p> <p>RDA3: Explicar las funciones y las características del sistema operativo Windows necesarias para el análisis de ciberseguridad</p>	<p><u>Unidad I: Introducción, Peligro en la red, Análisis de S.Os.</u></p> <p><u>Semana 1</u> Actividades Bicentenario UNT</p> <p><u>Semana 2</u> Teoría: Descripción del Silabo. El peligro Combatientes en la guerra contra la ciberdelincuencia. Práctica: Conformación de grupos. Focus group. Laboratorio: Visualizar a los hackers de sombrero negro. Y Convertirse en defensor</p> <p><u>Semana 3</u> Teoría: Sistema operativo Windows. Práctica: Focus group. Laboratorio: Monitorear y administrar recursos del sistema en Windows</p>	<p>1. Presentación Docente</p> <p>2. Socialización del sílabo</p> <p>3. Exposición docente</p> <p>4. Foro de consultas.</p> <p>5. Presentación de tareas</p>	<p>-Actividad asignada.</p> <p>-Guía de practica</p> <p>-Cuestionario.</p>	<p>Rúbrica para las actividades asignadas</p> <p>Autoevaluación.</p>	<p><u>Semana 1</u> Del 06 de mayo al 10 de mayo</p> <p><u>Semana 2</u> Del 13 de mayo al 17 de mayo</p> <p><u>Semana 3</u> Del 20 de mayo al 24 de mayo</p>



Visado

		<u>Semana 4</u> Teoría: Descripción General de Linux. Práctica: Uso del Shell linux. Laboratorio: Administración Básica del Servidor				Semana 4 Del 27 de mayo al 31 de mayo
		<u>Semana 5</u> Teoría: Examen de la Unidad I. Práctica: Solución del examen parcial. Retroalimentación. Laboratorio: Retroalimentación de trabajos de unidad.				Semana 5 Del 03 de junio al 07 de junio
CT 1.7 Contribuye con los resultados de la investigación a resolver problemas de la comunidad nacional e internacional. CT 2.7 Reconoce y valora las relaciones entre	RDA4: Explicar las funciones y las características del sistema operativo Linux. RDA5: Analizar el funcionamiento de los	<u>Unidad II: Planificación de procesos, Sincronización y Gestión de Memoria fase - I.</u> <u>Semana 6</u> Teoría: Protocolos de Red. Práctica: Encapsulamiento y desencapsulamiento. Laboratorio: Introducción a Wireshark.	1. Exposición docente 2. Foro de consultas. 3. Presentación de tareas (Aula virtual)	-Actividad asignada. -Guía de practica -Cuestionario.	Rúbrica para las actividades asignadas Autoevaluación.	<u>Semana 6</u> Del 10 de junio al 14 de junio



Informática y
Seguridad.

Visado

	protocolos y servicios de red..	<u>Semana 7</u> Teoría: Protocolo de Internet y Ethernet. Practica: Direcccionamiento IP Laboratorio: IPv4 e IPv6				<u>Semana 7</u> Del 17 de junio al 21 de junio
	RDA6: Explicar el funcionamiento de la infraestructura de red					
	RDA7: Clasificar los diversos tipos de ataques a la red.	<u>Semana 8</u> Teoría: Verificación de la Conectividad . Practica: Utilidades Ping y Tracer route. Laboratorio: Trazado de ruta				<u>Semana 8</u> Del 24 de junio al 28 de junio
	RDA8: Emplear herramientas de monitoreo de redes para identificar ataques a servicios y protocolos de red.					
	RDA9: Explicar cómo evitar el acceso malicioso a las redes informáticas, los hosts y los datos	<u>Semana 9</u> Teoría: Protocolo ARP y capa de Transporte. Práctica: Caso capa de transporte. Laboratorio: Exploración de Nmap.				<u>Semana 9</u> Del 01 de julio al 05 de julio
	RDA10: Explicar el impacto de la criptografía en el monitoreo de la seguridad de redes					



Visado

		<p><u>Semana 10:</u> Teoría: Examen de la Unidad II. Práctica: Solución del examen parcial. Retroalimentación. Laboratorio: Retroalimentación de trabajos de unidad.</p>				<p><u>Semana 10</u> Del 08 de julio al 12 de julio</p>
<p>CT 1.3 Desarrolla la capacidad de aprendizaje de forma autónoma a lo largo de su vida.</p> <p>CT 1.6 Realiza investigaciones con rigor científico.</p>	<p>RDA11: Explicar cómo investigar los ataques y las vulnerabilidades de los terminales.</p> <p>RDA12: Evaluar alertas de seguridad de la red</p>	<p><u>Unidad III Gestión de Memoria fase – II, Gestión de almacenamiento masivo, Protección y Seguridad</u></p> <p><u>Semana 11</u> Teoría: Servicios de Red Practica: Servidores DNS, DHCP, NAT</p>	<p>1. Exposición docente</p> <p>2. Foro de consultas.</p> <p>3. Presentación de tareas (Aula virtual)</p>	<p>-Actividad asignada.</p> <p>-Guía de practica</p> <p>-Cuestionario.</p>	<p>Rúbrica para las actividades asignadas.</p> <p>Rúbrica para Artículo estado del arte.</p>	<p><u>Semana 11</u> Del 15 de julio al 19 de julio</p>



Visado

	RDA13: Analizar datos de intrusiones en redes para identificar vulnerabilidades y hosts afectados.	Laboratorio: Utilizar wireshark para examinar capturas TCP y UDP			Autoevaluación.	
	RDA14: Aplicar modelos de respuesta ante incidentes para administrar los incidentes relacionados con la seguridad de la red	<p><u>Semana 12</u> Teoría: Dispositivos de comunicaciones de redes – Infraestructura de Seguridad Practica: Dispositivos de redes – Servidores AAA. Laboratorio: Demostración de ACL - Netflow</p>				<p><u>Semana 12</u> Del 22 de julio al 26 de julio</p>
		<p><u>Semana 13</u> Teoría: Los atacantes y sus herramientas – Amenazas y ataques comunes Practica: Herramientas de los atacantes Laboratorio: Ingeniería social</p>				<p><u>Semana 13</u> Del 29 de julio al 02 de agosto</p>



Visado

		<p><u>Semana 14</u> Teoría: Monitoreo de red y sus herramientas. Práctica: Herramientas de monitoreo de red. Laboratorio: Registrar la actividad en la red.</p>				<p><u>Semana 14</u> Del 05 de agosto al 09 de agosto</p>
		<p><u>Semana 15</u> Teoría: Examen de la Unidad III. Práctica: Solución del examen parcial. Retroalimentación. Laboratorio: Retroalimentación de trabajos de unidad.</p>				<p><u>Semana 15</u> Del 12 de agosto al 16 de agosto</p>
		<p><u>Semana 16</u> Examen sustitutorio.</p> <p><u>Semana 17</u> Examen de aplazado.</p>				<p><u>Semana 16</u> Del 19 de agosto al 24 de agosto</p> <p><u>Semana 17</u> Del 26 de agosto al 30 de agosto</p>



IA DE EVALUACIÓN

Visado Base Legal.

Reglamento de normas generales de evaluación y aprendizaje, de los estudiantes de pregrado de la Universidad Nacional de Trujillo.

5.2. Principios y procedimientos:

- La evaluación por competencias se caracteriza por ser progresiva, formativa y auténtica; por lo que es de procesos e integral, y se orienta a asegurar el logro de los aprendizajes esperados, capacidades y competencias.
- Se evalúan las evidencias concretas a través de las cuales los estudiantes demuestran haber logrado aprendizajes (informes, portafolio digital.) y sirven para recoger información, tomar decisiones oportunas e informar a los propios estudiantes y a las autoridades respectivas de las acciones de mejora.
- Al valorar los resultados y/o productos se debe tener en cuenta una ponderación específica según los instrumentos de evaluación empleados.

5.3. Obtención de promedio.

Descripción	Porcentaje
Unidad 1.	
Práctica(s) de laboratorio.	30%
Desarrollo de Actividades.	20%
Examen de Unidad.	50%
Unidad 2.	
Práctica(s) de laboratorio.	30%
Desarrollo de Actividades.	20%
Examen de Unidad.	50%
Unidad 3.	
Práctica(s) de laboratorio.	20%
Desarrollo de Actividades.	10%
Trabajo Final.	40%
Examen de Unidad.	30%
Examen sustitutorio.	
Examen de aplazado.	

$$PU_1 = (PL * 0.3) + (DA * 0.2) + (EU * 0.5)$$

$$PU_2 = (PL * 0.3) + (DA * 0.2) + (EU * 0.5)$$

$$PU_3 = (PL * 0.2) + (DA * 0.1) + (EU * 0.3) + (TF * 0.4)$$

Donde:

PU: Promedio de unidad.

PL : Práctica(s) de laboratorio.

DA: Desarrollo de actividad(es).

TF : Trabajo final de curso(Artículo estado de arte).

EU: Examen de unidad.

Descripción	Porcentaje
PU ₁	33%
PU ₂	33%
PU ₃	34%

$$PP = PU_1 * 0.33 + PU_2 * 0.33 + PU_3 * 0.34$$

Donde:



PP: Promedio promocional del curso.

PU_(n): Promedio de unidad.

Visado n : Número de unidad (1, 2, 3)

2.5. Criterios para la promoción.

- El sistema de calificación es vigesimal (0-20).
- La nota aprobatoria es 14.
- En el promedio promocional, el medio punto (0.5) favorece al estudiante.
- El fundamento para la promoción en una asignatura es el cumplimiento oportuno de los productos de aprendizaje.
- La asistencia es obligatoria, tener más del 30% de inasistencias injustificadas es causal de inhabilitación.
- Los estudiantes que alcancen el nivel de inicio pasarán a un examen sustitutorio el cual reemplazará a la nota más baja obtenida en las tres unidades, se dará en la última semana de la programación.
- En el caso de los estudiantes aplazados la nota que obtengan será promediada con la nota promocional obtenida en el ciclo regular.

2.6. Nivel de logro.

Es el aprendizaje alcanzado por el estudiante. Para la determinación de los niveles de logro de los resultados de aprendizaje de los estudiantes se toma en cuenta lo siguiente:

- **Nivel Inicial (0-13):** Necesita reforzar las capacidades previstas en coordinación con Dirección de Escuela y/o Estudios Generales, según corresponda.
- **Nivel Logrado (14-17):** Muestra un nivel adecuado de dominio de las capacidades en la asignatura.
- **Nivel Avanzado (18-20):** Posee un alto nivel de dominio de las capacidades de la asignatura.

VI. TUTORÍA ACADÉMICA

6.1 Propósito:

Acompañamiento y monitoreo académico oportuno al estudiante que no logra las competencias programadas en el proceso del desarrollo de la experiencia curricular como parte del plan de mejora.

6.2 Desarrollo de la Tutoría

- Día : Miércoles
- Medio : oficina cubil
- Horario : 11:00 am. a 13:00 pm.

VII. REFERENCIAS.

PROQUEST

Calder, Alan. ISO27001/ISO27002: una Guía de Bolsillo, IT Governance Ltd, 2017. ProQuest Ebook Central, <https://ebookcentral.proquest.com/lib/unitrupe/detail.action?docID=5255172>.

Biblioteca de la facultad CCFFMM:

GIL VERA, VÍCTOR DANIEL & GIL VERA, JUAN CARLOS. (2017) SEGURIDAD INFORMÁTICA ORGANIZACIONAL: una guía de estudios. Sin editorial.

Medio virtual:

Hector giusepphe Iñiguez Estrada,.(2020) SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES. <https://es.b-ok.lat/book/14023838/f175d6>

Guillermo Navarro Arribas "Sistema de Cortafuegos" Universidad Oberta de Cataluña UOC (Libro Texto Acceso Libre)..



[penaccess.uoc.edu/webapps/o2/bitstream/10609/62865/6/Seguridad%20en%20redes_M%C3%B3dulo
Sistemas%20de%20cortafuegos.pdf](https://penaccess.uoc.edu/webapps/o2/bitstream/10609/62865/6/Seguridad%20en%20redes_M%C3%B3dulo%20Sistemas%20de%20cortafuegos.pdf)

Visado

El presente Sílabo de la Experiencia Curricular “Seguridad Informática”, ha sido Visado por el director de la Escuela Profesional de Informática, quien da conformidad al sílabo registrado por el docente que fue designado por el jefe del Departamento Académico de Informática.