



**Universidad de las Regiones Autónomas  
de la Costa Caribe Nicaragüense**  
**Nombre del Recinto, CUR o Extensión**

**Nombre del Área**  
**Nombre de la Carrera**

**Sílabo**  
**Nombre de la Asignatura**

**Elaborado por:**  
**Nombre del autor**

**Plan de Estudio 20XX**  
**X Año**  
**X Semestre**  
**Año Lectivo 20XX**

**5 de febrero de 2025**

# 1. Datos Generales

<b>Nombre de la institución:</b>	Universidad de las Regiones Autónomas de la Costa Caribe Nicaragüense
<b>Área académica:</b>	Nombre del Area Académica
<b>Nombre de la carrera:</b>	Nombre de la Carrera
<b>Nombre de la asignatura:</b>	Nombre de la asignatura
<b>Código de la asignatura:</b>	XXX-XXX
<b>Plan de estudio:</b>	20XX
<b>Turno:</b>	Diurno/Nocturno
<b>Modalidad</b>	Presencial
<b>Ubicación del ciclo académico:</b>	X año cuatrimestral/X año semestral
<b>Cuatrimestre/Semestre:</b>	X Cuatrimestre/X Semestre
<b>Número total de horas:</b>	X horas (x horas de atención directa, x horas de trabajo independiente)
<b>Frecuencia semanal:</b>	X horas semanales
<b>Número de créditos:</b>	X créditos
<b>Área de formación:</b>	Profesionalizante
<b>Requisito de procedencia:</b>	Nombre de la asignatura requisito
<b>Autor:</b>	Nombre del autor del sílabo

## **2. Descriptor de la asignatura**

Acá va el descriptor de la asignatura.

### **3. Resultados de aprendizaje**

#### **Conceptuales:**

- Conceptual 1
- Conceptual 2
- Conceptual 3

#### **Procedimentales:**

- Procedimental 1
- Procedimental 2
- Procedimental 3

#### **Actitudinales:**

- Actitudinal 1
- Actitudinal 2
- Actitudinal 3

## 4. Contenidos

No.	Unidad	Horas Teóricas	Horas Prácticas	Horas de Trabajo Independiente	Total de Horas
I	Nombre de la unidad I	4	4	16	24
II	Nombre de la unidad II	4	4	16	24
III	Nombre de la unidad III	4	4	16	24
IV	Nombre de la unidad IV	4	4	16	24
V	Nombre de la unidad V	4	4	16	24
VI	Nombre de la unidad VI	4	4	16	24
<b>Evaluaciones</b>		4	4	16	24
<b>Total</b>		4	4	16	24

## 5. Estrategias Metodológicas

A continuación, se presenta una propuesta híbrida para la clase de Seguridad Aplicada a la Informática, en la que se combinan estrategias tradicionales actualizadas con enfoques innovadores. El objetivo es transformar el proceso de enseñanza en una experiencia inmersiva, colaborativa y motivadora, en la que se integren simulaciones, gamificación, actividades de metacognición y eventos tipo Capture The Flag (CTF).

La propuesta parte de un enfoque humanístico e inclusivo, en el que se valoran y respetan las diversidades culturales, de género y los distintos estilos de aprendizaje. Se busca crear un ambiente en el que los estudiantes se sientan acogidos y puedan expresar sus ideas libremente. Para ello, se promueve la comunicación asertiva y la resolución de conflictos a través de actividades como role-playing y debates, que ayudan a fortalecer la empatía y el compromiso ético. Además, se fomenta el trabajo en equipo mediante la conformación de grupos heterogéneos que permitan compartir perspectivas y desarrollar habilidades interpersonales y técnicas de manera simultánea.

Las sesiones teóricas se llevan a cabo de forma interactiva, combinando el modelo de aula invertida con técnicas de microaprendizaje. Antes de cada clase, se facilita a los estudiantes el acceso a contenidos multimedia –como videos, podcasts y lecturas interactivas– que les permitan familiarizarse con los temas. Este enfoque permite que el tiempo en el aula se dedique a la discusión, a la aplicación práctica y a la resolución de problemas reales, utilizando herramientas de respuesta en tiempo real que ayudan a verificar la comprensión y a fomentar la participación activa.

El componente práctico del curso se refuerza mediante talleres y laboratorios virtuales, en los que se utilizan simuladores para recrear escenarios reales de ataques y defensas en sistemas informáticos. En estos espacios, los estudiantes pueden poner a prueba sus conocimientos en un entorno seguro y controlado, aplicando técnicas de análisis, detección y mitigación de vulnerabilidades. Las simulaciones se integran con estudios de caso y talleres que permiten establecer conexiones directas entre la teoría y su aplicación en situaciones reales.

Un elemento central e innovador en esta propuesta es la incorporación de la gamificación y la realización de eventos tipo Capture The Flag (CTF). Se diseñan actividades lúdicas y competitivas que transforman el aprendizaje en una experiencia motivadora. El sistema de gamificación se basa en la asignación de puntos, niveles y recompensas simbólicas, reconociendo el esfuerzo y el logro de competencias técnicas a medida que los estudiantes resuelven desafíos en tiempo real. Los eventos CTF, organizados de forma individual o en equipos, desafían a los participantes a identificar y explotar vulnerabilidades en entornos simulados, fomentando el pensamiento crítico, la creatividad y el trabajo colaborativo.

La integración de tecnologías es otro pilar fundamental de esta propuesta. Se emplean plataformas educativas como MOODLE para gestionar contenidos y evaluaciones en línea, y repositorios colaborativos como GitHub para facilitar la documentación y revisión de proyectos. Además, se utilizan aplicaciones de mensajería y, en algunos casos, chatbots o aplicaciones móviles que proporcionan asistencia inmediata durante las actividades prácticas. Estas herramientas permiten también el seguimiento del desempeño

de los estudiantes, facilitando una retroalimentación automatizada que ayuda a ajustar las estrategias pedagógicas en función de las necesidades de cada grupo.

Por último, se pone especial énfasis en la evaluación formativa y en el desarrollo de habilidades metacognitivas. A lo largo del curso se realizan evaluaciones continuas mediante quizzes, autoevaluaciones y evaluaciones entre pares, que ofrecen retroalimentación inmediata y permiten identificar áreas de mejora. Los estudiantes mantienen portafolios digitales en los que registran su progreso, reflexionan sobre sus aprendizajes y planifican estrategias para superar desafíos. Al final de cada unidad o evento significativo, como los hackathons o CTF, se realizan sesiones de reflexión en las que se analizan tanto los aciertos como las áreas que requieren mayor atención, consolidando así el ciclo de mejora continua y promoviendo la autorreflexión.

En resumen, esta propuesta híbrida combina la solidez de métodos tradicionales –actualizados con simulaciones y el uso intensivo de tecnologías– con elementos innovadores que incluyen gamificación, actividades metacognitivas y eventos CTF. El resultado es un ambiente de aprendizaje integral y dinámico, en el que los estudiantes no solo adquieren competencias técnicas en seguridad informática, sino que también desarrollan habilidades blandas, éticas y colaborativas, preparándolos de manera óptima para los desafíos del entorno profesional actual.