





UNIVERSIDAD DE GUAYAQUIL  
VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL

				UNIVERSIDAD DE GUAYAQUIL SYLLABUS				 Carrera de <b>SOFTWARE</b> <small>Ciencia e innovación para la excelencia</small>			
A: DATOS INFORMATIVOS											
Facultad:		CIENCIAS MATEMÁTICAS Y FÍSICAS					Dominio:		CIENCIAS BÁSICAS, BIOCONOCIMIENTO Y DESARROLLO INDUSTRIAL		
Carrera:		SOFTWARE									
Asignatura:		SEGURIDAD INFORMÁTICA		Código:	814		UOC:	UNIDAD PROFESIONAL		Campo Formación:	PRAXIS PROFESIONAL
Semestre:		OCTAVO		Paralelo:				Horario:			
Plan de estudios:		N° Créditos:	3	Horas componente docencia:	24(S)	Horas componente de práctica y experimentación:		24(S)		Horas componente trabajo autónomas:	96(A)
Prerrequisitos:		414 REDES DE COMPUTADORAS / 511 DISEÑO Y ARQUITECTURA DE SOFTWARE									
Período académico:		2021-2022							Ciclo:		I
Docente:						Título de posgrado:					



UNIVERSIDAD DE GUAYAQUIL  
VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL

**B: JUSTIFICACIÓN DEL CONOCIMIENTO DEL SYLLABUS EN EL CAMPO DE FORMACIÓN**

**Breve justificación de los contenidos del Syllabus:**

La seguridad informática introduce al estudiante en los conocimientos básicos que permita identificar los elementos que forman parte de la seguridad de la información y proponer políticas de seguridad contra intrusos en redes corporativas, empresariales e institucionales mediante el análisis de métodos y técnicas adecuadas. Se busca diseñar estructuras de redes que permitan transmitir información en las redes, aplicando modelos de encriptaciones para establecer comunicaciones seguras.

**Objetivo General:**

Crear esquemas de seguridad mediante el uso y análisis de herramientas, técnicas y metodologías contemporáneas para salvaguardar los activos de información dentro de una organización

Aportes teóricos	Aportes metodológicos	Aporte a la comprensión de los problemas del campo profesional	Contextos de aplicación
Provee los conceptos y definiciones relacionadas a la seguridad informática, los tipos de ataques y los actores que participan para diseñar estructuras de comunicaciones seguras.  Emplea herramientas para diseñar estructuras de comunicaciones seguras para la transferencia de información.	Análisis de estructuras básicas de los tipos de ataques informáticos, los métodos, modelos y componentes básicos en la seguridad de la información.  Desarrollo de trabajos colaborativos para el diseño de estructuras de redes seguras, tomando como referencia las normas ISO 27001.	Analiza las condiciones mediante casos de estudios con el fin de aplicar la seguridad en sistemas de información y gestión de la seguridad lógica y física de un departamento de sistemas.	El campo de aplicación son áreas de sistemas tecnológicos, de información y comunicación que necesiten una evaluación exhaustiva de las seguridades de comunicación incluyendo la revisión de políticas y procedimientos internos de seguridad en una organización.



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

**C: PROPÓSITOS Y APORTES AL PERFIL DE EGRESO**

Propósitos del aprendizaje del syllabus relacionado con el campo de estudio y objetivos de la carrera:	Aportes al perfil de egreso: Capacidades integrales y/o competencias, logros o resultados de aprendizaje			
	Genéricas de la UG.	Específicas de la carrera.	Logros de aprendizaje.	Ámbito.
Aplicar los conocimientos para diseñar arquitecturas de seguridad que permitan salvaguardar los datos como principal activo en las organizaciones.	Organiza, interpreta, construye y evalúa el conocimiento de forma crítica, creativa e integrada, para la toma de decisiones y la resolución de problemas.	Evalúe estrategias, tome decisiones y procese información en el desarrollo de algoritmos Computacionales.	Diseña soluciones de seguridad perimetral que permitan proteger los recursos de la organización contra intrusiones, amenazas, ataques y degradaciones de servicio.	Conocimientos.
Analizar las diferentes herramientas, métodos, técnicas y metodologías que sirven de protección a la información dentro de instituciones públicas y privadas.	Piensa, gestiona y evalúa tensiones y problemas con enfoque sistémico, utilizando los lenguajes, métodos, procesos y procedimientos disciplinarios para la explicación e intervención de la realidad, asumiendo sus transformaciones y complejidades.	Emplee principios, normas y reglas teórico/prácticos con herramientas tecnológicas	Evalúa las diferentes tecnologías utilizadas para la encriptación de la información en la red; aplica técnicas de hacking utilizadas por intrusos maliciosos para ejecutar mecanismos de control que previenen ataques informáticos.	Habilidades.
Conformar equipos de trabajo que permitan reconocer los elementos adecuados para establecer políticas y mecanismo de seguridad acordes al negocio.	Utiliza recursos de comunicación y TIC para ampliar las fuentes de información relevantes, desarrollando la capacidad de indagación y exploración, así como de trasfencia de conocimiento y conectividad de su praxis profesional.	Se comprometa con al aprendizaje continuo y el conocimiento de temas contemporáneos de manera autónoma de acuerdo con las necesidades actuales del entorno.	Analiza problemas de seguridad que permiten encontrar soluciones efectivas y eficientes, así como implementar políticas de seguridad que garanticen el uso correcto de los recursos.	Valores y actitudes.



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

**D: UNIDADES TEMÁTICAS O DE ANÁLISIS:**

D: UNIDADES TEMÁTICAS O DE ANÁLISIS:							
Unidad #: <u>1</u>		Descripción: FUNDAMENTOS DE CIBERSEGURIDAD					
Objetivo: Caracterizar los conceptos teóricos de la ciberseguridad mediante la articulación de terminologías que forman el ecosistema de la seguridad de la información, estudiando las técnicas de los principales ataques de ciberseguridad.							
Contenidos: conocimientos a desarrollar.	Métodos, técnicas e instrumentos en función de las actividades de organización del aprendizaje.				Tiempo de aprendizaje.	Escenarios en función de los ambientes de aprendizaje.	Recursos didácticos.
	Componente de docencia.		Componente de prácticas de aplicación y experimentación de los aprendizajes.	Componente de aprendizaje autónomo.			
	Actividades de aprendizaje asistido por el profesor.	Actividades de aprendizaje colaborativo.					
1.1. Ciberseguridad 1.1.1. Conceptos fundamentales de la ciberseguridad. 1.1.2. Características de la Ciberseguridad: Integridad, confidencialidad y Disponibilidad. 1.1.3. Seguridad Física y Lógica 1.1.4. Conceptos de Amenaza, Vulnerabilidad, Riesgo e Impacto 1.2. Ciberdelincuencia 1.2.1. Tipos de Amenazas 1.2.2. Ataques Informáticos 1.2.3. Delitos Informáticos	Clases Online - teórico prácticas	Completar desarrollo de ejercicios o Resolución de problemas.	Desarrollo de ejercicios o resolución de problemas (grupal o individual).  Defensa y/o Exposición de Proyectos (grupal o individual).	Revisión y análisis de videos.  Desarrollo de Ejercicios o Resolución de problemas.  Repaso de contenidos	6(S) + 6 (S) +24 (A) = 36 horas	Aula Virtual	Plataformas virtuales (Entornos de aprendizaje virtual) – Moodle.  Chat  Software virtual para trabajo colaborativo.  Videos tutoriales.  Bibliotecas virtuales



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

**D: UNIDADES TEMÁTICAS O DE ANÁLISIS:**

D: UNIDADES TEMÁTICAS O DE ANÁLISIS:							
Unidad #: <u>  2  </u>		Descripción: SEGURIDAD EN LA CONECTIVIDAD Y SISTEMAS					
Objetivo: Evaluar las diferentes técnicas de protección usando dispositivos de red y mejorando las configuraciones de los sistemas operativos y endureciendo la seguridad sobre los servicios brindados.							
Contenidos: conocimientos a desarrollar.	Métodos, técnicas e instrumentos en función de las actividades de organización del aprendizaje.				Tiempo de aprendizaje.	Escenarios en función de los ambientes de aprendizaje.	Recursos didácticos.
	Componente de docencia.		Componente de prácticas de aplicación y experimentación de los aprendizajes.	Componente de aprendizaje autónomo.			
	Actividades de aprendizaje asistido por el profesor.	Actividades de aprendizaje colaborativo.					
2.1. Seguridad en la conectividad 2.1.1. Arquitecturas de red: Tipos de Redes 2.1.2. Interfaces, Protocolos y Servicios de Red 2.1.3. Control de acceso a las redes 2.1.4. Defensa de Red 2.1.5. Seguridad en Firewalls y equipos de conectividad 2.2. Seguridad en los sistemas y aplicaciones. 2.2.1. Hardening 2.2.2. Seguridad en aplicaciones y Seguridad en móviles 2.2.3. Seguridad en la nube 2.2.4. Seguridad en los Sistemas operativos	Clases Online - teórico prácticas	Completar desarrollo de ejercicios o Resolución de problemas.	Desarrollo de ejercicios o resolución de problemas (grupal o individual).  Defensa y/o Exposición de Proyectos (grupal o individual).	Revisión y análisis de videos.  Desarrollo de Ejercicios o Resolución de problemas.  Repaso de contenidos	6(S) + 6 (S) +24 (A) = 36 horas	Aula Virtual	Plataformas virtuales (Entornos de aprendizaje virtual) – Moodle.  Chat  Software virtual para trabajo colaborativo.  Videos tutoriales.  Bibliotecas virtuales



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

**D: UNIDADES TEMÁTICAS O DE ANÁLISIS:**

D: UNIDADES TEMÁTICAS O DE ANÁLISIS:							
Unidad #: <u>3</u>		Descripción: SEGURIDAD EN DATOS Y SOFTWARE					
Objetivo: Evaluar los diferentes mecanismos para asegurar los datos y proteger la información incluyendo los sistemas a usarse con el fin de salvaguardar y proteger la información transmitida a través de los sistemas, ya sea en ambientes cliente servidor como en entornos web.							
Contenidos: conocimientos a desarrollar.	Métodos, técnicas e instrumentos en función de las actividades de organización del aprendizaje.				Tiempo de aprendizaje.	Escenarios en función de los ambientes de aprendizaje.	Recursos didácticos.
	Componente de docencia.		Componente de prácticas de aplicación y experimentación de los aprendizajes.	Componente de aprendizaje autónomo.			
	Actividades de aprendizaje asistido por el profesor.	Actividades de aprendizaje colaborativo.					
3.1. Seguridad en Datos 3.1.1. Fundamentos de Criptografía 3.1.2. Integridad de Datos 3.1.3. Privacidad de Datos 3.1.4. Seguridad en las Bases de Datos 3.1.5. Seguridad en el almacenamiento de la Información 3.1.6. Fundamentos de Forensia Digital 3.2. Seguridad en el Software 3.2.1. Desarrollo de software seguro 3.2.2. OWASP: Open Web Application Security Project	Clases Online - teórico prácticas	Completar desarrollo de ejercicios o Resolución de problemas.	Desarrollo de ejercicios o resolución de problemas (grupal o individual).  Defensa y/o Exposición de Proyectos (grupal o individual).	Revisión y análisis de videos.  Desarrollo de Ejercicios o Resolución de problemas.  Repaso de contenidos	6(S) + 6 (S) +24 (A) = 36 horas	Aula Virtual	Plataformas virtuales (Entornos de aprendizaje virtual) – Moodle.  Chat  Software virtual para trabajo colaborativo.  Videos tutoriales.  Bibliotecas virtuales



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

**D: UNIDADES TEMÁTICAS O DE ANÁLISIS:**

D: UNIDADES TEMÁTICAS O DE ANÁLISIS:							
Unidad #: <u>4</u>		Descripción: SEGURIDAD EN LAS ORGANIZACIONES					
Objetivo: Revisar la Ciberseguridad en las organizaciones, su aplicación, las normas y entidades certificadoras internacionales para una formación formal.							
Contenidos: conocimientos a desarrollar.	Métodos, técnicas e instrumentos en función de las actividades de organización del aprendizaje.				Tiempo de aprendizaje.	Escenarios en función de los ambientes de aprendizaje.	Recursos didácticos.
	Componente de docencia.		Componente de prácticas de aplicación y experimentación de los aprendizajes.	Componente de aprendizaje autónomo.			
	Actividades de aprendizaje asistido por el profesor.	Actividades de aprendizaje colaborativo.					
4.1.1. Políticas y Gobierno de la Seguridad 4.1.2. Ethical Hacking 4.1.3. Normas Internacionales de Seguridad de la Información 4.2.1. Áreas de Aplicación 4.2.2. Entrenamiento y Certificaciones	Clases Online - teórico prácticas	Completar desarrollo de ejercicios o Resolución de problemas.	Desarrollo de ejercicios o resolución de problemas (grupal o individual).  Defensa y/o Exposición de Proyectos (grupal o individual).	Revisión y análisis de videos.  Desarrollo de Ejercicios o Resolución de problemas.  Repaso de contenidos	6(S) + 6 (S) +24 (A) = 36 horas	Aula Virtual	Plataformas virtuales (Entornos de aprendizaje virtual) – Moodle.  Chat  Software virtual para trabajo colaborativo.  Videos tutoriales.  Bibliotecas virtuales



**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

<b>E: EVALUACIÓN DE LOS APRENDIZAJES.</b>			
Sistema de evaluación de los aprendizajes en función de:		Actividades.	
Gestión formativa.	60 %	a) Trabajo participativo en clase, b) Reportes de talleres y equipos colaborativos, c) Controles de lectura, d) Exposición de casos y situaciones. e) Otros: (Detallar) Lección Online_____	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>
Gestión práctica y autónoma.		a) Demostración de uso directo de los acervos bibliotecarios o en red, b) Trabajo de laboratorio, talleres, seminarios, c) Ejercicios orales y escritos de técnica jurídica, d) Prácticas diversas, incluyendo la de los laboratorios, e) Trabajos de campo, f) Trabajos individuales de lectura, análisis y aplicación, g) Uso creativo y orientado de nuevas TICs y la multimedia, h) Lectura crítica y análisis comparado de casos, i) Asistencia y reporte de eventos académicos. j) Otros: (Detallar) Deberes, Proyecto	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>





**UNIVERSIDAD DE GUAYAQUIL**  
**VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL**

Acreditación y validación.	40 %	a) Exámenes orales y escritos teóricos, b) Exámenes orales y escritos prácticos, c) Sustentación de proyectos de investigación y casos prácticos. d) Otros: (Detallar) <u>Examen Online</u>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>
----------------------------	------	--	---

F: BIBLIOGRAFÍA				
BÁSICA	No	Título de la obra.	Existencia en biblioteca.	Número de ejemplares.
	1	CIBERSEGURIDAD: UN ENFOQUE DESDE LA CIENCIA DE DATOS <a href="https://elibro.net/es/ereader/uguayaquil/120435?page=1">https://elibro.net/es/ereader/uguayaquil/120435?page=1</a>	Sí	Biblioteca online
	2	SALVAGUARDA Y SEGURIDAD DE LOS DATOS: ADMINISTRACIÓN DE BASES DE DATOS <a href="https://elibro.net/es/ereader/uguayaquil/44140?page=1">https://elibro.net/es/ereader/uguayaquil/44140?page=1</a>	Sí	Biblioteca online
	3	Big data: para seguridad privada <a href="https://elibro.net/es/ereader/uguayaquil/118591?page=1">https://elibro.net/es/ereader/uguayaquil/118591?page=1</a>	Si	Biblioteca online
	4			
COMPLEMENTARIA	1	El Arte de la Intrusión: La Verdadera Historia de las Hazañas de Hackers, Intrusos e Impostores. Autores: Mitnick, Kevin D.; Simon, William L. 2007	Sí	1
	2	Hacking y Seguridad en Internet. Autores Picouto Ramos, Fernando; Lorente Pérez, Iñaki (et...al). 2008	No	0
	3		No	0
	4			
SITIOS WEB	No	Dirección electrónica / URL		
	1	El Instituto SANS URL: <a href="http://www.sans.org">http://www.sans.org</a> .		
	2	Graham, Robert. "FAQ: Network Intrusion Detection Systems." Version 0.8.3. 21 March 2000. URL: <a href="http://www.ticm.com/kb/faq/idsfaq.html">http://www.ticm.com/kb/faq/idsfaq.html</a> (3 March 2013).		



UNIVERSIDAD DE GUAYAQUIL  
VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL

	3	CISSP Certified Information Systems, Security Professional Study Guide
	4	Claudio Hernández, (2001) "Hackers – Los piratas del Chip"



UNIVERSIDAD DE GUAYAQUIL  
VICERRECTORADO DE FORMACIÓN ACADÉMICA Y PROFESIONAL

G: FIRMAS DE RESPONSABILIDAD			
Responsabilidad.	Nombre del responsable.	Firma.	Fecha entrega.
Elaborado por:			
Revisado por:	LSI. Angel Veloz Rodríguez, Mgs.		14/05/2021
	Ing. Verónica Mendoza Morán. M.Sc.		14/05/2021
Aprobado por:	Ing. Lorenzo Cevallos Torres. Mgs.		14/05/2021
Secretaría de la carrera:	Ab. Juan Chávez Atocha.		14/05/2021