FACULTAD:	**FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES**
CARRERA:	**COMPUTACION**
MODALIDAD:	**PRESENCIAL**
CICLO:	**7**
PERÍODO ACADÉMICO ORDINARIO:	**Pregrado: período académico octubre 2023-marzo 2024 modalidad presencial. Régimen 2019**

SÍLABO DE LA ASIGNATURA

Seguridad de la Información

Responsable: Narvaez Guillen Cristian Ramiro

Correo electrónico: cristian.narvaez@unl.edu.ec

Dependencia para tutoría: Dependencia Física: Bloque 8 - Aula A821 Dependencia Virtual: (Zoom ID: 932 386 2087).

2023

1. DATOS GENERALES DE LA ASIGNATURA

1.1. DENOMINACIÓN DE LA ASIGNATURA: Seguridad de la Información

1.2. CÓDIGO DE LA ASIGNATURA: INSTITUCIONAL: E2C7A8 - UNESCO: 1203.99

1.3. UNIDAD DE ORGANIZACIÓN CURRICULAR: Unidad profesional

1.4. NÚMERO DE HORAS: 120

COMPONENTE DE APRENDIZAJE	NRO. HORAS SEMANALES	NRO. HORAS AL PERÍODO ACADÉMICO ORDINARIO
APRENDIZAJE EN CONTACTO CON EL DOCENTE	3,0	48
APRENDIZAJE PRÁCTICO EXPERIMENTAL	1,0	16
APRENDIZAJE AUTÓNOMO	3,5	56
TOTAL	**7,5**	**120**
NRO. TOTAL DE HORAS DE PRÁCTICAS PREPROFESIONALES / VINCULACIÓN CON LA SOCIEDAD	NO APLICA	NO APLICA

1.5. REQUERIMIENTOS:

1.5.1. PRERREQUISITOS:

CÓDIGO INSTITUCIONAL	CÓDIGO UNESCO	NOMBRE DE LA ASIGNATURA
E2C4A4	1203.11	Sistemas Operativos
E2C6A5	1203.99	Gestión de Redes y Comunicaciones

1.5.2. CORREQUISITOS:

CÓDIGO INSTITUCIONAL	CÓDIGO UNESCO	NOMBRE DE LA ASIGNATURA
NO APLICA		

2. DATOS ESPECÍFICOS DE LA ASIGNATURA

2.1. PROPÓSITO DE LA ASIGNATURA:

El propósito de la asignatura de Seguridad de la Información, es desarrollar en el estudiante la capacidad de describir y comprender conceptos, técnicas y controles relacionados a la seguridad de la información, así como los pilares de la seguridad de la información confidencialidad, integridad y disponibilidad de la información así como la correcta empleo controles y actividades para la mitigación de riesgos asociados al uso de las nuevas tecnologías de la Información.

2.2. CONTRIBUCIÓN DE LA ASIGNATURA AL LOGRO DE LOS RESULTADOS DE APRENDIZAJE DEL PERFIL DE EGRESO:

Esta asignatura adquiere una importancia dentro del plan curricular, ya que brinda un sólido respaldo, bases y experiencia necesaria para llevar a cabo el proceso de definir, estrategias mediante estándares y normas de seguridad, arquitecturas de seguridad lógica y física que creará salvaguardas tanto para el software y la infraestructura crítica de una organización.

La evaluación de las competencias se llevará a cabo de manera continua, formativa y sumativa, utilizando técnicas e instrumentos que se adapten a los procesos de enseñanza-

aprendizaje contemporáneos. Desarrollando con proyectos tecnológicos innovadores para la resolución de problemas y optimización de procesos en servicio de la sociedad, basados en la metodología de la investigación en computación, proyectos tecnológicos, seguridad de la información, utilizando técnicas y herramientas actuales necesarias para la práctica de la computación e investigación científica/tecnológica. Esto implica que los profesionales formados en esta asignatura sean capaces de ofrecer soluciones de seguridad eficientes a los problemas prácticos de la sociedad, basándose en las necesidades del sector local.

Con el fin de lograr dicho perfil de egreso, La evaluación de las competencias se realizará de manera continua, formativa y sumativa, utilizando técnicas e instrumentos que se ajusten a los procesos de enseñanza-aprendizaje actuales. Esto permitirá aportar al perfil de egreso deseado, capacitando a los estudiantes para ofrecer soluciones efectivas a los desafíos del sector productivo en el campo de la seguridad del software.

3. ESTRUCTURA Y DESARROLLO DE LA ASIGNATURA

3.1. CONTENIDOS Y ACTIVIDADES DE APRENDIZAJE POR UNIDAD:

NÚMERO DE LA UNIDAD:	NOMBRE DE LA UNIDAD:	DURACIÓN DE LA UNIDAD:	
		SEMANAS	HORAS
1	Gestión de la seguridad de la información, riesgos y gobernanza	5	37,5
RESULTADOS DE APRENDIZAJE DE LA UNIDAD	R1. Analiza las ventajas y desventajas de equilibrio de las propiedades clave de seguridad, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad		

CONTENIDOS TEÓRICOS	ACTIVIDADES DE APRENDIZAJE					
	Aprendizaje en contacto con el docente (ACD)	NRO. HORAS	Aprendizaje práctico experimental (APE)	NRO. HORAS	Aprendizaje autónomo (AA)	NRO. HORAS
Principios de la Seguridad de la Información.	Comprendiedo la Seguridad de la Información. Importancia en la Seguridad de la información. Seguridad de la información en la actualidad. Los tres pilares de la Seguridad de la Información. Principios de la Seguridad de la Información.	4,0	Taller 01. Taller sobre los principales conceptos de información y ciberseguridad.	1,0	- Mapa Mental Cap. 01 "Introduction to Information and Cybersecurity / Libro: Information Security Management"	3,5
Tipos de Amenazas en Organización	Introducción a las Amenazas. Amenazas Internas (insiders). Amenazas Externas (outsiders). Activos. Vulnerabilidades. Definición de impacto. Riesgo.	2,0	Taller 02. Análisis de amenazas internas y externas en una organización.	1,0	Mapa Mental: Amenazas Internas - Externas. - Mapa Mental Cap. 02 Libro: Information Security Management"	3,5
Arquitecturas de Seguridad.	Capas Primarias de la Seguridad de la Información. Situaciones que comprometen la Seguridad de la Información. Marcos de seguridad de la información y arquitectura de seguridad de la información. Modelo de Defensa en Profundidad. Seguridad por niveles. El ciclo de implantación de la seguridad de la información.	4,0	Taller 03. Tema: "Fortaleciendo las Capas Primarias de la Seguridad de la Información"	2,0	Ensayo: Modelos de Defensa en Profundidad. Ensayo: Seguridad por Niveles.	7,0
Protección de una Organización.	Gestión de Riesgos de Seguridad y Controles. Evaluación de riesgos y amenazas. Análisis de vulnerabilidades y amenazas. Normas y estándares de Seguridad de la Información. Estándares de Calidad.. ISO 27001. – NIST 800-39 – NIST 800-53 Metodología P.D.C.A.	4,0	Taller 04: Tema: "Gestión de Riesgos con MAGERIT e Implementación de ISO 27001/NIST 800-39 / NIST 800-53"	2,0	Ensayo: Metodología de Análisis de Riesgos (Magerit). Ensayo: Metodología PDCA.	3,5
TOTAL DE HORAS		**14.0**		**6.0**		**17.5**
ESTRATEGIAS DE EVALUACIÓN:	Aprendizaje en contacto con el docente (20%): -Control de lectura de temas investigados, lecciones sobre la temática abordada. Aprendizaje práctico experimental (20%): -Talleres prácticos / Casos de Estudio / otros.					

	Aprendizaje autónomo (25%): -Ensayos / Foros / Mapas mentales / Proyecto Integrador de Saberes / otros. Evaluación sumativa de Unidad (35%): -Evaluación de fin de unidad didáctica: Al término de la unidad, se tomará un examen integral (teórico - práctico) de los conocimientos adquiridos.
ESCENARIOS DE APRENDIZAJE:	Aula física: A324. Virtual (Zoom ID: 932 386 2087). Sílabo. Entorno virtual de aprendizaje EVA. ISO 27000 NIST (800) Magerit.
APORTE DE LA ASIGNATURA AL PROYECTO INTEGRADOR DE SABERES:	El aporte de la asignatura de "Seguridad de la información" al proyecto integrador de saberes de la carrera de computación ya que permitirá desarrollar proyectos de tecnológicos, seguros y confiables mediante la implementación de las mejores prácticas y estándares en el campo de la seguridad de la información, además estar preparados para enfrentar los desafíos en el Trabajo de Integración Curricular (T.I.C) que se presentará al finalizar el ciclo.

NÚMERO DE LA UNIDAD:	**NOMBRE DE LA UNIDAD:**	**DURACIÓN DE LA UNIDAD:**	
		SEMANAS	**HORAS**
2	Criptografía computacional	6	45,0
RESULTADOS DE APRENDIZAJE DE LA UNIDAD	R2. Explica los conceptos de autenticación, autorización, control de acceso, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad.		

CONTENIDOS TEÓRICOS	**ACTIVIDADES DE APRENDIZAJE**					
	Aprendizaje en contacto con el docente (ACD)	**NRO. HORAS**	**Aprendizaje práctico experimental (APE)**	**NRO. HORAS**	**Aprendizaje autónomo (AA)**	**NRO. HORAS**
Criptografía	Introducción a la criptografía: - Definición y objetivos de la criptografía. - Historia de la criptografía y su evolución a lo largo del tiempo. - Importancia de la criptografía en la seguridad de la información. Criptografía simétrica: - Concepto de criptografía simétrica y su funcionamiento. - Algoritmos de cifrado simétrico, como AES (Advanced Encryption Standard) y DES (Data Encryption Standard). - Modos de operación en criptografía simétrica, como ECB (Electronic Codebook), CBC (Cipher Block Chaining) y CTR (Counter). Criptografía asimétrica: -Concepto de criptografía asimétrica y su funcionamiento. -Algoritmos de cifrado asimétrico, como RSA (Rivest-Shamir-Adleman).	6,0	Taller 05: Tema: "Cryptohack – Creación de cuenta. (Cifrado Cesar)"	1,0	Mapa Mental Cap. 10. Libro: Information Security Management". Ensayo: Criptografía Simétrica. Ensayo: Criptografía Asimétrica.	7,0
Criptoanálisis	Introducción al criptoanálisis: -Definición y objetivos del criptoanálisis. -Relación entre criptografía y criptoanálisis. Tipos de ataques criptoanalíticos. -Ataques de fuerza bruta. -Búsqueda exhaustiva: Criptoanálisis de cifrado simétrico: -Ataques de confusión y sustitución AES. -Ataques de cifrado por bloques y cifrado de flujo. Criptoanálisis de cifrado asimétrico: -Ataques de factorización y logaritmo discreto. -Ataques de texto claro elegido y texto cifrado elegido.	6,0	Taller 06: Reto Cryptohack (https://cryptohack.org) Algoritmos Simétricos – Algoritmos Asimétricos.	2,0	Ensayo: Ataque utilizados en retos criptografía Simétrica. Ensayo: Ataque utilizados en retos criptografía RSA.	7,0
Criptografía Moderna	Protocolos de intercambio de claves, como Diffie-Hellman. Protocolos de autenticación, como HMAC (Hash-based Message Authentication Code). Criptografía de curva elíptica. Funciones Digestivas.	3,0	Taller 07: Reto Cryptohack (https://cryptohack.org) Algoritmos Diffie-Hellman.– Funciones HASH.	1,0	Ensayo: Ataque utilizados en retos Diffie-Hellman Ensayo: Curvas Elípticas..	3,5
Firma electrónica	Protocolos de autenticación, como HMAC (Hash-based Message Authentication Code). Digital Signatures.	4,0	Taller 09. Implementación Ransonware mediante la aplicación de criptografía.	1,0	Ensayo: Digital Signature. Foro: Criptografía Aplicada. Exposición: HMAC.	3,5
TOTAL DE HORAS		**19.0**		**5.0**		**21.0**
ESTRATEGIAS DE EVALUACIÓN:	Aprendizaje en contacto con el docente (20%): -Control de lectura de temas investigados, lecciones sobre la temática abordada. Aprendizaje práctico experimental (20%): -Talleres prácticos / Casos de Estudio / otros. Aprendizaje autónomo (25%):					

	-Ensayos / Foros / Mapas mentales / Proyecto Integrador de Saberes / otros. Evaluación sumativa de Unidad (35%): -Evaluación de fin de unidad didáctica: Al término de la unidad, se tomará un examen integral (teórico - práctico) de los conocimientos adquiridos.
ESCENARIOS DE APRENDIZAJE:	Aula física: A324. Virtual (Zoom ID: 932 386 2087). Sílabo. Entorno virtual de aprendizaje EVA. Criptohack. Python - Colab. Notas.
APORTE DE LA ASIGNATURA AL PROYECTO INTEGRADOR DE SABERES:	El aporte de la asignatura de "Seguridad de la información" al proyecto integrador de saberes de la carrera de computación ya que permitirá desarrollar proyectos de tecnología, seguros y confiables mediante la implementación de las mejores prácticas y estándares en el campo de la seguridad de la información, además estar preparados para enfrentar los desafíos en el Trabajo de Integración Curricular (T.I.C) que se presentará al finalizar el ciclo.

NÚMERO DE LA UNIDAD:	**NOMBRE DE LA UNIDAD:**	**DURACIÓN DE LA UNIDAD:**	
		SEMANAS	**HORAS**
3	Seguridad de la información operativa.	5	37,5
RESULTADOS DE APRENDIZAJE DE LA UNIDAD	R3. Describe cuestiones éticas importantes a considerar en la seguridad informática, incluyendo cuestiones éticas asociadas a fijar o no fijar vulnerabilidades y revelar o no revelar vulnerabilidades, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad		

CONTENIDOS TEÓRICOS	**ACTIVIDADES DE APRENDIZAJE**					
	Aprendizaje en contacto con el docente (ACD)	**NRO. HORAS**	**Aprendizaje práctico experimental (APE)**	**NRO. HORAS**	**Aprendizaje autónomo (AA)**	**NRO. HORAS**
Integridad de Datos.	Protección de Datos de carácter Personal. Normas y Principios obligaciones legales en materia de privacidad. Responsables del tratamiento. Mejores prácticas en la protección de datos personales.	3,0	Taller 10: "Diseño de políticas y procedimientos de protección de datos"	1,0	- Mapa Mental Cap. 03 Libro: Information Security Management". - Ensayo: Ley de Protección de Datos Personales (Ecuador).	3,5
Diseño de sistemas de información seguros	Mejores prácticas para evaluar y mitigar las vulnerabilidades. -Nivel de Hardware. -Nivel de Software. -Nivel de Red. Buenas prácticas en el diseño de sistemas de información seguros. -Controles conocidos y sus mitigaciones. -Consideraciones en dispositivos alternativos.	6,0	Taller 10: "Diseño de políticas y procedimientos de protección de datos"	2,0	- Mapa Mental Cap. 04 Libro: Information Security Management" - Mapa Mental Cap. 05 Libro: Information Security Management"	7,0
Diseño y protección de la seguridad de las redes	Diseño Seguro de Arquitectura de Redes. Estrategias para el aseguramiento de Redes. Plan de Continuidad de Operaciones. (BCP) Plan de Recuperación ante Desastres. (DRP)	3,0	Taller 11: What Went Wrong? (Resolución cuestionario del Libro Pag. 247.)	1,0	Ensayo: Plan de Continuidad de Operaciones. (BCP) Ensayo: Plan de Recuperación ante Desastres. (DRP)	3,5
Controles acceso y gestión de la Identidad	Modelos de Control de Acceso, Mecanismos de Autenticación y Autorización. Manejo de Identidades (IAM). Control de acceso físico a los activos.	3,0	Taller 11: What Went Wrong? (Resolución cuestionario del Libro Pag. 247.)	1,0	Ensayo: Manejo de Identidades (IAM) en la Nube.	3,5
TOTAL DE HORAS		**15.0**		**5.0**		**17.5**
ESTRATEGIAS DE EVALUACIÓN:	Aprendizaje en contacto con el docente (20%): -Control de lectura de temas investigados, lecciones sobre la temática abordada. Aprendizaje práctico experimental (20%): -Talleres prácticos / Casos de Estudio / otros. Aprendizaje autónomo (25%): -Ensayos / Foros / Mapas mentales / Proyecto Integrador de Saberes / otros. Evaluación sumativa de Unidad (35%): -Evaluación de fin de unidad didáctica: Al término de la unidad, se tomará un examen integral (teórico - práctico) de los conocimientos adquiridos.					
ESCENARIOS DE APRENDIZAJE:	Aula física: A324. Virtual (Zoom ID: 932 386 2087). Sílabo. Entorno virtual de aprendizaje EVA. ISO 27000 NIST (800) Magerit.					

APORTE DE LA ASIGNATURA AL PROYECTO INTEGRADOR DE SABERES:	El aporte de la asignatura de "Seguridad de la información" al proyecto integrador de saberes de la carrera de computación ya que permitirá desarrollar proyectos de tecnológicos, seguros y confiables mediante la implementación de las mejores prácticas y estándares en el campo de la seguridad de la información, además estar preparados para enfrentar los desafíos en el Trabajo de Integración Curricular (T.I.C) que se presentará al finalizar el ciclo.

3.2. ACTITUDES Y VALORES QUE SE DESARROLLAN Y/O FORTALECEN:

- Honestidad.- Al proceder con rectitud, disciplina, honradez y mística en el cumplimiento de sus obligaciones en todos los procesos institucionales, relaciones interinstitucionales y personales, como valores esenciales para la convivencia organizada confiable y segura a lo interno y externo de la universidad.
- Transparencia.- Al demostrar íntegramente sus conocimientos, actuar con idoneidad y efectividad en el marco de principios éticos y morales de la convivencia institucional y social.
- Creatividad e innovación
- Socialización del conocimiento.- aplicando aprendizaje continuo, equilibrado democrático y colaborador.

3.3. ESTRATEGIAS METODOLÓGICAS:

Se implementarán metodologías que promuevan la participación e involucramiento directo del estudiante en la construcción del aprendizaje. Para ello, se seleccionarán, adaptarán y aplicarán estrategias metodológicas apropiadas en cada uno de los componentes de aprendizaje.
A continuación, se detallan algunas de las estrategias que se utilizarán:
Aprendizaje en Contacto con el Docente: • Conferencias Magistrales
• Cátedra Compartida • Lectura Centrada en las Ideas y Conceptos Fundamentales
• Conversatorios
• Trabajo o Dinámica Grupal (Game Thinking)
• Pensamiento Visual (Visual Thinking)
• Presentación y/o Exposición de Casos
• Foros
• Laboratorios.
Aprendizaje Autónomo:
• Aprendizaje por Descubrimiento
• Conversatorios Virtuales
• Foros Virtuales
Aprendizaje Práctico-Experimental:
• Prácticas de Laboratorio
• Casos de Estudio.
Evaluación Sumativa:
• Evaluaciones Teóricas/Prácticas
Se empleará el aprendizaje sensorial (multimedia) y aprendizaje concreto.

3.4. RECURSOS Y MATERIALES DIDÁCTICOS:

Entorno virtual de aprendizaje UNL (EVA)
Servicios de aprendizaje virtual en seguridad (Cryptohack - HacR0ck).
ISO 27001 - NIST - Magerit.
Libros digitales.

3.5. TIPO DE APRENDIZAJE QUE SE DESARROLLA:

Aprendizaje en contacto con el docente	(X)	Aprendizaje práctico experimental	(X)	Aprendizaje autónomo	(X)

4. HORARIO DE CLASE DE LA ASIGNATURA

DÍA / HORA	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
07:30:00-08:30:00		X		X			
08:30:00-09:30:00		X		X			

5. CRITERIOS DE EVALUACIÓN DE LA ASIGNATURA

	EVALUACIÓN 1		EVALUACIÓN 2		EVALUACIÓN 3	
COMPONENTE A SER EVALUADO	**INSTRUMENTOS DE EVALUACIÓN**	**PONDERACIÓN (%-PUNTOS)**	**INSTRUMENTOS DE EVALUACIÓN**	**PONDERACIÓN (%-PUNTOS)**	**INSTRUMENTOS DE EVALUACIÓN**	**PONDERACIÓN (%-PUNTOS)**
Aprendizaje en contacto con el docente	Lecciones (orales o escritas) Controles de lectura Exposición de temas	20 % - 2,0	Lecciones (orales o escritas) Controles de lectura Exposición de temas	20 % - 2,0	Lecciones (orales o escritas) Controles de lectura Exposición de temas	20 % - 2,0
Aprendizaje práctico experimental	Resolución de ejercicios Talleres Estudios de caso	25 % - 2,5	Resolución de ejercicios Talleres Estudios de caso	25 % - 2,5	Resolución de ejercicios Talleres Estudios de caso	25 % - 2,5
Aprendizaje autónomo	Productos académicos que elabora el estudiante, de modo individual y grupal	20 % - 2,0	Productos académicos que elabora el estudiante, de modo individual y grupal	20 % - 2,0	Productos académicos que elabora el estudiante, de modo individual y grupal	20 % - 2,0
Evaluación sumativa	Evaluación de fin de unidad didáctica o tema de estudio (teórica, práctica o teórico-práctica)	35 % - 3,5	Evaluación de fin de unidad didáctica o tema de estudio (teórica, práctica o teórico-práctica)	35 % - 3,5	Evaluación de fin de unidad didáctica o tema de estudio (teórica, práctica o teórico-práctica)	35 % - 3,5
TOTAL:		100 %		100 %		100 %

NOTA:

- **CALIFICACIÓN FINAL DE LA ASIGNATURA:** conforme a las **"DIRECTRICES INSTITUCIONALES PARA LA PLANIFICACIÓN ACADÉMICA Y DE CARGA HORARIA DE LOS DOCENTES DE LA UNIVERSIDAD NACIONAL DE LOJA"**, en su **Anexo 3** sección **"4.6. PROCEDIMIENTOS PARA LA EVALUACIÓN DE LOS RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA"** manifiesta que: "... la calificación final de la asignatura **resulta del promedio de las calificaciones** de cada una de las unidades". **(Ver directrices de planificación)**
- **EVALUACIÓN DE RECUPERACIÓN:** conforme los **"LINEAMIENTOS GENERALES PARA LA APLICACIÓN DE LA PRUEBA DE RECUPERACIÓN...."** en sus **Puntos 2.1 a 2.4** manifiesta que: "Se aplicará la evaluación ... a los estudiantes que hayan reprobado **menos del 20% del total de ... horas**", "... rendirán **una sóla evaluación de recuperación** en la o las asignaturas en las que no ha alcanzado la noma mínima ... (7/10 puntos)", "La evaluación de recuperación **será calificada con el 60% y será sumada al 40% de la calificación lograda por el estudiante en la o las asignaturas reprobadas.** De esto, **la calificación mínima que debe tener el estudiante para acceder a la evaluación de recuperación es de 2,75/10 puntos.**" y "... **no podrá ser aplicada a los estudiantes que reprueben la asignatura por inasistencias o por retirno y, a quienes cursen la o las asignaturas en tercera matrícula.**". **(Ver lineamientos)**

6. BIBLIOGRAFÍA

6.1 BÁSICA:

6.1.1 FÍSICA:

AUTOR	TÍTULO DEL LIBRO	CIUDAD, PAÍS DE PUBLICACIÓN	EDICIÓN	AÑO DE PUBLICACIÓN	EDITORIAL	ISBN
Costas Santos, Jesús.	Seguridad informática.	Bogotá	Primera	2011	Ediciones de la U	9789588675701

AUTOR	TÍTULO DEL LIBRO	CIUDAD, PAÍS DE PUBLICACIÓN	EDICIÓN	AÑO DE PUBLICACIÓN	EDITORIAL	ISBN
Jordi Guijarro Olivares, Joan Caparrós Ramírez, Lorenzo Cubero Luque	DevOps y seguridad cloud	Barcelona, España	Primera Edición	2019	UOC	9788491806240
Nichols, Randall K., Lekkas, Panos C.	Seguridad para comunicaciones inalámbricas: redes, protocolos, criptografía y soluciones.	Madrid	Primera	2003	McGrawHill	8448137825

6.1.2 VIRTUAL:

AUTOR	TÍTULO DEL LIBRO	DIRECCIÓN ELECTRÓNICA	AÑO DE PUBLICACIÓN	EDITORIAL	ISBN
Robert Sloan, Richard Warner	Unauthorized Access : The Crisis in Online Privacy and Security	Acceder a recurso	2014	CRC Press. 2014	9781439830130
Joseph MacMillan	Infosec Strategies and Best Practices	Acceder a recurso	2021	Packt Publishing	978-1-80056-635-4

6.2 COMPLEMENTARIA:

6.2.1 FÍSICA:

AUTOR	TÍTULO DEL LIBRO	CIUDAD, PAÍS DE PUBLICACIÓN	EDICIÓN	AÑO DE PUBLICACIÓN	EDITORIAL	ISBN

6.2.2 VIRTUAL:

AUTOR	TÍTULO DEL LIBRO	DIRECCIÓN ELECTRÓNICA	AÑO DE PUBLICACIÓN	EDITORIAL	ISBN
Choose Your InfoSec Path	Alexander J. Roxon	Acceder a recurso	2021	APRESS	978-1-4842-7036-3
Jason Andress	The basics of information security : understanding the fundamentals of InfoSec in theory and practice	Acceder a recurso	2014	Elsevier	978-0-12-800744-0
Michael Workman	Information Security Management	Acceder a recurso	2023	Jones & Bartlett	9781284211658

6.2.3 RECURSOS DE INTERNET:

AUTOR	TÍTULO	CIUDAD, PAÍS DE PUBLICACIÓN	DIRECCIÓN ELECTRÓNICA	AÑO DE PUBLICACIÓN	ISBN/ISSN

7. PERFIL DEL PROFESOR O PROFESORA DE LA ASIGNATURA

7.1. TÍTULO(S) DE TERCER NIVEL, REGISTRADO EN LA SENESCYT:

INGENIERO EN SISTEMAS

7.2. TÍTULO(S) DE CUARTO NIVEL, REGISTRADO EN LA SENESCYT:

MAGISTER EN TECNOLOGIAS DE LA INFORMACION

7.3. AÑOS DE EXPERIENCIA DOCENTE:

4

7.4. AÑOS DE EXPERIENCIA PROFESIONAL:

3

8. RELACIÓN DE LOS CONTENIDOS CON LOS RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA

CONTENIDOS DE LA ASIGNATURA	CONTRIBUCIÓN	RESULTADOS DE APRENDIZAJE
Unidad 1 - Gestión de la seguridad de la información, riesgos y gobernanza	ALTA	R1. Analiza las ventajas y desventajas de equilibrio de las propiedades clave de seguridad, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad
Unidad 2 - Criptografía computacional	MEDIA	R2. Explica los conceptos de autenticación, autorización, control de acceso, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad.
Unidad 3 - Seguridad de la información operativa.	MEDIA	R3. Describe cuestiones éticas importantes a considerar en la seguridad informática, incluyendo cuestiones éticas asociadas a fijar o no fijar vulnerabilidades y revelar o no revelar vulnerabilidades, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad

9. RELACIÓN DE LOS RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA CON LOS RESULTADOS DE APRENDIZAJE DEL PERFIL DE EGRESO

RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA	CONTRIBUCIÓN	PERFIL DE EGRESO DE LA CARRERA
R3. Describe cuestiones éticas importantes a considerar en la seguridad informática, incluyendo cuestiones éticas asociadas a fijar o no fijar vulnerabilidades y revelar o no revelar vulnerabilidades, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad	ALTA	Analiza, diseña, implementa y evalúa sistemas computacionales, basados en los estándares de los procesos en al área de sistemas inteligentes, ingeniería de software, computación aplicada; que garanticen la elaboración de un producto de calidad que solvente las necesidades de la sociedad, considerando los principios básicos de la ética profesional.
R3. Describe cuestiones éticas importantes a considerar en la seguridad informática, incluyendo cuestiones éticas asociadas a fijar o no fijar vulnerabilidades y revelar o no revelar vulnerabilidades, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad	ALTA	Identifica e interpreta métodos, modelos, técnicas, herramientas, y procesos, a partir del conocimiento de los fundamentos de la lógica, matemáticas, física, ciencias tecnológicas, ciencias económicas, lingüística, ética, investigación científica/tecnológica y del área de sistemas inteligentes, ingeniería de software, computación aplicada; que serán utilizados en los distintos roles bajo los principios estandarizados que sustentan la práctica profesional.
R2. Explica los conceptos de autenticación, autorización, control de acceso, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad.	MEDIA	Incorpora conocimientos diferentes interactuando en grupos multidisciplinares para desarrollar proyectos tecnológicos innovadores basados en la investigación e innovación tecnológica y la comunicación y redacción técnica, priorizando los sectores más vulnerables de la región y del país, fomentando la igualdad, solidaridad y respeto por el entorno.
R1. Analiza las ventajas y desventajas de equilibrio de las propiedades clave de seguridad, bajo los principios de solidaridad, transparencia, responsabilidad y honestidad	ALTA	Integra la conducta ética en el desarrollo del ámbito profesional, basada en valores de solidaridad, transparencia, responsabilidad, honestidad, principios morales y humanísticos, que constituyan en toda instancia los pilares fundamentales de la sociedad

10. ELABORACIÓN Y APROBACIÓN

10.1. PROFESOR RESPONSABLE DE LA ELABORACIÓN DEL SÍLABO:

APELLIDOS Y NOMBRES	FIRMAS	FECHA
Narvaez Guillen Cristian Ramiro	Firmado electrónicamente por: CRISTIAN RAMIRO NARVAEZ GUILLEN	18 de Octubre de 2023

10.2. FECHA DE APROBACIÓN: 20 de Octubre de 2023

10.3. FIRMAS DE APROBACIÓN:

F) ----------

DIRECTOR/A Y/O ENCARGADO/A DE GESTIÓN ACADÉMICA DE LA CARRERA