CURRÍCULO DE LA FIGURA PROFESIONAL "SEGURIDAD INFORMÁTICA"

1. Objetivo general

Desarrollar en los estudiantes las competencias técnicas, éticas y legales necesarias para proteger la información, los sistemas informáticos y las infraestructuras tecnológicas frente amenazas, vulnerabilidades y ataques, promoviendo una cultura de seguridad digital, responsabilidad profesional y mejora continua, en conformidad con la normativa nacional e internacional.

2. Plan de estudios

Total periodos pedagógicos tronco común		**1ro**	**2do**	**3ro**
		19	**19**	**19**
Módulos Genéricos de la Familia Profesional	Fundamentos de las Tecnologías de la Información y la Comunicación	3	2	
	Pensamiento Computacional y Resolución de Problemas	3	3	
	Ética, Legislación y Ciudadanía Digital	2		
Módulos Especialización	Fundamentos de Seguridad Informática	3	2	
	Manejo de incidentes y recuperación informática	4	3	
	Gestión y análisis de Vulnerabilidades		3	5
	Monitoreo de redes y sistemas informáticos		2	3
	Cultura y Conciencia en Ciberseguridad	3	3	4
	Auditorías básicas de seguridad informática			5
Módulo práctico/experimental		3	3	4
Total periodos pedagógicos formación técnica		**21**	**21**	**21**

3. Módulos genéricos

Durante el primer y segundo año de formación, el estudiante desarrolla competencias genéricas vinculadas a la Familia Profesional Tecnologías. Gracias a las características de los módulos trabajados en esta etapa, el estudiante adquiere herramientas que le permiten construir una opinión más informada y tomar decisiones con mayor fundamento. Esto favorece su capacidad para, en caso de que lo desee, transitar entre distintas figuras profesionales dentro de la misma familia, continuar con su trayectoria educativa, insertarse en el mundo laboral o emprender un proyecto propio.

Se estructuran los siguientes módulos genéricos:

- Fundamentos de las Tecnologías de la Información y la Comunicación
- Pensamiento Computacional y Resolución de Problemas
- Ética, Legislación y Ciudadanía Digital

Módulo Genérico Nro. 1	
Nombre del módulo:	Fundamentos de las Tecnologías de la Información y la Comunicación
Nivel:	1ro, 2do
Duración:	200 periodos pedagógicos
Unidad de competencia asociada:	**UC1:** Aplicar fundamentos de tecnologías de la información y la comunicación mediante el análisis de su evolución, la identificación de la arquitectura de hardware, software y principios básicos de electricidad y electrónica, la operación básica de redes y sistemas operativos y, la gestión de información digital, con el fin de resolver requerimientos tecnológicos.
Objetivo del módulo: Desarrollar en el estudiante competencias que analice la evolución de las tecnologías de la información y la comunicación, identifique la arquitectura, el funcionamiento de hardware y software, manipule sistemas de redes y sistemas operativos, organice la información digital, con el fin de resolver de manera efectiva requerimientos en distintos entornos tecnológicos.	
Resultados de Aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1. Analizar la evolución de las tecnologías de la información y la comunicación reconociendo sus hitos históricos, transformaciones tecnológicas y su impacto en los entornos productivos, educativos y sociales. **CE1.1:** Distingue la evolución de las TIC con base en líneas de tiempo o esquemas cronológicos. **CE1.2:** Emplea los avances tecnológicos con sus aplicaciones en distintos sectores de la sociedad. **CE1.3:** Define las generaciones de computadoras y dispositivos en función de su capacidad y arquitectura. **CE1.4:** Argumenta el impacto social, económico y cultural del uso de las TIC, mediante análisis de casos actuales o discusiones dirigidas. **RA.2 Examinar la arquitectura de sistemas informáticos, identificando componentes de hardware, software y su funcionamiento integrado en distintos entornos tecnológicos.** **CE2.1:** Inspecciona los componentes físicos de un sistema informático, clasificándolos según su función principal (entrada, procesamiento, almacenamiento, salida y comunicación). **CE2.2:** Distingue entre software de sistema, de aplicación y de desarrollo, explicando su propósito funcional con ejemplos representativos.	

CE2.3: Elabora esquemas de arquitectura de computadoras donde ubicar los componentes funcionales y describe el flujo básico de información entre ellos.
CE2.4: Determina el tipo de sistema informático (doméstico, industrial, educativo, entre otros) a partir de su estructura y características técnicas, según el contexto de uso.
RA.3 Emplear sistemas operativos y entornos digitales gestionando recursos, configuración inicial y funciones elementales en la administración del sistema.
CE3.1: Ejecuta tareas básicas de administración de archivos y carpetas, diferenciando procedimientos entre sistemas operativos gráficos y basados en línea de comandos.
CE3.2: Identifica parámetros esenciales del sistema operativo como nombre de usuario, configuración de red y capacidad de almacenamiento, utilizando herramientas del entorno.
CE3.3: Aplica funciones básicas de herramientas de mantenimiento del sistema operativo para optimizar su funcionamiento.
CE3.4: Emplea instrucciones en los entornos gráficos o de línea de comandos según el tipo de operación administrativa requerida, justificando su elección.
RA.4. Utiliza los fundamentos básicos de electricidad y electrónica digital para la construcción de circuitos simples.
CE4.1: Examina los principios básicos de electricidad y su relación con el funcionamiento de dispositivos electrónicos utilizados en computación.
CE4.2: Analiza componentes electrónicos digitales y su aplicación en sistemas informáticos.
CE4.3: Establece conocimientos de lógica en la resolución de problemas digitales.
CE4.4: Diseña esquemas y diagramas electrónicos básicos para comprender la estructura de circuitos eléctricos simples.
RA.5 Diseñar redes informáticas comprendiendo su estructura, tipos, dispositivos, protocolos de comunicación y funciones esenciales.
CE5.1: Clasifica elementos físicos y lógicos de una red informática según su función en el sistema.
CE5.2: Diferencia tipos de redes (LAN, WAN, WLAN) en función de su alcance, propósito y características.
CE5.3: Representa dispositivos de red en esquemas funcionales según su rol en la infraestructura.
CE5.4: Elabora cuadros técnicos sobre el funcionamiento de protocolos de comunicación en la transmisión de datos.
RA.6. Gestionar información digital utilizando herramientas tecnológicas mediante la organización, almacenamiento, protección y compartición de datos.
CE6.1: Analiza información digital considerando su tipo, relevancia y nivel de confidencialidad en contextos educativos o profesionales.
CE6.2: Organiza carpetas y archivos con nombres coherentes en soportes físicos y virtuales con base en criterios de estructuración lógica.
CE6.3: Implementa medidas básicas de protección de datos mediante contraseñas, permisos de acceso o cifrado en entornos digitales.
CE6.4: Transfiere información en plataformas colaborativas o servicios en la nube respetando estándares de seguridad y compatibilidad.

Contenidos

Conceptuales	Procedimentales	Actitudinales
Evolución histórica de las Tecnologías de la Información y la Comunicación (TIC). Hitos tecnológicos y generaciones de computadoras. Impacto social, económico y cultural de las TIC. Software libre y software propietario, licenciamiento y pagos. Arquitectura de sistemas informáticos: componentes de hardware y sus funciones. Tipos de software: de sistema, de aplicación y de desarrollo, según su contexto, funciones y características. Estructura funcional de computadoras y flujo de información entre componentes. Clasificación de sistemas informáticos según su contexto de uso. Redes informáticas, elementos físicos y lógicos. Tipos de redes (LAN, WAN, WLAN) y sus características principales. Dispositivos de red y sus funciones (switch, router, módem, punto de acceso, repetidor).	Analizar líneas de tiempo y esquemas cronológicos para identificar hitos y evolución de las TIC. Clasificar dispositivos de hardware y software según su función y tipo. Organizar esquemas y diagramas de arquitectura de sistemas informáticos. Identificar el flujo de información entre componentes de hardware y software. Manipular sistemas operativos para gestionar archivos, carpetas y configuraciones básicas. Configurar parámetros de usuario, red y almacenamiento en sistemas operativos. Aplicar funciones básicas de mantenimiento del sistema operativo. Utilizar entornos gráficos y línea de comandos para tareas de administración. Catalogar y diferenciar elementos físicos y lógicos de redes informáticas. Describir tipos de redes y sus características mediante ejemplos prácticos. Configurar dispositivos de red y simular funciones de	Mostrar responsabilidad y ética en el manejo y protección de la información digital. Valorar la importancia de la evolución tecnológica y su impacto en la sociedad. Desarrollar una actitud crítica y reflexiva ante los cambios y avances en las TIC. Fomentar el interés por el aprendizaje continuo y actualización en tecnologías emergentes. Promover el trabajo colaborativo y la comunicación efectiva en ambientes tecnológicos. Adoptar prácticas de seguridad digital para proteger datos personales y profesionales. Reconocer la importancia del respeto a la privacidad y la confidencialidad en el uso de tecnologías. Desarrollar autonomía en la gestión y solución de problemas tecnológicos básicos. Mantener una postura abierta y flexible ante nuevas metodologías y herramientas tecnológicas. Impulsar la conciencia sobre el impacto ambiental y social del uso responsable de las TIC.

Protocolos de comunicación en redes. Conceptos de gestión, organización, almacenamiento, normas y buenas prácticas en seguridad informática y protección de datos. Herramientas tecnológicas para compartir información en entornos digitales. Fundamentos de trabajo colaborativo y comunicación efectiva en entornos tecnológicos. Organización, planificación y gestión de proyectos tecnológicos. Unidades de medidas de la información. Fundamentos eléctricos y electrónicos: conceptos básicos y práctica con circuitos. Protección eléctrica y puesta a tierra. Componentes eléctricos y electrónicos. Esquemas, diagramas y circuitos electrónicos Lógica digital.	protocolos de comunicación. Organizar, almacenar y proteger información digital mediante herramientas tecnológicas. Implementar medidas básicas de seguridad en entornos digitales (contraseñas, permisos, cifrado). Compartir información en plataformas colaborativas y servicios en la nube, respetando normas de seguridad y formatos. Probar nuevas herramientas tecnológicas y entornos digitales. Diagnosticar y resolver problemas técnicos con actitud analítica y perseverante. Documentar procesos y resultados técnicos de manera clara y ordenada. Utilizar plataformas colaborativas para la gestión del trabajo en equipo. Identificar componentes eléctricos y electrónicos básicos visualmente y por código. Construir circuitos eléctricos básicos en protoboard y simuladores digitales.	Mantener una actitud positiva y resiliente ante fallos y errores técnicos. Fomentar el trabajo en equipo con comunicación abierta, respeto y cooperación. Priorizar la gestión adecuada del tiempo y recursos para cumplir objetivos. Demostrar responsabilidad en el manejo seguro de herramientas e instrumentos eléctricos y electrónicos.
Perfil del o la docente		

- Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines
- Experiencia en el campo amplio de la Educación, debidamente certificada.

Orientaciones Metodológicas

- Aprendizaje Basado en Proyectos (ABP)
- Aprendizaje en Contextos Reales
- Role-Playing y Simulaciones
- Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)

Materiales y recursos

Denominación	Especificaciones técnicas	Cantidad
Infraestructura/espacio	Entorno de aprendizaje (aula)	1
Laboratorio	Computadoras con acceso a internet Proyector	1

Referencias Bibliográficas

Libros:

- García, R., & Pérez, M. (2022). Introducción a las Tecnologías de la Información y la Comunicación: Bases y Aplicaciones. Editorial Alfaomega, México.
- Sánchez, L. (2021). Redes de Computadoras para Principiantes. Editorial McGraw-Hill, España.
- Morales, J. (2020). Fundamentos de Hardware y Software. Editorial Pearson, España.
- Torres, A. (2023). Sistemas Operativos: Principios y Administración. Editorial Marcombo, España.
- Ramírez, C. (2019). Tecnologías de la Información y Comunicación en el Mundo Actual. Editorial Trillas, México.

Sitios Web:

- Ministerio de Educación del Ecuador (2023). Currículo Nacional para el Bachillerato Técnico: Fundamentos de las Tecnologías de la Información y la Comunicación. Quito, Ecuador.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) (2020). Política Nacional de Tecnologías de Información y Comunicación. Quito, Ecuador.
- Educatina. https://educatina.com
- Khan Academy en español. https://es.khanacademy.org
- AulaFacil TIC. https://aulafacil.com/cursos/tecnologia-informacion-comunicacion

Módulo Genérico Nro.2	
Nombre del módulo:	Pensamiento Computacional y Resolución de Problemas
Nivel:	1ro, 2do

Duración:	240 periodos pedagógicos
Unidad de competencia asociada:	**UC2:** Proponer soluciones informáticas y computacionales mediante el análisis lógico-matemático, manejo de sistemas numéricos, lógica de conjuntos, formulación algorítmica con diagramas y pseudocódigo, aplicación de programación básica, levantando documentación técnica, como fundamento del desempeño profesional en tecnologías de la información y comunicación.
Objetivo del módulo: Fortalecer en el estudiante competencias técnicas en la formulación y representación algorítmica, programación básica, aplicando metodologías de desarrollo, conceptos lógicos matemáticos y sistemas numéricos para la resolución de problemas computacionales.	
Resultados de aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1 Aplicar conceptos de lógica matemática, conjuntos y sistemas numéricos en la resolución de problemas computacionales. **CE1.1:** Distingue proposiciones y operaciones lógicas utilizando tablas de verdad y leyes del álgebra booleana. **CE1.2:** Representa operaciones de conjuntos en problemas computacionales mediante diagramas y notación formal. **CE1.3:** Transforma valores entre sistemas numéricos binario, decimal, hexadecimal y octal como base para el tratamiento de datos. **CE1.4:** Resuelve problemas que combinan lógica proposicional y sistemas numéricos en contextos computacionales específicos. **RA.2 Resolver algoritmos de aplicaciones informáticas, representarlos mediante diagramas de flujo y pseudocódigo.** **CE2.1:** Descompone problemas en pasos secuenciales mediante la elaboración de diagramas de flujo estructurados. **CE2.2:** Traduce diagramas de flujo a pseudocódigo utilizando sintaxis estructurada y lógica funcional. **CE2.3:** Verifica algoritmos mediante pruebas y simulaciones, identificando errores de lógica y eficiencia. **CE2.4:** Contrasta resultados esperados y obtenidos para evaluar el comportamiento funcional del algoritmo. **RA.3 Utilizar programación en la construcción de soluciones computacionales.** **CE3.1:** Emplea estructuras secuenciales, condicionales y repetitivas al desarrollar programas en un lenguaje de programación resolviendo problemas computacionales básicos. **CE3.2:** Construye clases, atributos y métodos aplicando principios de encapsulamiento, herencia y polimorfismo en un lenguaje orientado a objetos. **CE3.3**: Elabora estructuras de datos simples como vectores, listas y matrices para la gestión de información en aplicaciones básicas. **CE3.4**: Codifica programas simples verificando la funcionalidad conforme a los requerimientos establecidos y resultados esperados.	

CE3.5: Documenta mediante comentarios técnicos explicando la lógica, estructura y funcionamiento del código fuente.

RA.4 Diseñar interfaces básicas facilitando la interacción con usuarios en aplicaciones de consola y GUI.

CE4.1: Aplica elementos visuales, etiquetas y campos adecuados al tipo de aplicación (consola o GUI) para representar la funcionalidad esperada.

CE4.2: Integra principios de usabilidad y accesibilidad en el diseño de interfaces, considerando la disposición, navegación y comprensión visual

CE4.3: Programa eventos y validaciones que responden correctamente a las acciones del usuario, previniendo errores en tiempo de ejecución.

CE4.4: Realiza pruebas para identificar mejoras en la interacción y funcionalidad de la interfaz desarrollada.

RA.5 Implementar metodologías de desarrollo de software en función del tipo de proyecto, integrando tiempos de entrega y colaboración en equipo.

CE5.1: Selecciona adecuadamente la metodología de desarrollo (ágil, tradicional, híbrida) según los requerimientos del proyecto.

CE5.2: Realiza las tareas de desarrollo de acuerdo con la metodología seleccionada, cumpliendo entregables y estándares.

CE5.3: Coordina la colaboración en equipo utilizando herramientas digitales que facilitan la comunicación y el seguimiento de actividades.

CE5.4: Documenta el proceso de desarrollo mediante registros técnicos que evidencian el avance y la gestión del proyecto.

Contenidos

Conceptuales	**Procedimentales**	**Actitudinales**
Principios del pensamiento computacional. Componentes de un problema computacional. Criterios de optimización en soluciones computacionales. Metodología para la resolución de problemas computacionales. Identificación de patrones y relaciones. Algoritmos, definición y características. Tipos de datos, variables, constantes y expresiones.	Descomponer problemas complejos en subproblemas manejables mediante estrategias de pensamiento lógico. Identificar patrones comunes en distintos problemas para proponer soluciones generalizables. Representar procesos a través de diagramas de flujo, pseudocódigo u otras formas de modelado lógico. Formular algoritmos eficientes considerando secuencia, selección, iteración y modularidad.	Emplear el pensamiento analítico en la resolución de problemas. Mostrar disposición para explorar situaciones problemáticas desde múltiples perspectivas antes de proponer soluciones. Asumir responsabilidad en la coherencia lógica de los diseños propuestos, considerando el contexto del problema. Mostrar flexibilidad para ajustar los modelos diseñados ante nuevas condiciones o sugerencias.

Lenguajes de pseudocódigo y diagramas de flujo. Estructuras de control secuencial, condicional y repetitiva. Tipos de errores, sintácticos, lógicos y de ejecución. Buenas prácticas en la resolución de problemas computacionales Heurísticas para la toma de decisiones. Operadores lógicos y tablas de verdad. Funciones de modelamiento de bases de datos. Fundamentos de lógica y matemáticas aplicadas, operadores lógicos, proposiciones, tablas de verdad, operaciones entre conjuntos, sistemas numéricos y conversiones. Tipos de lógica, proposicional, booleana y matemática. Interfaz gráfica de usuario GUI, usabilidad y accesibilidad. Metodologías de desarrollo, herramientas colaborativas y documentación técnica y de usuario.	Simular algoritmos en entornos digitales o físicos para comprobar su funcionalidad. Evaluar soluciones en función de su eficiencia, claridad y capacidad de resolución del problema. Aplicar heurísticas para resolver problemas donde no existe un camino único o completamente definido. Construir soluciones computacionales básicas empleando herramientas de programación. Revisar errores lógicos o sintácticos en algoritmos o programas mediante procesos de depuración. Integrar estrategias de mejora continua en la solución de problemas computacionales. Verificar sistemáticamente la funcionalidad lógica de las soluciones antes de validarlas. Aplicar operadores lógicos en la resolución de problemas computacionales. Transformar números entres distintos sistemas numéricos, entendiendo los procesos computacionales. Diseñar interfaces graficas con elementos interactivos	Aplicar buenas prácticas en la elaboración de algoritmos organizados, claros y eficientes. Reflexionar sobre los resultados obtenidos como una oportunidad para mejorar las soluciones propuestas. Aceptar con apertura la retroalimentación de otros como parte fundamental del proceso de aprendizaje. Mostrar comunicación asertiva en la resolución de problemas computacionales, Colaborar activamente con sus pares para enriquecer ideas y construir soluciones colectivas. Valorar la importancia de la lógica matemática en la resolución de problemas. Adoptar una actitud perseverante en la resolución de problemas con algoritmos claros y eficientes. Demostrar empatía hacia el usuario final en el diseño de interfaces. Fomentar la colaboración de trabajo en equipo

	aplicando principios de usabilidad y accesibilidad con enfoque al usuario. Utilizar herramientas colaborativas para el trabajo en equipo. Elaborar documentación técnica y de usuario del software.	

Perfil del o la docente

- Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines
- Experiencia en el campo amplio de la Educación, debidamente certificada.

Orientaciones Metodológicas

- Aprendizaje Basado en Proyectos (ABP)
- Aprendizaje en Contextos Reales
- Role-Playing y Simulaciones
- Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)

Requisitos básicos de infraestructuras, espacio y equipamiento:

Denominación	Especificaciones técnicas	Cantidad
Infraestructura/espacio	Entorno de aprendizaje (aula)	1
Laboratorio	Computadoras con acceso a internet Proyector	1

Referencias Bibliográficas

Libros:

- López, A., & Torres, J. (2022). Algoritmos y Programación para Principiantes. Editorial Pearson, México.
- Mendoza, F. (2021). Pensamiento Computacional: Fundamentos y Aplicaciones. Editorial Universitaria, Chile.
- Castro, L. (2023). Introducción a la Programación y Lógica Computacional. Editorial Alfaomega, México.
- Jiménez, R. (2019). Estructuras de Datos y Algoritmos Básicos. Editorial McGraw-Hill, España.
- Hernández, P. (2020). Resolución de Problemas con Programación. Editorial Trillas, México.

Sitios Web:

- Ministerio de Educación del Ecuador (2023). Currículo Nacional para el Bachillerato Técnico: Pensamiento Computacional y Resolución de Problemas.

Quito, Ecuador.

- Instituto Nacional de Estadística y Censos (INEC) Ecuador (2020). Informe sobre competencias digitales en la educación secundaria. Quito, Ecuador.
- Code.org (versión en español). https://code.org
- Scratch (MIT). https://scratch.mit.edu
- Programamos. https://programamos.com

Módulo Genérico Nro.3	
Nombre del módulo:	Ética, Legislación y Ciudadanía Digital
Nivel:	1ro
Duración:	80 periodos pedagógicos
Unidad de competencia asociada:	**UC3**: Integrar principios éticos y legales en el uso de tecnologías, protección de datos, propiedad intelectual y responsabilidad digital con el fin de asumir desempeño consciente y responsable en entornos digitales.
Objetivo del módulo: Fomentar la comprensión y aplicación de principios éticos, normativas legales y prácticas responsables en el uso de las tecnologías digitales, fortaleciendo una ciudadanía digital crítica, respetuosa, segura y consciente de los derechos y deberes en entorno virtuales.	
Resultados de aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1. Analizar los principios éticos relacionados con el uso responsable de las tecnologías digitales. **CE1.1:** Analiza casos o situaciones que evidencias conflictos éticos en el uso de tecnologías digitales. **CE1.2:** Relaciona el uso de herramientas digitales con posibles impactos éticos y sociales en distintos contextos. **CE1.3:** Muestra respeto a los derechos de propiedad intelectual en entornos digitales. **CE1.4:** Reflexiona críticamente sobre sus prácticas digitales cotidianas en el uso ético y responsable de la tecnología en actividades personales, académicas, culturales o profesionales. **RA.2. Diferenciar el uso lícito e ilícito de recursos digitales, software y contenidos en línea.** **CE2.1:** Clasifica recursos digitales según su tipo de licencia y condiciones de uso. **CE2.2:** Discrimina prácticas ilícitas como el uso de software pirata, descargas ilegales, reproducción sin autorización o plagio digital. **CE2.3:** Aplica criterios de legalidad y responsabilidad en la selección, uso y difusión de recursos digitales en contextos educativos o institucionales. **CE2.4:** Evalúa las consecuencias legales y éticas del uso indebido de software y contenidos protegidos por derechos de autor. **RA.3. Aplicar normas legales relacionadas con la protección de datos personales y**	

privacidad digital.

CE3.1: Distingue el tipo de información que se considera dato personal y sensible según la normativa vigente.

CE3.2: Analiza situaciones de vulneración de privacidad en entornos digitales y sus implicaciones legales y éticas.

CE3.3: Aplica buenas prácticas en la recolección, almacenamiento y uso responsable de datos personales en contextos laborales, académicos o comunitarios.

CE3.4: Verifica que las plataformas, formularios o recursos digitales utilizados respeten principios de confidencialidad, seguridad y protección de datos.

RA.4. Promover comportamientos responsables y seguros en el uso de tecnologías y redes digitales.

CE4.1: Distingue situaciones de riesgo digital derivadas de vulnerabilidades de hardware y software, y propone formas de prevención.

CE4.2: Emplea normas básicas de conducta digital (netiqueta) promoviendo valores como el respeto, la responsabilidad, la empatía y la honestidad en entornos laborales, educativos y sociales, haciendo un uso ético y consciente de las tecnologías.

CE4.3: Participa de manera crítica, ética y responsable en entornos digitales, promoviendo el uso de la tecnología y contribuyendo a una cultura digital inclusiva y respetuosa.

CE4.4: Propone actividades que promuevan la ciudadanía digital, el respeto a los demás y el cuidado del entono virtual.

Contenidos

Conceptuales	Procedimentales	Actitudinales
Ética y moral en entornos digitales: • Definición de ética y moral. • Diferencias entre ética personal, profesional y digital • Dilemas éticos en el entorno tecnológico **Principios éticos aplicados a la tecnología:** • Responsabilidad • Integridad • Justicia y equidad • Respeto a la privacidad • Transparencia **Legislación Digital:** • Marco legal • Derechos y deberes • Delitos cibernéticos • Importancia **Ciudadanía Digital:**	Analizar casos reales o simulados de dilemas éticos digitales. Evaluar el cumplimiento de principios éticos en el uso de plataformas tecnológicas. Aplicar criterios éticos en la toma de decisiones digitales (uso de información, comunicación, privacidad). Elaborar códigos de conducta o guías de comportamiento digital para contextos educativos o laborales. Participar en debates o foros sobre temas éticos	Mantener compromiso con el uso responsable de las tecnologías. Respetar la privacidad y la identidad digital propia y ajena. Promover el uso ético de las TIC evitando acoso digital, difusión de contenido falso, piratería. Manifestar actitud crítica y reflexiva frente a la información y a la conducta digital. Demostrar empatía y responsabilidad en la interacción virtual.

• Definición • Componentes • Habilidades • Participación • Ética • Seguridad **Diferencias culturales y legales** **Tendencias futuras en ética digital** Ejemplos de ética digital • Privacidad de datos • Bias algorítmico • Ciberseguridad • Brecha digital **Uso responsable de las tecnologías digitales** • Comportamiento ético en redes sociales y plataformas digitales. • Derechos y deberes de los usuarios digitales • Netiqueta y ciudadanía digital **Consecuencias del uso no ético de la tecnología**: • Ciberacoso, suplantación de identidad, desinformación. • Impactos sociales, legales y personales del mal uso de las TIC Ética profesional en el ámbito tecnológico Sociedad digital Datos y seguridad	relacionados con la tecnología. Participar en campañas sociales digitales o en espacios de discusión respetuosa. Configurar la privacidad en redes sociales. Realizar prácticas de recolección de datos no éticas. Usar contraseñas seguras, reconocer correos fraudulentos o evitar el acceso a sitios web peligrosos	Mantener disposición a actuar con integridad y honestidad en entornos digitales.

Perfil del o la docente
• Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines • Experiencia en el campo amplio de la Educación, debidamente certificada.

Orientaciones Metodológicas

- Aprendizaje Basado en Proyectos (ABP)
- Aprendizaje en Contextos Reales
- Role-Playing y Simulaciones
- Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)

Requisitos básicos de infraestructuras, espacio y equipamiento:

Denominación	Detalle de especificaciones técnicas	Cantidad
Infraestructura/espacio	Entorno de aprendizaje Laboratorio informático	1
Laboratorio	Computadoras con acceso a internet Proyector	1

Referencias Bibliográficas

Normativas y Regulaciones

- Ley Orgánica de Protección de Datos Personales (LOPDP)
- Código Orgánico Integral Penal (COIP), sección delitos informáticos
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Reglamentos emitidos por la Superintendencia de Protección de Datos Recursos Digitales y Plataformas

Marcos de referencia y estrategias:

- Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible)
- OWASP Top 10 (riesgos en aplicaciones web)
- MITRE ATT&CK (catálogo de técnicas y tácticas de ataque)

Sitios Web:

- Plataforma para licencias abiertas y uso responsable de contenido digital. https://creativecommons.org/
- UNESCO: Alfabetización en privacidad https://unesdoc.unesco.org/ark:/48223/pf0000377064
- Organización Mundial de la Propiedad Intelectual (OMPI)
- Legislación internacional, derechos de autor y propiedad intelectual.
- https://www.wipo.int/portal/es/
- Instituto Ecuatoriano de la Propiedad Intelectual (SENADI)
- En caso de estar en Ecuador.
- https://www.propiedadintelectual.gob.ec/
- Common Sense Education
- Recursos para educadores sobre ciudadanía digital, ética, redes y privacidad.
- https://www.commonsense.org/education
- INTEF (España)
- Competencia Digital Docente – incluye módulos sobre ética digital.
- https://intef.es/
- UNESCO – Ciudadanía digital
- Informes y guías para formar en el uso responsable de la tecnología.

- https://unesdoc.unesco.org/ark:/48223/pf0000377064

4. Módulos de especialización

Las y los jóvenes que cursen el Bachillerato Técnico en Seguridad Informática se caracterizarán por contar con una sólida formación en protección de la información digital, administración de sistemas y gestión de riesgos tecnológicos.

Se estructuran los siguientes módulos de especialización:

- Fundamentos de Seguridad Informática
- Manejo de incidentes y recuperación informática
- Gestión y análisis de Vulnerabilidades
- Monitoreo de redes y sistemas informáticos
- Cultura y Conciencia en Ciberseguridad
- Auditorías básicas de seguridad informática

Módulo de Especialización Nro. 1	
Nombre del módulo:	Fundamentos de Seguridad Informática
Nivel:	1ro, 2do
Duración:	200 periodos pedagógicos
Unidad de competencia asociada:	**UC1:** Analizar el estado de seguridad y vulnerabilidades de la red y de los sistemas informáticos, con el fin de reducir amenazas y proponer soluciones digitales.
Objetivo del módulo: Comprender los principios, conceptos y mecanismos de seguridad informática, identificando amenazas, vulnerabilidades y controles, aplicando buenas prácticas en la protección de la información, el uso seguro de tecnologías digitales.	
Resultados de aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1 Seleccionar los activos informáticos que contengan información crítica para la organización, aplicando principios de seguridad de la información. **CE1.1:** Distingue los activos clave (hardware, software, datos, servicios) considerando su valor para la organización. **CE1.2:** Clasifica los activos según su importancia en la confidencialidad, integridad y disponibilidad de la información. **CE1.3:** Analiza principios de análisis de riesgos en la priorización de los activos con base en su impacto potencial frente a amenazas. **CE1.4:** Cataloga los activos identificados en un inventario básico, incluyendo su ubicación, tipo de información que manejan y criticidad. **RA:2 Distinguir las amenazas potenciales internas y externas que pueden afectar los sistemas informáticos utilizando marcos de referencia para su clasificación.** **CE2.1:** Diferencia correctamente amenazas internas como accesos indebidos, errores de configuración, negligencia o sabotaje.	

CE2.2: Compara amenazas externas como malware, phishing, ransomware, ataques por fuerza bruta, entre otros.
CE2.3: Relaciona amenazas con vulnerabilidades, evaluando su impacto en la confidencialidad, integridad y disponibilidad.
CE2.4: Utiliza listas y marcos de referencia simplificados (como OWASP Top 10) para describir tipos comunes de amenazas.

RA:3 Detectar vulnerabilidades y brechas de seguridad utilizando herramientas básicas, interpretando los resultados y proponiendo acciones de mitigación.

CE3.1: Usa herramientas accesibles y seguras para identificar configuraciones inseguras o servicios expuestos.
CE2.3: Aplica técnicas básicas de escaneo en entornos de laboratorio o simulación, respetando políticas de no intrusión.
CE3.3: Interpreta los resultados de las herramientas, diferenciando falsos positivos y priorizando hallazgos por criticidad.
CE3.4: Propone acciones básicas de corrección o mitigación en base a buenas prácticas y al entorno evaluado.

RA:4. Justificar los hallazgos de seguridad en un informe técnico con lenguaje adecuado, respetando estándares de manejo seguro de la información.

CE4.1: Organiza la información recolectada de manera estructurada, siguiendo un formato prediseñado.
CE4.2: Elabora informes con lenguaje técnico claro y adecuado al contexto educativo o institucional.
CE4.3: Presenta el informe aplicando principios básicos de manejo seguro de la información (confidencialidad, integridad y trazabilidad).

Contenidos

Conceptuales	**Procedimentales**	**Actitudinales**
Historia la seguridad informática. Introducción y conceptos básicos de la seguridad informática. • Elementos de la red • Software • Spam • Phishing • Cookies • Bluetooth • Smishing • Vishing • Fake News Principios básicos • Confidencialidad	Debatir la historia de la seguridad informática. Identificar elementos claves de la seguridad informática. Clasificar los principios de la seguridad informática. Analizar amenazas y vulnerabilidades en diferentes contextos. Evaluar situaciones o casos donde se presentan riesgos digitales.	Mostrar responsabilidad en el uso de tecnologías. Usar de forma ética y legal los recursos informáticos. Cooperar en actividades de concienciación y formación en seguridad. Compartir buenas prácticas y conocimientos con respeto y apertura. Demostrar Pensamiento crítico y reflexivo. Mostrar respeto por la privacidad y los derechos digitales.

• Integridad • Disponibilidad • Autenticidad Tipos de seguridad • Seguridad de Red • Seguridad de Software • Seguridad de Hardware •Seguridad de la Información • Seguridad de Aplicaciones • Seguridad de Identidad Herramientas de seguridad esenciales • Antivirus • Firewall • Cifrado •Escáneres de vulnerabilidades • Control de acceso a la red (NAC). • Sistemas de prevención de intrusiones (IPS). • Contraseñas Seguridad física y seguridad lógica. Vulnerabilidades, tipos y factores Amenazas y sus tipos. Ciclo de la seguridad informática. Controles y medidas de seguridad. Tipos de ataques informáticos.	Configurar contraseñas seguras y autentificar correctamente el acceso. Detectar y evitar correos o enlaces sospechosos (phishing). Verificar certificados y protocolos seguros de navegación web. Instalar, actualizar y configurar antivirus y firewall. Utilizar herramientas de análisis malware y escaneo básico.	Fomentar el uso responsable y ético de plataformas digitales. Valorar la confidencialidad de la información propia y ajena.
Perfil del o la docente		
• Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines.		

<table>
<tr><td colspan="3">• Experiencia en el campo amplio de la Educación, debidamente certificada.</td></tr>
<tr><td colspan="3">Orientaciones Metodológicas</td></tr>
<tr><td colspan="3">• Aprendizaje Basado en Proyectos (ABP)
• Aprendizaje en Contextos Reales
• Role-Playing y Simulaciones
• Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)</td></tr>
<tr><td colspan="3">Requisitos básicos de infraestructuras, espacio y equipamiento:</td></tr>
<tr><td>Denominación</td><td>Especificaciones técnicas</td><td>Cantidad</td></tr>
<tr><td>Infraestructura/espacio</td><td>Entorno de aprendizaje (aula)</td><td>1</td></tr>
<tr><td>Infraestructura/espacio</td><td>Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización.</td><td>1</td></tr>
<tr><td>Recursos</td><td>Sistemas de detección y análisis:
• Consolas básicas de Snort (mínimo requerido)
• Suricata integrado con Kibana o ELK Stack (recomendado)
Herramientas de diagnóstico y análisis:
• Nmap
• OpenVAS o Nessus Essentials
• Metasploit Framework
• Wireshark
• Snort o Suricata
• Zeek (recomendado)
• OSSEC (recomendado para monitoreo de integridad)
• Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados)
Gestión de tickets e incidentes:
• GLPI o OTRS (recomendado)</td><td></td></tr>
<tr><td colspan="3">Referencias Bibliográficas</td></tr>
<tr><td colspan="3">Normativas y Políticas Públicas en Ecuador
• Ley Orgánica de Protección de Datos Personales (LOPDP)
• Código Orgánico Integral Penal (COIP), sección delitos informáticos
• Ley de Comercio Electrónico, Firmas y Mensajes de Datos
• Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles)
Sitios Web:
• Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible)</td></tr>
</table>

- NIST SP 800-30 (análisis de riesgos)
- NIST SP 800-53 (controles de seguridad para sistemas de información)
- ISO/IEC 27001 (gestión de la seguridad de la información)
- ISO/IEC 27002 (controles de seguridad)
- OWASP Top 10 (riesgos en aplicaciones web)
- MITRE ATT&CK (catálogo de técnicas y tácticas de ataque)
- Introducción a los fundamentos de la seguridad informática (Erik de Luis Gallardo)
- https://openaccess.uoc.edu/server/api/core/bitstreams/174d92aa-6c4d-495e-8ac4-bccb6dc680a1/content
- Fundamentos de seguridad informática (Carlos Arturo Avenía Delgado)
- https://core.ac.uk/download/pdf/326424171.pdf

Módulo de Especialización Nro. 2	
Nombre del módulo:	Manejo de incidentes y recuperación informática
Nivel:	1ro, 2do
Duración:	280 periodos pedagógicos
Unidad de competencia asociada:	**UC2:** Aplicar protocolos de respuesta ante incidentes, recuperando sistemas y respaldos de información, garantizando la continuidad operativa de los servicios.
Objetivo del módulo: Aplicar procedimientos y protocolos de respuesta ante incidentes de seguridad informática, identificando y clasificando eventos, mitigando daños, recuperando sistemas comprometidos y restaurando respaldos de información, conforme a normas técnicas y buenas prácticas.	
Resultados de aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1. Clasificar los tipos de incidentes de seguridad informática distinguiendo eventos y aplicando las etapas del ciclo de respuesta. **CE1.1:** Distingue eventos de seguridad como errores humanos, fallos técnicos, accesos no autorizados o ataques maliciosos. **CE1.2:** Clasifica los incidentes por origen (interno/externo), tipo (tecnológico/humano) e intencionalidad (accidental/deliberado), utilizando categorías simplificadas. **CE1.3:** Aplica las etapas básicas del ciclo de respuesta ante incidentes: detección, análisis, contención, erradicación y recuperación. **RA:2 Establecer acciones básicas de contención y mitigación frente a incidentes utilizando procedimientos controlados y registrando la trazabilidad de las acciones ejecutadas .** **CE2.1:** Usa comandos, herramientas o procedimientos básicos (como deshabilitación de servicios, aislamiento de red o uso de antivirus) en entornos controlados. **CE2.2:** Justifica la decisión de aislar sistemas comprometidos evitando la propagación del	

incidente, según protocolos preestablecidos en prácticas simuladas.

CE2.3: Cataloga las acciones ejecutadas utilizando una bitácora técnica clara, manteniendo trazabilidad de los pasos tomados.

RA:3. Restaurar los sistemas afectados utilizando respaldos verificados y validación funcional.

CE3.1: Verifica que las copias de respaldo estén completas y sin alteraciones antes de restaurar datos.

CE3.3: Evalúa el nivel de daño sufrido por los sistemas y selecciona el método de restauración más apropiado.

CD4.3: Restaura correctamente sistemas operativos, configuraciones o archivos desde copias de seguridad locales o en la nube.

CE4.4: Realiza pruebas de funcionalidad básicas (servicios activos, accesos permitidos, ausencia de errores) para validar la correcta recuperación del sistema.

Contenidos

Conceptuales	**Procedimentales**	**Actitudinales**
Conceptos fundamentales de incidentes de seguridad • Evento • Incidente de seguridad •Incidente de seguridad computacional • Sistema de información Manejo de Incidentes • Preparación • Detección y análisis • Contención, Erradicación y recuperación • Revisión post incidente Prevención de incidentes. Detección y análisis. Clasificación de los incidentes. Protocolos de respuesta ante incidentes. Ciclo de gestión de incidentes. Síntomas de un incidente.	Analizar registros (logs) y alertas generadas por herramientas de monitoreo. Documentar el incidente y reportarlo según el protocolo establecido. Evaluar el tipo, origen, impacto y alcance del incidente. Asignar niveles de criticidad de acuerdo con criterios predefinidos. Determinar la urgencia de respuesta y aplicar políticas de escalamiento. Aplicar protocolos de respuesta ante incidentes. Ejecutar acciones de contención para evitar la propagación del daño. Realizar la recuperación de sistemas afectados.	Cumplir con los procedimientos establecidos para la gestión de incidentes. Asumir con seriedad las tareas asignadas durante la respuesta y recuperación. Proteger la confidencialidad de la información durante y después del incidente. Verificar cuidadosamente los registros y evidencias antes de actuar. Mantener una comunicación efectivamente con el equipo durante situaciones críticas. Presentar una actitud proactiva y preventiva.

Análisis del incidente. Priorización de los incidentes y tiempos de respuesta. Recolección y manejo de evidencias. Recursos para la mitigación y remediación. Componentes de un Plan de Manejo de Incidentes. Fases del Manejo de Incidentes (según el NIST). Gestión de respaldo de información. Normativa, estándares y buenas prácticas. Principios de la comunicación técnica. Características de la comunicación técnica: claridad, precisión, objetividad. Diferencias entre comunicación técnica y comunicación general. Tipos de destinatarios: técnicos, usuarios, directivos. Elementos y estructura de un informe técnico. Tipos de documentación de incidentes de seguridad informática.	Restaurar el funcionamiento de sistemas y servicios comprometidos. Verificar la integridad del sistema tras la recuperación. Validar la operación normal con pruebas de funcionalidad. Realizar respaldos periódicos según cronograma. Probar la integridad de los respaldos. Restaurar datos de forma efectiva en caso de pérdida o corrupción. Proponer medidas preventivas y correctivas para evitar futuros incidentes. Organizar cronológicamente la información obtenida. Registrar y documentar acciones durante la gestión del incidente. Utilizar formatos estandarizados para describir procedimientos, hallazgos y decisiones. Incorporar capturas, archivos de registro y datos de respaldo como evidencia documental. Redactar documentos utilizando lenguaje claro, técnico y objetivo. Proteger los documentos digitales mediante contraseñas,	Demostrar ética y confidencialidad en el manejo de la información. Cumplir con los procedimientos establecidos para la elaboración y resguardo de documentación técnica. Respetar las políticas de privacidad, propiedad de la información y uso adecuado de los datos. Rechazar prácticas como la alteración de datos o la omisión de información relevante.

Buenas prácticas en el registro de información técnica. Confidencialidad y resguardo de la información.	cifrado o almacenamiento seguro.	

Perfil del o la docente

- Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines.
- Experiencia en el campo amplio de la Educación, debidamente certificada.

Orientaciones Metodológicas

- Aprendizaje Basado en Proyectos (ABP)
- Aprendizaje en Contextos Reales
- Role-Playing y Simulaciones
- Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)

Requisitos básicos de infraestructuras, espacio y equipamiento:

Denominación	Detalle de especificaciones técnicas	Cantidad
Infraestructura/espacio	Entorno de aprendizaje (aula)	1
Laboratorio	Laboratorio de Informática equipado con acceso a Internet, redes internas aisladas y estaciones con capacidad de virtualización.	1
	Computadoras con acceso a internet Proyector Software de gestión para recetas, menús, inventarios y planificación de compras.	
Equipos/herramientas	**Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Sistemas de detección y análisis:**	

	• Consolas básicas de Snort (mínimo requerido) • Suricata integrado con Kibana o ELK Stack (recomendado) **Hardware complementario:** • Switch gestionable básico (recomendado) • Router o firewall físico (recomendado) • Dispositivos IoT para prácticas de evaluación de riesgos (recomendado)	

Normativas y Políticas Públicas en Ecuador

- Ley Orgánica de Protección de Datos Personales (LOPDP)
- Código Orgánico Integral Penal (COIP), sección delitos informáticos
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles)

Normativas y Estrategias:

- Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible)
- NIST SP 800-30 (análisis de riesgos)
- NIST SP 800-53 (controles de seguridad para sistemas de información)
- ISO/IEC 27001 (gestión de la seguridad de la información)
- ISO/IEC 27002 (controles de seguridad)
- OWASP Top 10 (riesgos en aplicaciones web)
- MITRE ATT&CK (catálogo de técnicas y tácticas de ataque)

Recursos Digitales y Plataformas

- Gestión de incidentes de seguridad de la información - Subdirección de Diseño y Análisis Estratégico Bogotá 2017
- In_069_Gestion_De_Incidentes_De_Seguridad.pdf.pdf
- Seguridad y privacidad de la información – MINTIC – Colombia
- https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf
- Guía de respuesta a incidentes Publicación: enero de 2024 Agencia de Ciberseguridad y Seguridad de Infraestructura
- https://www.cisa.gov/sites/default/files/2024-05/WWS-Sector_Incident-Response-Guide_ES.pdf
- Gestión de datos de investigación - CEPAL
- https://biblioguias.cepal.org/c.php?g=495473&p=4398114
- **Guías técnicas y buenas prácticas:**
- CIS Benchmarks para hardening de sistemas
- Guías de configuración segura de NIST
- Manuales institucionales o académicos para Windows/Linux

Módulo especialización Nro.3	
Nombre del módulo formativo:	Cultura y Conciencia en Ciberseguridad
Nivel:	1ero, 2do, 3ro
Duración:	400 periodos pedagógicos
Unidad de competencia asociada:	**UC4:** Emplear normas de protección de datos y de ciberseguridad en sistemas informáticos, garantizando la protección de información sensible. **UC 6:** Promover la cultura de seguridad informática en el entorno escolar, empresarial o comunitario, aplicando prácticas seguras y prevención de incidentes, contribuyendo a la creación de entornos digitales confiables. **UC8:** Aplicar fundamentos del hacking ético y análisis forense básico en la evaluación de la seguridad de sistemas y redes en entornos controlados, interpretando hallazgos, proponiendo mejoras de protección y cumpliendo principios legales y éticos.
Objetivo del módulo: Fomentar una cultura de seguridad digital mediante la identificación de riesgos cibernéticos, la adopción de comportamientos responsables en el uso de tecnologías de la información y la promoción de prácticas seguras que contribuyan a la protección de datos.	
Resultados de aprendizaje (RA) y Criterios de Evaluación (CE)	
RA.1: Clasificar las principales normas, leyes y marcos regulatorios aplicables a la protección de datos y ciberseguridad, interpretando sus principios fundamentales y relacionándolos con situaciones prácticas. **CE1.1:** Cataloga las principales leyes y normas relacionadas con la protección de datos y la ciberseguridad, como la LOPDP y el COIP en Ecuador, e instrumentos internacionales como el RGPD e ISO/IEC 27001. **CE1.2:** Explica las consecuencias legales, técnicas y organizacionales del incumplimiento de normas sobre protección de datos. **CE1.3:** Aplica los principios fundamentales de la protección de datos, tales como consentimiento informado, minimización, finalidad, seguridad y responsabilidad.CD1.4: Relaciona correctamente marcos normativos con situaciones comunes en entornos educativos, laborales o comunitarios. **CE1.4:** Relaciona correctamente marcos normativos con situaciones comunes en entornos educativos, laborales o comunitarios. **RA.2: Analizar los principios de protección de datos con la seguridad de la información, evaluando riesgos y proponiendo medidas para proteger datos sensibles.** **CE2.1:** Analiza cómo se aplican los principios de protección de datos personales en casos reales o simulados de manejo de información.	

CE2.2: Relaciona los principios de protección de datos con los pilares de la seguridad de la información: confidencialidad, integridad, disponibilidad y trazabilidad.
CE2.3: Examina los riesgos y consecuencias de no aplicar los principios de protección de datos sobre los titulares de la información.
CE2.4: Propone medidas básicas como encriptación, control de accesos, respaldos o anonimización, para proteger datos sensibles.
RA3: Aplicar políticas organizacionales y controles técnicos conforme a normas y estándares básicos de seguridad, configurando parámetros adecuados y realizando mejoras ante debilidades detectadas.
CE3.1: Utiliza controles técnicos como autenticación, cifrado, respaldo y bitácoras, alineados con políticas organizacionales de seguridad.
CE3.2: Configura parámetros de seguridad adecuados para proteger el acceso y la integridad de los datos, en plataformas o entornos simulados.
CE3.3: Evalúa de forma general la eficacia de los controles frente a amenazas comunes.
CE3.4: Realiza mejoras prácticas ante debilidades o incumplimientos detectados en los controles aplicados.
RA4: Aplicar buenas prácticas de seguridad informática en distintos contextos incorporando medidas de protección y procedimientos de prevención de incidentes.
CE4.1: Muestra buenas prácticas de protección de datos personales y corporativos en actividades escolares, laborales y comunitarias.
CE4.2: Reporta comportamientos o incidentes que comprometen la seguridad de la información, conforme a protocolos básicos.
CE4.3: Utiliza contraseñas robustas, cifrado y respaldos como mecanismos esenciales de protección.
CE4.4: Emplea principios como consentimiento informado y privacidad en el tratamiento de datos personales.
RA5: Relacionar los controles de seguridad con los requisitos establecidos en normas de referencia, identificando tipos, utilizando mapeos y considerando el marco legal aplicable.
CE5.1: Analiza los tipos de controles de seguridad: preventivos, detectivos y correctivos, sus aplicaciones en la protección de sistemas y datos.
CE5.2: Utiliza herramientas o esquemas de mapeo normativo básico para verificar el cumplimiento de requisitos.
CE5.3: Demuestra comprensión del marco legal nacional e internacional y su importancia en la gestión de la seguridad de la información.
RA6: Fomentar comportamientos seguros mediante recursos digitales y acciones formativas adaptando los mensajes y materiales al contexto y necesidades del entorno.
CE6.1: Distingue necesidades y riesgos del entorno para diseñar estrategias de sensibilización contextualizadas.
CE6.2: Selecciona contenidos relevantes sobre amenazas, buenas prácticas y normas de ciberseguridad básicas.
RA7: Diseñar estrategias de sensibilización en ciberseguridad adaptadas al entorno, integrando recursos apropiados para el público objetivo.

CE7.1: Distingue las necesidades, características y riesgos específicos del entorno en la construcción de estrategias de sensibilización.
CE7.2: Crea mensajes claves sobre el uso responsable de las tecnologías, protección de datos personales y gestión segura de contraseñas.
CE7.3: Elabora materiales de apoyo de sensibilización en ciberseguridad para difundir en su entorno social, educativo u organizacional.
RA8: Promover el uso ético, legal y responsable de los recursos informáticos en diferentes contextos, integrando estrategias que fomenten la protección de la información y la propiedad intelectual.
CE8.1: Selecciona normativas básicas sobre el uso adecuado de tecnología y protección de la propiedad intelectual.
CE8.2: Distingue las practicas inadecuadas o riesgosas en el uso de la información y propone alternativas responsables.
CE8.3: Aplica el uso responsable y consciente de tecnologías digitales en contextos educativos, sociales o laborales.
CE8.4: Propone estrategias que fomenten el respeto por los derechos de autor, licencias de software y uso correcto de contenidos digitales.
RA9: Diferenciar el hacking ético del hacking malicioso, destacando el rol del consentimiento y aplicando normativa vigente.
CE9.1: Analiza los principios del hacking ético, incluyendo legalidad, autorización, confidencialidad y responsabilidad profesional.
CE9.2: Distingue las fases de una prueba de penetración (reconocimiento, escaneo, explotación simulada y reporte).
CE9.3: Aplica técnicas básicas de reconocimiento y escaneo de vulnerabilidades utilizando herramientas autorizadas y en entornos simulados.
CE9.4: Documenta los hallazgos de forma técnica, sin comprometer la operación o integridad del entorno evaluado.
RA10: Emplear herramientas básicas de análisis forense para recolectar y preservar evidencia digital, asegurando la integridad, trazabilidad de los hallazgos en entornos controlados.
CE10.1: Distingue conceptos clave del análisis forense: cadena de custodia, integridad de la evidencia, duplicación forense.
CE10.2 Utiliza herramientas básicas de adquisición y análisis de datos digitales en discos o sistemas de archivos.
CE10.3: Aplica procedimientos de preservación de evidencia en entornos simulados, asegurando su integridad y trazabilidad.
CE10.4: Describe hallazgos relevantes derivados del análisis forense, considerando su valor probatorio en contextos educativos o institucionales.
RA11: Interpretar los hallazgos de pruebas éticas y análisis forense básico para apoyar decisiones de seguridad, evaluando el origen de incidentes y presentando resultados de forma clara, estructurada.
CE11.1: Relaciona las vulnerabilidades encontradas con los riesgos de seguridad identificados.

CE11.2: Evalúa la información obtenida en análisis forense para comprender el origen y tipo de incidente simulado.
CE11.3: Propone medidas preventivas o correctivas básicas basadas en los hallazgos.
CE11.4: Presenta los resultados de manera clara, estructurada y respetando principios de confidencialidad.
RA12: Aplicar principios legales y éticos en todas las etapas del hacking ético y análisis forense básico, respetando normativa legal, marcos éticos y consentimiento.
CE12.1: Distingue los límites legales del hacking ético en Ecuador, incluyendo delitos informáticos definidos en el COIP.
CE12.2: Reconoce los marcos éticos y normativos internacionales que rigen el análisis forense y las pruebas de penetración (ej. EC-Council, NIST).
CE12.3: Justifica la importancia del consentimiento informado y la autorización previa en toda práctica de evaluación de seguridad.
CE12.4: Utiliza una postura ética en la interpretación y uso de los hallazgos, evitando su uso indebido o malicioso.

Contenidos

Conceptuales	**Procedimentales**	**Actitudinales**
Uso ético y legal de la información y recursos digitales. Normativa y principios éticos. Concepto de vulnerabilidad, amenaza, exploit y vector de ataque. Definición de cultura de ciberseguridad. Buenas prácticas para la navegación, comunicación y uso de dispositivos. Importancia de la cultura de ciberseguridad. Componentes de la cultura de ciberseguridad. Ciberseguridad personal y organizacional. Desarrollo de la cultura de ciberseguridad.	Evaluar el comportamiento digital propio y de otros con base en criterios de seguridad. Aplicar buenas prácticas para la protección de datos y cuentas personales. Simular escenarios de riesgo y proponer respuestas seguras. Identificar servicios y vulnerabilidades con escáneres. Simular ataques controlados en entornos virtualizados. Configurar y utilizar entornos de laboratorio para pruebas. Aplicar exploits de forma ética para validar fallas de seguridad.	Demostrar responsabilidad y compromiso en el uso de tecnologías digitales. Valorar la privacidad y respeta la información personal y ajena. Promover el comportamiento ético en entornos virtuales. Reconocer el papel del usuario como primera línea de defensa en la ciberseguridad. Mantener una actitud crítica y reflexiva frente al uso de internet y redes sociales. Respetar por la ética profesional y la legalidad en el uso de técnicas de hacking. Demostrar conciencia del impacto social y legal del mal uso del conocimiento técnico. Manifestar confidencialidad en el tratamiento de hallazgos

Impacto de la cultura en la ciberseguridad. Ciudadanía digital responsable. Derechos y deberes digitales. Nociones de programación, cifrado y descifrado enfocados a la seguridad informática. Definición y principios del hacking ético. Tipos de hackers. Ciclo del hacking ético: reconocimiento, escaneo, explotación, post-explotación y reporte. Marco legal y ético del hacking (normas, consentimiento, privacidad). Metodologías de pruebas de penetración (OWASP, OSSTMM, PTES).	Recolectar evidencia digital en pruebas . Documentar hallazgos y redactar informes técnicos con lenguaje claro y técnico. Utilizar máquinas virtuales y redes simuladas para prácticas seguras. Emplear formatos estándar para reportes de pruebas de penetración. Elaborar campañas, charlas o materiales de concienciación sobre ciberseguridad. Participar en actividades colaborativas para fortalecer la cultura de seguridad informática.	técnicos.
Perfil del o la docente		
• Experiencia en el área técnica, poseer título de tercer o cuarto nivel, registrados y reconocidos por el órgano rector del Sistema de Educación Superior en: Tecnologías de la Información, Ciencias de la Computación, Ingeniería en Sistemas, Ingeniería en Software, Tecnologías de la Información y Comunicación, o ramas afines. • Experiencia en el campo amplio de la Educación, debidamente certificada.		
Orientaciones Metodológicas		
• Aprendizaje Basado en Proyectos (ABP) • Aprendizaje en Contextos Reales • Role-Playing y Simulaciones • Metodología STEAM (Integración de Ciencia, Tecnología, Arte y Matemáticas)		
Requisitos básicos de infraestructuras, espacio y equipamiento:		

Denominación	Especificaciones técnicas	Cantidad
Infraestructura/espacio	Entorno de aprendizaje (aula)	1
Laboratorio	Laboratorio de Informática equipado con acceso a Internet	1
Recursos	**Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados) **Herramientas de diagnóstico y análisis:** • Nmap • OpenVAS o Nessus Essentials • Metasploit Framework • Wireshark • Snort o Suricata • Zeek (recomendado) • OSSEC (recomendado para monitoreo de integridad) • Hashcat / John the Ripper (recomendado para ejercicios de recuperación de contraseñas en entornos simulados)	

Referencias Bibliográficas

Normativas y Políticas Públicas en Ecuador

- Ley Orgánica de Protección de Datos Personales (LOPDP)
- Código Orgánico Integral Penal (COIP), sección delitos informáticos
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Reglamentos emitidos por la Superintendencia de Protección de Datos (si están disponibles)

Normativas y Estrategias:

- Estrategia Nacional de Ciberseguridad del Ecuador (última versión disponible)
- NIST SP 800-30 (análisis de riesgos)
- NIST SP 800-53 (controles de seguridad para sistemas de información)
- ISO/IEC 27001 (gestión de la seguridad de la información)

- ISO/IEC 27002 (controles de seguridad)
- OWASP Top 10 (riesgos en aplicaciones web)
- MITRE ATT&CK (catálogo de técnicas y tácticas de ataque)

Recursos Digitales y Plataformas

- Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial.
- Https://biblioteca.unapec.edu.do/media/gdibsyuc/ciberseguridad.pdf
- Hacking ético: Guía de estudio para el Certified Ethical Hacker (CEH): (Spanish Edition). Autor: S0mbr3r3r0, Sr. Editorial: Amazon.com.mx.
- Hacking ético: (Informática y Comunicaciones). Autor: Esteban Sánchez, Pablo, Berenguel Gómez, Jose Luis. Editorial: Anaya Multimedia.
- Hacking ético: Autor(es): Jose Luis Berenguel Gómez, Pablo Esteban Sánchez. Editorial: Ediciones Paraninfo.

5. Módulo práctico/experimental

Este módulo fortalece la formación del estudiantado mediante su participación en situaciones reales de aprendizaje, simulaciones, acercamiento a entornos de trabajo, giras de observación, articulación con el sector productivo, proyectos interdisciplinarios y metodologías basadas en proyectos. Todas estas actividades tienen como finalidad consolidar los conocimientos teóricos y favorecer la aplicación de competencias en contextos reales. Asimismo, promueven el desarrollo de habilidades blandas, tales como el trabajo en equipo, la comunicación asertiva, la resolución de problemas y la adaptación a entornos cambiantes.

En síntesis, este módulo constituye la aplicación práctica e integral de lo aprendido en los módulos previos, permitiendo al estudiantado experimentar, analizar y resolver situaciones reales, al tiempo que refuerza sus capacidades técnicas y fomenta el desarrollo de competencias conceptuales, procedimentales y actitudinales, tanto de los módulos genéricos como de los de especialización.

Módulo Práctico Experimental		
Nombre del módulo:	Practico Experimental	
Nivel:	1ro, 2do, 3ro	
Duración:	400 periodos pedagógicos	
Unidad de competencia asociada:	Practicar el monitoreo de redes y sistemas informáticos en la detección de eventos de seguridad y riesgos, aplicando herramientas de supervisión, análisis de datos y elaboración de reportes técnicos conforma a protocolos establecidos.	
Objetivo del módulo: Aplicar de forma integrada y experimental los conocimientos, procedimientos y herramientas de seguridad informática en entornos controlados o simulados, mediante la ejecución de prácticas técnicas orientadas a la detección de vulnerabilidades, respuesta ante incidentes, protección de sistemas y evaluación de riesgos, promoviendo el pensamiento crítico y el trabajo colaborativo.		
Resultados de aprendizaje (RA)	**Criterios de evaluación (CE)**	**Actividades Prácticas Experimentales**
RA1: Aplicar técnicas básicas de análisis de vulnerabilidades y pruebas de penetración en entornos simulados	**CE1.1:** Reconoce y clasifica incidentes simulados **CE1.2:** Aplica procedimientos adecuados de contención, erradicación y recuperación de sistemas de la información.	**Simulación de incidente y recuperación** Escenario de incidente: malware detectado, caída de servicio, acceso no autorizado. Aplicación del plan de respuesta: detección,

		contención, erradicación, recuperación. Restauración del sistema desde un respaldo previo.
RA2: Diseñar una campaña educativa para promover prácticas seguras en el uso de tecnologías y protección de la información.	**CE2.1**: Identifica de manera clara los temas clave de la campaña (phishing, contraseñas seguras, privacidad, uso responsable de redes, entre otros). **CE2.2**: Utiliza herramientas TIC para crear materiales atractivos.	**Campaña de concienciación en seguridad digital** Diseño de afiches, videos, charlas o infografías sobre buenas prácticas. Difusión del contenido en medios institucionales o murales.