CERTIFICADO UNIVERSITARIO
SEGURIDAD INFORMÁTICA

UNAH Ciudad Universitaria

Dirección
Académica
de Formación Tecnológica

VRA
Vicerrectoría
Académica

UNAH
UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS

Ficha de Registro del Certificado Universitario

Nombre del Certificado:	**Código de certificado:**
Seguridad Informática	103
Unidad Académica responsable:	**Nivel:**
– Facultad de Ciencias Económicas, Administrativas y Contables, Ciudad Universitaria.	**AVANZADO** Título Universitario de grado y posgrado
Carga Horaria en créditos académicos:	**Dirigido a:**
– DIA320 Seguridad Informática I 4 C.A. – DIA320 Seguridad Informática I 4 C.A. Condiciones curriculares: la clase de Seguridad Informática I es requisito para cursar Seguridad Informática II.	Profesionales universitarios en las áreas de tecnologías de la información, ingeniería, ciencias computacionales, redes y telecomunicaciones que buscan actualizar sus conocimientos, fortalecer habilidades prácticas y adquirir herramientas normativas y estratégicas para enfrentar amenazas actuales en entornos digitales, proteger activos tecnológicos, y garantizar la continuidad operativa de las organizaciones públicas o privadas en las que laboran.
Duración:	**Modalidad:**
Duración: 90 horas **Fecha de inicio:** octubre, 2025 **Vigencia de certificado:** 1 promoción (30 participantes) **Fecha de emisión:** fecha máxima de emisión de certificado III PAC 2026.	Presencial y a distancia (expresión semipresencial con mediación virtual).
Costo del certificado:	
En convenio con ECASS (Escuela Centroamericana de Capacitación en Seguridad Social).	
Elaborado por:	**Fecha:**
Departamento de Informatica Administrativa	Julio 2025
Revisado por:	**Fecha:**
DAFT	Julio 2025
Aprobado por:	**Fecha:**
Pendiente	Pendiente

Subcompetencias:

a. Identificar vulnerabilidades críticas en sistemas, redes y plataformas de información, utilizando criterios de evaluación técnica y normativa vigente en seguridad informática.

b. Planificar y gestionar entornos seguros en organizaciones públicas o privadas, mediante el diseño de estrategias de protección de datos, activos digitales y sistemas críticos.

c. Aplicar protocolos y estándares internacionales de seguridad de la información (como ISO/IEC 27002) para diseñar, implementar y auditar políticas internas de protección.

d. Utilizar herramientas especializadas para realizar análisis de malware, pruebas de penetración (Pentest) y simulaciones de ataques controlados, con fines de detección y respuesta.

e. Desarrollar e implementar planes de respuesta a incidentes cibernéticos, integrando la atención temprana, análisis forense y recuperación de sistemas.

f. Evaluar y seleccionar software, hardware y configuraciones de red que contribuyan a una arquitectura tecnológica resiliente frente a amenazas emergentes.

g. Monitorear y documentar los accesos, eventos y anomalías del sistema, construyendo una base de datos de incidentes que permita la trazabilidad y mejora continua.

h. Establecer políticas internas de ciberseguridad para el acceso, uso y gestión de información sensible, con enfoque en control de riesgos y continuidad del negocio

i. Aplicar metodologías de análisis forense digital y recuperación de evidencias electrónicas, garantizando el cumplimiento de estándares legales y éticos.

j. Implementar soluciones integrales de seguridad informática, considerando componentes técnicos, humanos, organizacionales y normativos.

Resultados de aprendizaje:

a. Aplica conocimientos y herramientas de seguridad informática para la identificación y mitigación de vulnerabilidades en sistemas operativos, bases de datos, redes y plataformas digitales, según estándares técnicos actuales.

b. Desarrolla e implementa planes de respuesta ante incidentes cibernéticos, incorporando análisis forense, gestión de riesgos, recuperación de servicios y documentación de eventos de seguridad.

c. Evalúa e integra soluciones tecnológicas (software, hardware y protocolos) que fortalezcan la protección de datos, la continuidad operativa y la infraestructura crítica de organizaciones públicas o privadas.

d. Diseña políticas y estrategias institucionales de seguridad de la información, considerando normativas internacionales como ISO/IEC 27002, la gobernanza organizacional y la protección integral de los activos digitales.

e. Utiliza herramientas de simulación, Ethical Hacking y pruebas de penetración (Pentest) para diagnosticar y reforzar los mecanismos de defensa de los sistemas informáticos, con un enfoque ético, preventivo y basado en evidencia

Contenidos:

Se anexan descripciones mínimas de los espacios de aprendizaje de:

- DIA320 Seguridad Informática I 4 C.A.
- DIA331 Seguridad Informática II 4 C.A.

Estrategias de Enseñanza-aprendizaje

- Uso de herramientas de software de simulación virtual, realidad aumentada, gamificación y equipo real.
- Participación en el campus virtual (pruebas, foros, entrega de actividades, conferencias y otros).
- Análisis y solución de problemas dentro y fuera del espacio de aprendizaje.
- Resolución de guías de estudio, ejercicios, resúmenes y otros.
- Discusión de casos mediante el aprendizaje cooperativo y colaborativo.
- Prácticas con equipo real, simulando fallas, realizando instalación, configurando, aplicando la seguridad y realizando respaldo.

Método de evaluación:

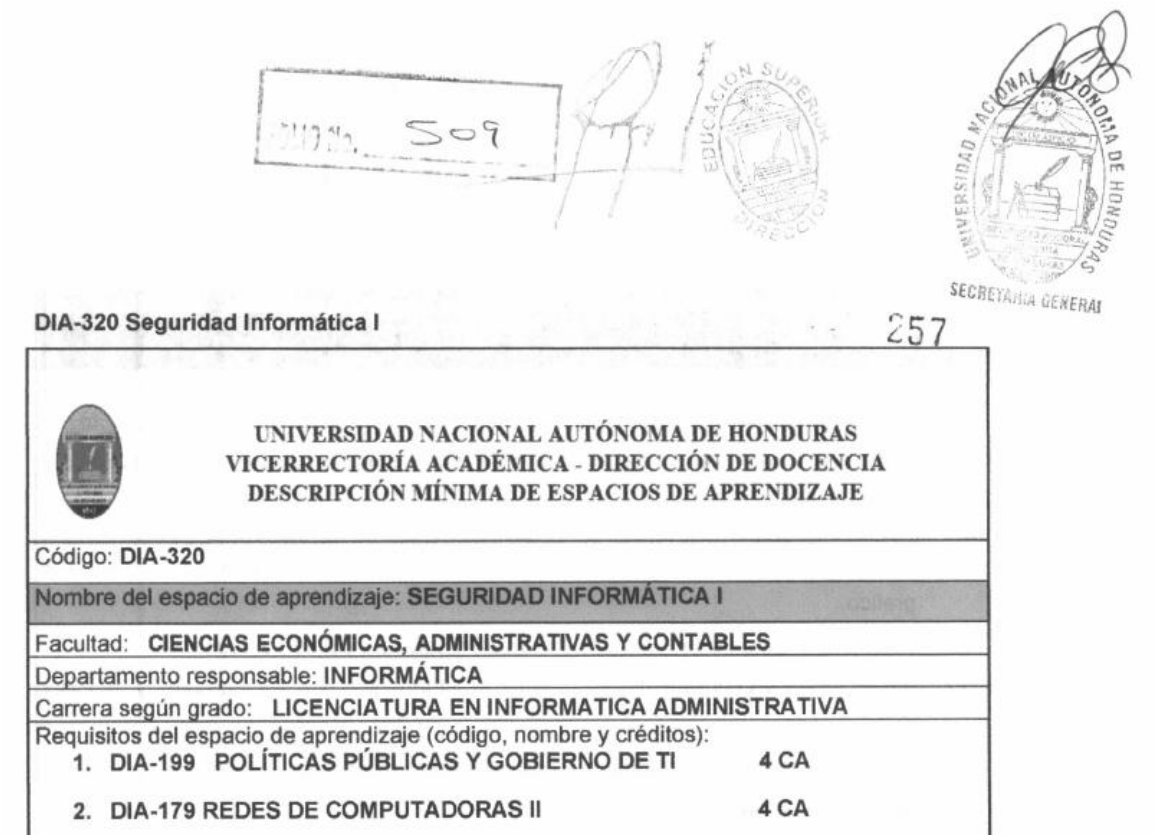
- Evaluación diagnóstica
- Evaluación formativa incluyendo 3 exámenes, foros, tareas, casos simulados, proyecto, cuestionarios, controles de lecturas y pruebas.

El estudiante se considera "APTO" para recibir el Diploma de aprobación cuando el docente a evaluado la totalidad de resultados de aprendizaje y cumpla con el 80% de asistencia. Si el estudiante solamente cumple con el 80% de asistencia, pero no cumple con la totalidad de los resultados de aprendizaje, se otorgará un Diploma de participación.

Contacto del Coordinador del Certificado

UNAH Ciudad Universitaria:
Nombre: Sandra Janeth Quan
Correo electrónico: sandra.quan@unah.edu.hn
Teléfono: 9586-8881

DIA 320 SEGURIDAD INFORMÁTICA I



DIA-320 Seguridad Informática I

257

UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS
VICERRECTORÍA ACADÉMICA - DIRECCIÓN DE DOCENCIA
DESCRIPCIÓN MÍNIMA DE ESPACIOS DE APRENDIZAJE

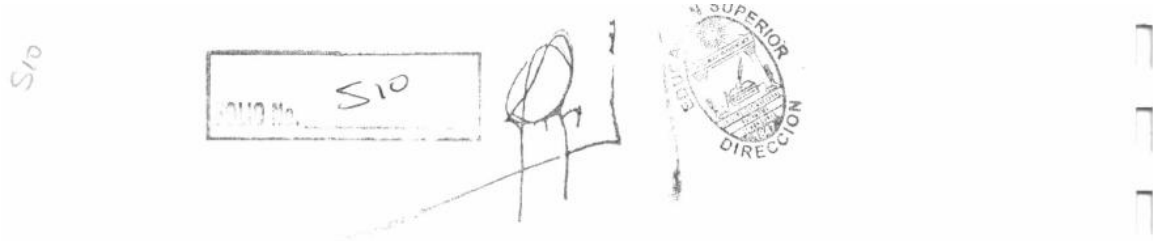
Código: **DIA-320**
Nombre del espacio de aprendizaje: **SEGURIDAD INFORMÁTICA I**
Facultad: **CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES**
Departamento responsable: **INFORMÁTICA**
Carrera según grado: **LICENCIATURA EN INFORMATICA ADMINISTRATIVA**
Requisitos del espacio de aprendizaje (código, nombre y créditos): 1. **DIA-199 POLÍTICAS PÚBLICAS Y GOBIERNO DE TI 4 CA** 2. **DIA-179 REDES DE COMPUTADORAS II 4 CA**

Modalidad en la que se presenta el proceso de aprendizaje:
1. Presencial Con el apoyo al uso de herramientas virtuales.

Distribución de la actividad académica del Espacio de Aprendizaje		
Total de Créditos: **4**	Número de semanas: **15** Horas Teóricas: **30** Horas Prácticas: **30**	Número de horas teóricas: **30** Número de horas prácticas: **30** Horas de trabajo independiente del estudiante en la semana: **8** Horas de trabajo independiente del estudiante en el periodo: **120**

Descripción del espacio de aprendizaje (Naturaleza y propósito):
La seguridad informática, es el área de las tecnologías de la información que se enfoca en la protección de tu infraestructura computacional para aminorar los ataques maliciosos que pudieran poner en peligro no solamente la operación, sino activos, empleados, información confidencial e inclusive la existencia del propio negocio si se trata de un robo. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas concebidas para minimizar los posibles riesgos.

505



Capacidades previas (conocimientos, habilidades, destrezas, valores adquiridos por los estudiantes):
Este espacio de aprendizaje se encuentra ubicada después de cursar más de la mitad de la carrera para logran tener en el estudiante la capacidad de tener el conocimiento necesario sobre los componentes computacionales y así poder comprender como se transmiten y comunican las redes. • Manejo básico de un sistema operativo de consola a nivel de comandos y de interfaz gráfico. • Manejo y manipulación básica del hardware y software del computador. • Experiencias y conocimiento en recabar la información con exploradores y motores de búsqueda. • Conocimientos y habilidades básicas de programación, bases de datos, redes y sistemas operativos. • Algunas prácticas relacionadas al uso y manejo de las TIC.

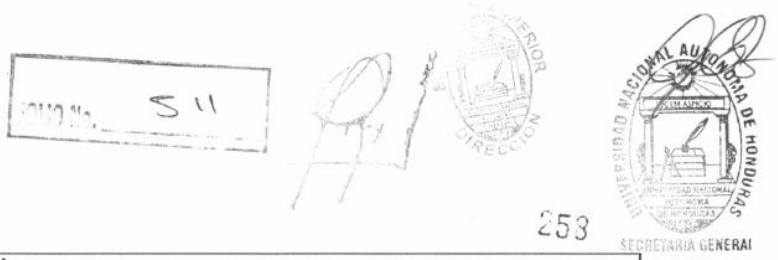
- Identifica y aplica conceptos fundamentales de redes, programación, bases de datos y sistemas operativos.
- Manejo de metodologías para el análisis de sistemas de información.
- Utiliza normas y estándares de la industria para diseñar e integrar soluciones dentro de las organizaciones y lograr la optimización de recursos existentes.
- Conocimiento y habilidades de diseño y planeación de centro de datos lógicos y virtuales.
- Conocimientos básicos de los tipos de amenazas a los sistemas y los daños que estos podrían causar.
- Conocimientos básicos de los equipos y software de protección y diagnostico

Ejes Curriculares Transversales:

El modelo educativo de la UNAH establece que el aprendizaje se fundamente en cuatro ejes curriculares:

1. Los objetivos de desarrollo sostenible y reducción de la pobreza
2. Violencia, vulnerabilidad y riesgo
3. Ética y bioética
4. Condiciones y calidad de vida

506



Desarrollo sostenible:

El espacio de aprendizaje proporciona herramientas de software para que el estudiante pueda diseñar e implementar sistemas muy semejantes a las que nos rodean en el campo laboral. Al conocer de los diferentes equipos seguridad que se utilizan en los sistemas informáticos podrán lograr ayudar en el resguardo de información valiosa para los usuarios y la empresa. Todas estas prácticas mejoran el conocimiento y aprendizaje significativo en el estudiante además de que reducen los costos en la compra de equipo y software.

Violencia, vulnerabilidad y riesgo:

Este espacio de aprendizaje se basa en la seguridad para minimizar las vulnerabilidades y riesgos de intrusión o ataques a nuestros sistemas. Bajo esa premisa podemos afirmar que la seguridad en los sistemas sí contribuye al sostenimiento óptimo de las empresas, que depende del buen funcionamiento y sobre todo que los sistemas sean seguras tanto para los intereses de las organizaciones como para la confianza de los usuarios que requieren que estén disponibles los sistemas y que no sean violados o vulnerados.

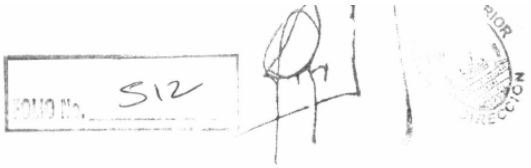
Ética:

La sociedad y las empresas buscan personas éticas con valores morales, cada una de las asignaturas de la Carrera de Informática Administrativa inculca y recalca en sus estudiantes la importancia de hacer su trabajo de la mejor manera teniendo como parte fundamenta la ética. En esta clase se da al estudiante las habilidades y conocimientos de monitorear y asegurar los datos transmitidos con la mayor transparencia, seguridad e integridad para el beneficio de la sociedad.

Condiciones y calidad de vida:

Cada estudiante tiene que finalizar la carrera con la habilidad de aportar a la sociedad soluciones y con este espacio de aprendizaje esas soluciones van orientadas a identificar las necesidades en cuanto a los requerimientos en seguridad tanto sea para crear, mejorar, reorganizar o prevenir mediante políticas, equipo y software. Cada área que deba tomar será siempre para obtener los mejores resultados de su gestión.

Competencias generales:



1. Capacidad de abstracción, análisis y síntesis.
2. Capacidad para trabajar en equipo Multidisciplinar e Interdisciplinar.
3. Capacidad de aplicar los conocimientos en la práctica y de generar conocimiento a partir de reflexionar sobre la práctica.
4. Habilidad de gestión y aplicación del conocimiento, la información y las tecnologías para contribuir a la solución de problemas y atención de necesidades de diferentes niveles de complejidad.

Competencias específicas:

1. Identifica el lenguaje técnico de Seguridad Informática.
2. Actualiza los sistemas operativos, aplicaciones y herramientas de protección que se necesitan en la organización.
3. Evalúa protocolos y herramientas de software y hardware para la protección de los sistemas.

4. Planifica y acondiciona los sistemas de información para disminuir las vulnerabilidades que provocan los daños a la integridad de los equipos que forman parte de los procesos sistematizados de la empresa o institución.

Sub-competencias:

1. Conoce el software encargado de la protección de los sistemas de información.
2. Conoce los dispositivos de hardware necesarios para la protección de los sistemas de informacion.
3. Actualiza los sistemas operativos y software que se necesiten en la organización.
4. Evalúa los protocolos de seguridad necesarios para la correcta aplicación en los sistemas de información.
5. Selecciona herramientas de software y hardware que se utilizarán para la protección ante inminentes amenazas.

Áreas temáticas (unidades de aprendizaje o bloques):

I Unidad

513

259

1.1 Conceptos de seguridad informática

1.2 Introducción a la criptografía

II Unidad

2.1 Análisis de vulnerabilidades en base de datos, lenguaje de programación y sistemas operativos

2.2 Protección al tráfico de redes

III Unidad

3.1 Análisis del malware

3.2 Administración de riesgo y prueba de vulnerabilidad

Estrategias Metodológicas de aprendizaje-enseñanza:

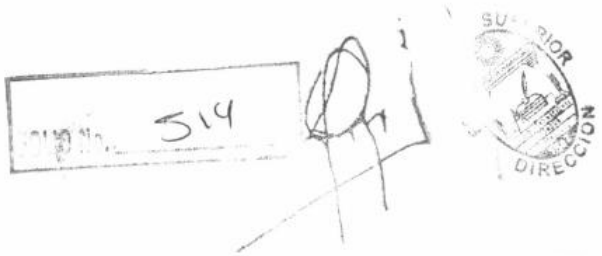
Según la naturaleza del curso, los métodos que se pueden utilizar, entre otros son:

- Uso de herramientas de software de simulación virtual, realidad aumentada, gamificación y equipo real.
- Participación en el campus virtual (pruebas, foros, entrega de actividades, conferencias y otros).
- Análisis y solución de problemas dentro y fuera del espacio de aprendizaje.
- Resolución de guías de estudios, ejercicios, resúmenes y otros.
- Discusión de casos mediante el aprendizaje cooperativo y colaborativo.
- Practicas con equipo real, simulando fallas, realizando instalación, configurando, aplicando la seguridad y realizando respaldo.

Logros de Aprendizajes:

Al finalizar este espacio de aprendizaje el estudiante:

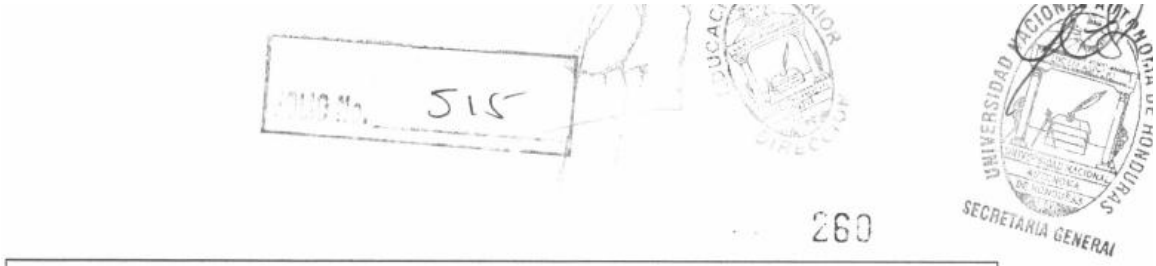
1. Explica el software encargado de la protección de equipo computacional.
2. Maneja el software apropiado para proteger equipo computacional.
3. Aplica el software de actualización de sistemas operativos.



4. Aplica actualizaciones de software.
5. Evaluará los protocolos de seguridad.
6. Determinará las herramientas de software y hardware para la protección ante inminentes amenazas.
7. Informes de las configuraciones, reportes y rendimientos de los equipos de seguridad.
8. Informe de la configuración de los dispositivos para optimizar el rendimiento y priorizar la seguridad en los servicios.
9. Informa sobre las diferentes pruebas de vulnerabilidad y administración de riesgo.
10. Archivo ejecutable donde se aprecia la correcta configuración del software y hardware.
11. Explica los protocolos de seguridad.

Estrategias de evaluación de los aprendizajes (Diagnóstica, Formativa, Sumativa):
El sistema de evaluación del aprendizaje comprende: **EVALUACIÓN DIAGNÓSTICA** Se realizará en la primera semana de clases mediante; una prueba de conocimientos en línea o en el aula de clases, aplicación de instrumento, una lista de chequeo competencias previas y otras actividades que el profesor considere pertinentes. **EVALUACIÓN FORMATIVA** Durante el desarrollo del espacio de aprendizaje, se evaluarán los logros obtenidos en el nivel conceptual, práctico, analítico, síntesis e interpretación mediante: Solución de problemas, elaboración de informes, participación de foros virtuales, resolución de casos, desarrollo de trabajo colaborativo y cooperativo. **EVALUACIÓN SUMATIVA** Se realizarán 3 exámenes por cada unidad de aprendizaje tal como se dispone en los calendarios de aplicación de examen parcial de la Facultad de Ciencias Económicas Administrativas y Contables.

510



Actividades de Aprendizaje	Criterio de Evaluación	Puntaje asignado
Foros Actividades	• Matriz de Valoración o Rúbricas de Evaluación • Lista de Cotejo	20%
Tareas	• Matriz de Valoración o Rúbricas de Evaluación	10%
Casos simulados	• Lista de chequeo • Matriz de Valoración o Rúbricas de Evaluación	10%

Avances de proyectos	• Guía de evaluación de Proyectos	30%
Cuestionarios en Moodle - Control de lectura	• Pruebas de Desempeño	5%
Pruebas objetivas	• Pruebas de Desempeño	25%

Referencias bibliográficas sugeridas:

a) **Básicas**

- Roa Buendía, J. F. (2013). *Seguridad Informática*. Madrid: McGraw-Hill.
- Erickson, J. (2009). Hacking técnicas fundamentales. Madrid: Anaya Multimedia
- Hadnagy, C. (2011) Ingeniería social el arte del hacking personal. Madrid: Anaya Multimedia
- Gómez Vieites, A. (2013) Seguridad en equipos informáticos. Bogotá: Ediciones de la U.
- Ribagorda Garnacho, A. y Ramos Álvarez, B. (2004) Avances en criptología y seguridad de la información. Ediciones Diaz de Santos.

b) **Complementarias**

- Rego, M. (2018) Un llamado a la acción para proteger ciudadanos sector privado y gobierno. Recuperado de http://www.oas.org/es/sms/cicte/awswhitepaper.pdf
- Peso Navarro, E., Ramos González, M. (2004) El documento de seguridad: análisis técnico y jurídico. Modelos. Ediciones Diaz de Santos.
- Dante, M. (2012). Administración de storage y backups. Madrid: AlfaOmega.

Recursos adicionales (revistas, páginas web, vídeos, películas, otros):

- Revista Forbes.
- Revista PC World.
- Revista de ciencia y tecnología Cuervo Blanco.
- Revista ComputerHoy.
- Revista Tecnología, Ciencia y Educación.
- Sito web del Sistema de Observación y Prospectiva Tecnológica.
- Sitio web de Ciencia, tecnología y sectores de producción, ONU.
- Sitio web de la Comisión de las Naciones Unidas en ciencia y tecnología para el desarrollo (CSTD).
- Revista El Economista sección de tecnología.
- Canal de Apple en youtube.

DIA 331 SEGURIDAD INFORMÁTICA II

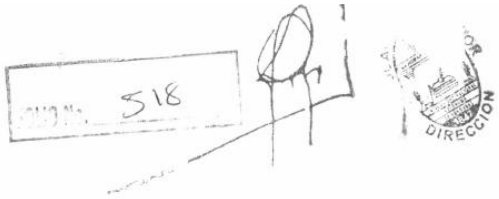
DIA-331 Seguridad Informática II 261

UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS
VICERRECTORÍA ACADÉMICA - DIRECCIÓN DE DOCENCIA
DESCRIPCIÓN MÍNIMA DE ESPACIOS DE APRENDIZAJE

Código: **DIA-331**
Nombre del espacio de aprendizaje: **SEGURIDAD INFORMATICA II**
Facultad: **CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES**
Departamento responsable: **INFORMÁTICA**
Carrera según grado: **LICENCIATURA EN INFORMATICA ADMINISTRATIVA**
Requisitos del espacio de aprendizaje (código, nombre y créditos): 1. **DIA-320 SEGURIDAD INFORMATICA I** **4 CA**

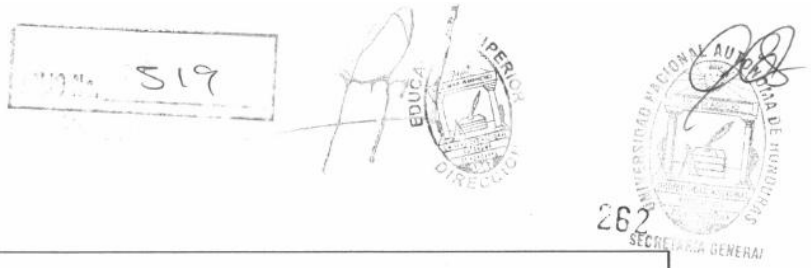
Modalidad en la que se presenta el proceso de aprendizaje:		
1. Presencial Con el apoyo al uso de herramientas virtuales.		☐
Distribución de la actividad académica del Espacio de Aprendizaje:		
Total de Créditos: **4**	Número de semanas: **15** Horas Teóricas: **30** Horas Prácticas: **30**	Número de horas teóricas: **30** Número de horas prácticas: **30** Horas de trabajo independiente del estudiante en la semana: **8** Horas de trabajo independiente del estudiante en el periodo: **120**
Descripción del espacio de aprendizaje (Naturaleza y propósito):		
Las organizaciones dependen más cada dia de la plataforma tecnológica. Se vuelve necesario emprender estrategia de continuidad del negocio eliminando las vulnerabilidades que pueden afectar las tecnologías de la información y afectar la operación de la organización. Dentro de este espacio de aprendizaje se harán prueba ética de penetración para vulnerar la seguridad de los sistemas, para que pueda realizarse un plan, lista de acceso, y políticas para mejorar la perspectiva de la empresa frente a esas amenazas.		

513



Capacidades previas (conocimientos, habilidades, destrezas, valores adquiridos por los estudiantes):
• Manejo de conceptos básicos en seguridad informática. • Conocimientos y habilidades básicas de programación, bases de datos, redes y sistemas operativos. • Utiliza pruebas de vulnerabilidad para lograr la optimización de sistemas de información. • Diseño y planeación de centro de datos lógicos y virtuales. • Manejo de las técnicas de cifrado para prevenir los distintos tipos de amenazas en los sistemas. • Identifica y aplica conceptos fundamentales de criptografía. • Manejo básico de los conceptos de seguridad Informatica. • Manejo de las pruebas de vulnerabilidad más comunes. • Experiencias y conocimiento en recabar la información con exploradores y motores de búsqueda. • Algunas prácticas relacionadas al uso y manejo de las TIC.

• Monitoreo de tráfico de datos en las redes.
Ejes Curriculares Transversales:
En el contexto de los ejes curriculares del modelo educativo de la UNAH este espacio de aprendizaje se fundamentará en: 1. Los objetivos de desarrollo sostenible y reducción de la pobreza 2. Violencia, vulnerabilidad y riesgo 3. Ética y bioética 4. Condiciones y calidad de vida **Desarrollo sostenible:** El espacio de aprendizaje proporciona herramientas de software para que el estudiante pueda diseñar e implementar sistemas seguros muy semejantes a las que nos rodean en el campo laboral. Al conocer de los diferentes equipos seguridad que se utilizan en los sistemas informáticos podrán lograr ayudar en el resguardo de información valiosa para los usuarios y la empresa. Todas estas prácticas mejoran el conocimiento y aprendizaje significativo en el estudiante además de que reducen los costos en la compra de equipo y software.



Violencia, vulnerabilidad y riesgo:
Este espacio de aprendizaje se basa en la seguridad para minimizar las vulnerabilidades y riesgos de intrusión o ataques a nuestros sistemas. Bajo esa premisa podemos afirmar que la seguridad en los sistemas sí contribuye al sostenimiento óptimo de las empresas, que depende del buen funcionamiento y sobre todo que los sistemas sean seguras tanto para los intereses de las organizaciones como para la confianza de los usuarios que requieren que estén disponibles los sistemas y que no sean violados o vulnerados.

Ética:
La sociedad y las empresas buscan personas éticas con valores morales, cada una de las asignaturas de la Carrera de Informática Administrativa inculca y recalca en sus estudiantes la importancia de hacer su trabajo de la mejor manera teniendo como parte fundamenta la ética. En esta clase se da al estudiante las habilidades y conocimientos de monitorear y asegurar los datos transmitidos con la mayor transparencia, seguridad e integridad para el beneficio de la sociedad.

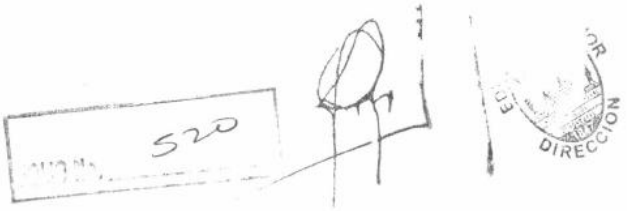
Condiciones y calidad de vida:
Cada estudiante tiene que finalizar la carrera con la habilidad de aportar a la sociedad soluciones y con este espacio de aprendizaje esas soluciones van orientadas a identificar las necesidades en cuanto a los requerimientos en seguridad tanto sea para crear, mejorar, reorganizar o prevenir mediante políticas, equipo y software. Cada área que deba tomar será siempre para obtener los mejores resultados de su gestión.

Competencias generales:

1. Capacidad de abstracción, análisis y síntesis.
2. Capacidad para trabajar en equipo multidisciplinar e interdisciplinar.
3. Habilidad de gestión y aplicación del conocimiento, la información y las tecnologías para contribuir a la solución de problemas y atención de necesidades de diferentes niveles de complejidad.

Competencias específicas:

1. Desarrolla la planeación estratégica orientada a la protección de datos y equipos, de



acuerdo con las necesidades de la organización.

2. Elabora un plan de respuesta a incidentes de seguridad, atender notificaciones de sospecha de ciberataque y documentar dichos incidentes.
3. Utiliza herramientas para realizar pruebas de penetración, Ethical Hacking y análisis de malware.
4. Utiliza estándares de la industria para mantener la protección de los equipos y los datos.
5. Aplica nuevas tecnologías y métodos de la ciencia del análisis forense digital

Sub-competencias:

1. Desarrolla un plan estratégico para la protección de los sistemas computacionales de la organización.
2. Establece políticas para el acceso de los usuarios internos y externos de la organización.
3. Establece misión y metas internas en cuanto a la seguridad de la información.
4. Aplica el estándar ISO 27002 en cada uno de los componentes del sistema de información de la organización.
5. Lleva a cabo una rutina de monitoreo de los accesos de los usuarios a aplicaciones o servidores dentro y fuera de la organización.
6. Elabora un plan de respuestas a incidentes de seguridad, con la finalidad de ofrecer una respuesta rápida que sirva para la investigación del evento, a fin de asegurar la continuidad del negocio y para la corrección del proceso mismo.
7. Atiende y responde inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
8. Crea una base de datos para el registro de incidentes en la red, la cual puede ser

accedida por cualquier miembro del área.

Áreas temáticas (unidades de aprendizaje o bloques):

I UNIDAD

a. Ethical Hacking y análisis de malware
b. Pruebas de penetración (Pentest)

II UNIDAD

a. ISO 27002 (Controles de seguridad, políticas, organización, recursos humanos, activos, accesos, cifrado, física y ambiental, operativa, telecomunicaciones, incidentes, continuidad del negocio, cumplimiento.)
b. Plan estratégico de SI

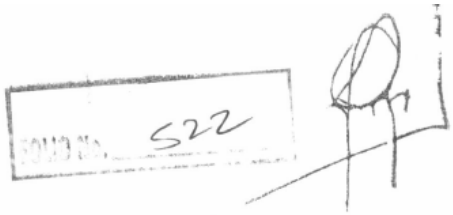
III UNIDAD

a. Análisis de riesgos y continuidad del negocio
b. Análisis forense y delitos informáticos

Estrategias Metodológicas de aprendizaje-enseñanza:

Según la naturaleza del curso, los métodos que se pueden utilizar, entre otros son:

- Uso de herramientas de software de simulación virtual, realidad aumentada, gamificación y equipo real.
- Participación en el campus virtual (pruebas, foros, entrega de actividades, conferencias y otros).
- Análisis y solución de problemas dentro y fuera del espacio de aprendizaje.
- Resolución de guías de estudios, ejercicios, resúmenes y otros.
- Discusión de casos mediante el aprendizaje cooperativo y colaborativo.
- Prácticas con equipo real, simulando fallas, realizando instalación, configurando, aplicando la seguridad y realizando respaldo.



Logros de Aprendizajes:

Al finalizar este espacio de aprendizaje el estudiante:

1. Explica el software encargado de la protección de equipo computacional.
2. Maneja el software apropiado para proteger equipo computacional.
3. Aplica el software de actualización de sistemas operativos.
4. Aplica actualizaciones de software.
5. Evalúa los protocolos de seguridad.
6. Determina las herramientas de software y hardware para la protección ante inminentes amenazas.
7. Construye un informe de las configuraciones, reportes y rendimientos de los equipos de seguridad.
8. Construye un informe de la configuración de los dispositivos para optimizar el rendimiento y priorizar la seguridad en los servicios.
9. Construye un informe sobre las diferentes pruebas de vulnerabilidad y administración de riesgo.
10. Construye un archivo ejecutable donde se aprecia la correcta configuración del software y hardware.
11. Explica los protocolos de seguridad

Estrategias de evaluación de los aprendizajes (Diagnóstica, Formativa, Sumativa):

El sistema de evaluación del aprendizaje comprende:

EVALUACIÓN DIAGNÓSTICA

Se realizará en la primera semana de clases mediante; una prueba de conocimientos en línea o en el aula de clases, aplicación de instrumento, una lista de chequeo competencias previas y otras actividades que el profesor considere pertinentes.

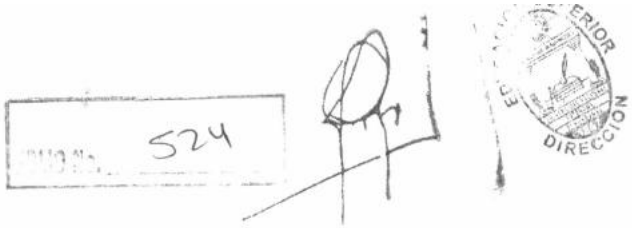
EVALUACIÓN FORMATIVA

Durante el desarrollo del espacio de aprendizaje, se evaluarán los logros obtenidos en el nivel conceptual, práctico, analítico, síntesis e interpretación mediante: Solución de problemas, elaboración de informes, participación de foros virtuales, resolución de casos, desarrollo de trabajo colaborativo y cooperativo.

EVALUACIÓN SUMATIVA

Se realizarán 3 exámenes por cada unidad de aprendizaje tal como se dispone en los calendarios de aplicación de examen parcial de la Facultad de Ciencias Económicas Administrativas y Contables.

Actividades de Aprendizaje	Criterio de Evaluación	Puntaje asignado
Foros Actividades	• Matriz de Valoración o Rúbricas de Evaluación. • Lista de Cotejo	20%
Tareas	• Matriz de Valoración o Rúbricas de Evaluación	10%
Casos simulados	• Lista de chequeo • Matriz de Valoración o Rúbricas de Evaluación	10%
Avances de proyectos	• Guía de evaluación de Proyectos	30%
Cuestionarios en Moodle - Control de lectura	• Pruebas de Desempeño	5%
Pruebas objetivas	• Pruebas de Desempeño	25%



Referencias bibliográficas sugeridas:

a) Básicas

- Calder, A., & Watkins, S. (2008). *IT Governance a manager's guide to Data Security and ISO 27001/ISO27002/ISO22301*.
- COBIT. (2019). *IT Governance Instituto COBIT 5*. Recuperado de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx
- Fisher, R.P. (1998). *Seguridad en los sistemas informáticos*. España: Ediciones Díaz de Santos.
- Fuster, A, Muñoz, J. Hernández, L., Martín, A. y Montoya, F. (2012). *Criptografía, protección de datos y aplicaciones*. Madrid: Alfaomega.
- Sallis, E., Caracciolo, C. y Rodríguez, M. (2012). *Ethical hacking - Un enfoque metodológico para profesionales*. Madrid: Alfaomega.
- Cano, J. (2015). *Computación forense - Descubriendo los Rastros Informáticos*. Madrid: Alfaomega.

b) Complementarias

- Seoane Ruano, C., Saiz Herrero, A. B., Fernández Álvarez, E., & Fernández Aranda, L. (2010). *Seguridad informática*. Madrid: McGraw-Hill/Interamericana de España, S.L.
- Gómez, Á. (2011). *Enciclopedia de la seguridad informática*. Madrid: AlfaOmega.
- Cano, J. (2012). *Inseguridad de la información - Una visión estratégica*. Madrid: AlfaOmega.

Recursos adicionales (revistas, páginas web, vídeos, películas, otros):

Whitepaper: OEA, Un llamado a la acción para proteger a ciudadanos sector privado y público (2018), http://www.oas.org/es/sms/cicte/awswhitepaper.pdf

- Revista Forbes.
- Revista PC World.

- Revista de ciencia y tecnología Cuervo Blanco.
- Revista ComputerHoy.
- Revista Tecnología, Ciencia y Educación.
- Sito web del Sistema de Observación y Prospectiva Tecnológica.
- Sitio web de Ciencia, tecnología y sectores de producción, ONU.
- Sitio web de la Comisión de las Naciones Unidas en ciencia y tecnología para el desarrollo (CSTD).
- Revista El Economista sección de tecnología.
- Canal de Apple en youtube.

UNAH

UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS