ASIGNATURA DE INFORMÁTICA FORENSE

1. Competencias	Diseñar y optimizar soluciones de redes digitales, a través, de la administración y dirección de proyectos tecnológicos, alineados a normas y estándares vigentes, para contribuir a la continuidad del negocio.
2. Cuatrimestre	Décimo
3. Horas Teóricas	33
4. Horas Prácticas	42
5. Horas Totales	75
6. Horas Totales por Semana Cuatrimestre	5
7. Objetivo de aprendizaje	El alumno evaluará metodologías y herramientas de informática forense apegado a normas y estándares nacionales e internacionales para contribuir en la continuidad del negocio en las organizaciones.

Unidades de Aprendizaje	**Horas**		
	Teóricas	**Prácticas**	**Totales**
I. Introducción a la informática forense	6	9	15
II. Metodologías para la investigación en informática forense	10	15	25
III. Técnicas y herramientas para el análisis forense	8	12	20
IV. Legislación y regulación en Informática forense	9	6	15
Totales	**33**	**42**	**75**

INFORMÁTICA FORENSE

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Introducción a la informática forense**
2. Horas Teóricas	6
3. Horas Prácticas	9
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno identificará los conceptos y elementos generales de informática forense para comprender la importancia del establecimiento de una estrategia de negocio ante delito cibernético.

Temas	Saber	Saber hacer	Ser
Tópicos de Informática Forense	Definir el concepto de Informática Forense. Definir el concepto de Delito Cibernético. Definir los tipos de Delito Cibernético. Identificar los actores y las funciones del personal involucrado en la investigación de delitos cibernéticos.	Clasificar los tipos de delitos cibernéticos.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.
Sistemas de Archivos	Distinguir las características de los diferentes tipos de sistemas de archivos. Comparar los diferentes tipos de sistemas de archivos.	Diagnosticar la estructura de los diferentes tipos de sistema de archivos	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.

Tipos de datos y su almacenamiento	Identificar las características especificas (tamaño, codificación, estructura) de las diferentes categorías de datos. Identificar las características de los diferentes medios de almacenamiento.	Documentar la estructura del almacenamiento de datos.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.

INFORMÁTICA FORENSE

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elabora y presenta un informe técnico, a partir de un caso de estudio, que incluya lo siguiente: -Estadísticas sobre los ataques cibernéticos, por categoría, más recurrentes en los últimos 4 años. -Descripción de las funciones específicas de los actores involucrados en la investigación de un delito cibernético. -Cuadro comparativo con las características principales y la estructura de los diferentes tipos de sistemas de archivos. -Descripción de la estructura física y lógica de un esquema de almacenamiento, contemplando diversos tipos de medios de almacenamiento.	1. Explicar los conceptos generales de Informática forense 2. Explicar las funciones específicas de los actores involucrados en la investigación de un delito cibernético 3. Identificar las características principales y la estructura de los diferentes tipos de sistemas de archivos 4. Identificar la estructura física y lógica de los esquemas de almacenamiento.	1. Estudio de caso 2. Lista de cotejo

INFORMÁTICA FORENSE

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo. -Software Especializado. -Proyector. -Internet. -Pintarrón.

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
.	**X**	

INFORMÁTICA FORENSE

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**II. Metodologías para la investigación en informática forense**
2. Horas Teóricas	10
3. Horas Prácticas	15
4. Horas Totales	25
5. Objetivo de la Unidad de Aprendizaje	El alumno determinará las metodologías adecuadas para el manejo de evidencia digital que permitan la elaboración de reportes de análisis forense.

Temas	Saber	Saber hacer	Ser
Metodologías para recolección, preservación y aseguramiento de la evidencia digital	Identificar los elementos básicos de la cadena de custodia de evidencias digitales. Identificar las etapas del procedimiento de cadena de custodia para la preservación de evidencia digital. Identificar estándares para la localización, recolección, preservación y aseguramiento de evidencia digital. Identificar las etapas del proceso de recolección de evidencia digital. Identificar las mejores prácticas de aseguramiento de evidencia digital. Identificar las técnicas para la preservación de evidencia digital.	Implementar las mejores prácticas para la identificación, recolección, preservación y aseguramiento de evidencia digital establecidas en el estándar ISO/IEC 27037. Obtener evidencia digital derivada de delitos cibernéticos. Mapear las etapas de la cadena de custodia de evidencias digitales. Establecer planes de acción para el aseguramiento de evidencias digitales. Implementar técnicas para la recolección de evidencia digital. Implementar técnicas de preservación de evidencia digital.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.

Metodologías para el análisis de la evidencia digital	Identificar estándares para la interpretación de evidencia digital. Enumerar las etapas del proceso de análisis de evidencia digital.	Implementar las mejores prácticas para el análisis de evidencia digital establecidas en el estándar ISO/IEC 27042. Ejecutar el protocolo para el análisis de evidencia digital. Preparar el entorno de trabajo para el análisis de evidencia digital. Implementar técnicas para el análisis de evidencia digital. Evaluar el impacto generado en la infraestructura informática derivado de un delito cibernético.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Documentación y redacción de reportes de Informática Forense	Identificar estándares para la interpretación de evidencia digital. Identificar los elementos básicos que integran un informe técnico de análisis forense. Identificar los elementos básicos que integran un informe ejecutivo de análisis forense. Explicar los elementos básicos de un informe técnico de análisis forense. Explicar los elementos básicos de un informe ejecutivo de análisis forense	Documentar los resultados de un análisis forense. Elaborar informes técnicos de análisis forense. Elaborar informes ejecutivos de análisis forense.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

INFORMÁTICA FORENSE

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elabora y presenta un informe técnico y ejecutivo, a partir de un caso de estudio, que incluya lo siguiente: -Descripción del procedimiento de cadena de custodia de la evidencia digital bajo normas y estándares. -Descripción de la metodología de análisis forense utilizada para la obtención de evidencia digital bajo normas y estándares. -Proceso de Implementación de las normas y estándares utilizados en la documentación y redacción de reportes de Informática Forense	1. Explicar la metodología para recolección, preservación y aseguramiento de la evidencia digital basado en normas y estándares. 2. Explicar el procedimiento de cadena de custodia de la evidencia digital basado en normas y estándares. 3. Explicar la metodología de análisis forense de evidencia digital. 4. Aplicar las normas y estándares utilizados en la documentación y redacción de reportes de Informática Forense.	1. Estudio de caso. 2. Lista de cotejo.

INFORMÁTICA FORENSE

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo. -Software Especializado. -Proyector. -Internet. -Pintarrón.

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

INFORMÁTICA FORENSE

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**III. Técnicas y herramientas para el análisis forense**
2. Horas Teóricas	8
3. Horas Prácticas	12
4. Horas Totales	20
5. Objetivo de la Unidad de Aprendizaje	El alumno evaluará herramientas de análisis forense para la resolución de incidentes derivados del delito cibernético.

Temas	Saber	Saber hacer	Ser
Peritaje informático	Identificar estándares y normas aplicables al peritaje informático. Identificar herramientas para el peritaje informático. Enumerar las etapas del proceso de peritaje informático.	Documentar los hallazgos derivados del proceso de peritaje informático.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.
Herramientas de Informática Forense	Identificar herramientas para el análisis forense. Describir las características de las herramientas de análisis forense.	Preparar el entorno de trabajo para el análisis forense. Implementar herramientas para el análisis forense.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.

INFORMÁTICA FORENSE

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elabora y presenta un informe técnico y ejecutivo, a partir de un caso de estudio, que incluya lo siguiente: -Descripción del proceso de peritaje informático -Descripción de la implementación de las herramientas de peritaje informático pertinentes al caso de estudio bajo normas y estándares. -Descripción de los hallazgos derivados del proceso de peritaje informático bajo normas y estándares .-Implementación de las normas y estándares utilizados en la documentación y redacción de reportes de Informática Forense	1. Explicar el proceso de peritaje informático 2. Analizar las herramientas de peritaje informático 3. Analizar los hallazgos derivados del proceso de peritaje informático bajo normas y estándares.	1. Estudio de caso 2. Lista de cotejo

INFORMÁTICA FORENSE

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo. -Software Especializado. -Proyector. -Internet. -Pintarrón.

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

INFORMÁTICA FORENSE

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**IV. Legislación y regulación en informática forense**
2. Horas Teóricas	9
3. Horas Prácticas	6
4. Horas Totales	15
5.Objetivo de la Unidad de Aprendizaje	El alumno evaluará la importancia de la legislación y regulación aplicable a los delitos cibernéticos para la adecuada elaboración de planes de recuperación.

Temas	Saber	Saber hacer	Ser
Normas y estándares nacionales e internacionales sobre Informática Forense.	Identificar estándares internacionales aplicables en informática forense. Identificar estándares para la regulación y gobernanza en informática forense.		Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico
Legislación nacional e internacional acerca de delito cibernético.	Identificar el marco regulatorio nacional aplicable al delito cibernético. Identificar el marco regulatorio internacional aplicable al delito cibernético.	Documenta las leyes y sanciones aplicables a delitos cibernéticos específicos.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico

Manejo de incidentes	Identificar normas y estándares para el manejo de incidentes derivados de delitos cibernéticos. Identificar protocolos para el manejo de incidentes derivados de delitos cibernéticos. Identificar los elementos que integran un Plan de Recuperación ante Desastres (DRP).	Elabora planes de recuperación ante desastres ocasionados por delitos cibernéticos.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador. Hábil para interpretar información. Ético. Trabajo en equipo. Metódico.

INFORMÁTICA FORENSE

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elabora y presenta un informe, a partir de un caso de estudio, que incluya lo siguiente: -Resumen de las leyes y sanciones aplicables a delitos cibernéticos específicos. -Descripción de las funciones específicas de los actores involucrados en las leyes y sanciones aplicables a delitos cibernéticos específicos. -Cuadro comparativo con las leyes y sanciones aplicables a delitos cibernéticos específicos. -Plan de recuperación ante desastres ocasionados por delitos cibernéticos específicos.	1. Identificar las normas, estándares nacionales e internacionales aplicables a Informática Forense para la regulación y gobernanza de datos. 2. Comprender las leyes y sanciones aplicables a delitos cibernéticos específicos. 3. Realizar planes de recuperación ante desastres ocasionados por delitos cibernéticos.	1. Estudio de caso. 2. Lista de cotejo.

INFORMÁTICA FORENSE

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo. -Software Especializado. -Proyector. -Internet. -Pintarrón.

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

INFORMÁTICA FORENSE

CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA

Capacidad	Criterios de Desempeño
Diagnosticar riesgos y vulnerabilidades en la seguridad de información a partir del análisis del entorno de las organizaciones, para desarrollar estrategias que permitan su mitigación.	Entrega un reporte técnico que incluya lo siguiente: -Análisis del contexto del negocio. -Listado requerimientos funcionales y no funcionales. -Análisis de la situación actual de la seguridad de información de la organización.
Establecer políticas de seguridad de información mediante estándares y procedimientos vigentes aplicables al entorno de la organización, para establecer las bases de continuidad de negocio.	Entrega un documento con la política de seguridad de información que considere los siguientes puntos: -Matriz de riesgos y vulnerabilidades. -Procesos de continuidad del negocio. -Políticas de salvaguarda de los activos de la organización. -Identificación y clasificación de los activos de la organización.
Seleccionar herramientas y servicios para la seguridad de información mediante la aplicación de estándares, para dar cumplimiento a las políticas de seguridad de las organizaciones.	Entrega una propuesta de solución que incluye lo siguiente: - Tabla comparativa de la evaluación de alternativas de solución. - Arquitectura de la solución propuesta. - Análisis del retorno de la inversión. - Hoja técnica de la solución propuesta.
Planear las estrategias de implementación de políticas, herramientas y servicios de seguridad de información a partir del análisis del entorno, para salvaguardar los activos de las organizaciones.	Entrega un plan de trabajo que incluye lo siguiente: - Actividades a desarrollar. - Responsables. - Tiempos asignados a cada tarea.
Implementar las soluciones de seguridad de información, a partir de los lineamientos organizacionales y en apego a los procedimientos y estándares aplicables a las tecnologías seleccionadas, para salvaguardar los activos de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: - Línea base del servicio. - Bitácora de implementación. - Pruebas de la implementación.

Evaluar la implementación de soluciones de seguridad de información mediante la aplicación de auditorías, pruebas e interpretación de métricas, para determinar áreas de oportunidad en los procesos de continuidad de negocio.	Entrega un reporte de auditoria de seguridad que incluye los siguiente: - Resultados de pruebas de penetración. - Análisis de vulnerabilidades. - Propuesta de mejoras a la política de seguridad de la organización.
Monitorear la implementación de soluciones y políticas de seguridad de información a través del análisis de los resultados de auditorías, para optimizar los procesos de continuidad del negocio.	Entrega un reporte que incluye lo siguiente: - Bitácora de eventos. - Lista de verificación de las políticas de seguridad de la organización. - Reportes de rendimiento y eficiencia de la solución.

INFORMÁTICA FORENSE

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Francisco Lázaro Domínguez	2014 ISBN:978-84-9964-209-3	Introducción a la Informática Forense	España	España	Ra-Ma S.A.
Antonio Postigo Palacios	2020 ISBN: 9788428344555	Seguridad Informática	Madrid	España	Parainfo
Jeimy J. Cano	2009 ISBN: 978-9586827676	Computación forense: Descubriendo los rastros informáticos	Madrid	España	Alfaomega
Luis Arrellano González	2011 ISBN: 978-9870112495	Manual de Informática Forense	Madrid	España	Errepar
Herlinda Vite Pérez	2016 ISBN: 978-6076102916	Informática forense. protocolo de actuación	CDMX	México	Coordinación General de Servicios Periciales
Cory Altheide, Harlan Carvey	2011 ISBN: 978-1597495868	Digital Forensics with Open Source Tools	USA	USA	Syngress Publishing
Nipun Jaswal	2019 ISBN: 978-1789344523	Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools	Birmingham	UK	Packt Publishing

Gerard Johansen	2020 ISBN: 978-1838649005	Digital Forensics and Incident Response	Birmingham	UK	Packt Publishing
William Oettinger	2020 ISBN: 978-1838648176	Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence	Birmingham	UK	Packt Publishing
Brian Carrier	2008 ISBN-13: 978-0321268174	File System Forensic Analysis	Boston, MA.	USA	Pearson Education, Inc.
Ivan M. Hidalgo Cajo, Saul Yasaca, Luis A. Lema, Byron G. Hidalgo	2018 ISBN: 978-9942-35-2248	Informática Forense	Riobamba	Ecuador	Aval ESPOCH