


ASIGNATURA DE SISTEMAS DE CALIDAD PARA TI

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	Noveno
3. Horas Teóricas	18
4. Horas Prácticas	27
5. Horas Totales	45
6. Horas Totales por Semana Cuatrimestre	3
7. Objetivo de aprendizaje	El alumno identificará las normas y estándares de la auditoría informática aplicables a los sistemas informáticos para salvaguardar la integridad de la organización.

Unidades de Aprendizaje	Horas		
	Teóricas	Prácticas	Totales
I. Normas y estándares de calidad para TI	6	9	15
II. Auditoría informática	12	18	30
Totales	18	27	45


ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

ASIGNATURA DE HACKING ÉTICO


UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	I. Normas y estándares de calidad para TI
2. Horas Teóricas	6
3. Horas Prácticas	9
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno identificará las normas y/o estándares que apliquen a los sistemas informáticos para salvaguardar la integridad de la organización.

Temas	Saber	Saber hacer	Ser
Normas de calidad aplicables a los sistemas informáticos.	<ul style="list-style-type: none"> Identificar las características del marco de referencia COBIT. Identificar las características de CMMI. Describir la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), sus ventajas y desventajas. Definir la norma ISO 27001, sus ventajas y desventajas. Definir la norma ISO 9001, sus ventajas y desventajas. 	<ul style="list-style-type: none"> Determinar las normas aplicables para la administración de los sistemas informáticos de la organización. 	Coherente Ordenado Sistemático Hábil en el trabajo Objetivo Crítico

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


Temas	Saber	Saber hacer	Ser
Herramientas de soporte para los sistemas informáticos	<ul style="list-style-type: none"> Identificar las diferentes herramientas de soporte de los sistemas informáticos. 	<ul style="list-style-type: none"> Determinar los formatos y guías de procedimientos aplicables a los sistemas informáticos de la organización. 	Coherente Ordenado Sistemático Hábil en el trabajo Objetivo Crítico
Técnicas para la aplicación de estándares y políticas	<ul style="list-style-type: none"> Conocer los métodos de aplicación de estándares y políticas en los sistemas informáticos de la organización. 	<ul style="list-style-type: none"> Determinar los métodos de aplicación de estándares y políticas en los sistemas informáticos de la organización. 	Coherente Ordenado Sistemático Hábil en el trabajo Objetivo Crítico

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

ASIGNATURA DE HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>El alumno desarrollará un reporte técnico que incluya los siguientes elementos, aplicables a los sistemas informáticos de una organización:</p> <ul style="list-style-type: none"> • Normas de calidad aplicables a la infraestructura, desarrollo y servicios de Tecnologías de la Información. • Herramientas de soporte informático, alineadas a normas, estándares y marcos de trabajo internacionales. • Técnicas y herramientas para la validación de la correcta aplicación de estándares y políticas. 	<ol style="list-style-type: none"> 1. Analizar los tipos de normas y estándares aplicables para los sistemas informáticos. 2. Comprender las características específicas de las herramientas de soporte para los sistemas informáticos 3. Comprender la aplicación de las normas y/o estándares en función a diferentes contextos. 	<p>Lista de cotejo Rúbrica</p>

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


ASIGNATURA DE HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
Casos de Estudios Equipos Colaborativos	Equipo de Cómputo Cañón Internet Herramientas ofimáticas Material bibliográfico

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		


ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

ASIGNATURA DE HACKING ÉTICO


UNIDADES DE APRENDIZAJE

6. Unidad de aprendizaje	II. Auditoría informática
7. Horas Teóricas	12
8. Horas Prácticas	18
9. Horas Totales	30
10. Objetivo de la Unidad de Aprendizaje	El alumno identificará las fases y conceptos de la auditoría informática para salvaguardar la integridad de la organización.

Temas	Saber	Saber hacer	Ser
Conceptos básicos de auditoría informática	<ul style="list-style-type: none"> Identificar los conceptos que involucra una auditoría informática. 	<ul style="list-style-type: none"> Analizar la eficiencia de los sistemas informáticos. Determinar el cumplimiento de la normativa de la auditoría informática en la organización. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo
Licenciamiento de software	<ul style="list-style-type: none"> Identificar los diferentes tipos de licenciamientos de software y condiciones de uso. 	<ul style="list-style-type: none"> Categorizar el software presente en la organización con base en los tipos de licenciamientos existentes. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo
Evaluación de hardware y software	<ul style="list-style-type: none"> Describir la finalidad de la evaluación del hardware. Describir la finalidad de la evaluación del software. Describir la operación y seguridad del hardware y software. 	<ul style="list-style-type: none"> Determinar el nivel de aplicación de las normas y estándares consideradas en la auditoría del hardware y de software. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


Temas	Saber	Saber hacer	Ser
Evaluación de sistemas	<ul style="list-style-type: none"> • Describir las etapas para evaluar sistemas informáticos. • Explicar los elementos de la evaluación del diseño lógico 	<ul style="list-style-type: none"> • Analizar las técnicas de los sistemas informáticos de sistemas operativos, software básico, software de tiempo real, tunning, programas de desarrollo, bases de datos, administración de bases de datos. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo
Evaluación de la Red	<ul style="list-style-type: none"> • Describir los elementos de la topología física de la red. • Describir los elementos de la topología lógica de la red. • Identificar las políticas de seguridad de la red. 	<ul style="list-style-type: none"> • Evaluar la topología física y lógica de la red dentro de la organización. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo
Pruebas de penetración	<ul style="list-style-type: none"> • Explicar los tipos de pruebas de penetración activas y pasivas. • Explicar en qué consisten las pruebas de penetración de Caja Negra, Caja Gris y Caja Blanca. • Explicar en qué consisten las pruebas de penetración Internas y Externas. 	<ul style="list-style-type: none"> • Determinar los tipos de pruebas de penetración aplicables a la organización. • Proponer las fases de pruebas de penetración. 	Ordenado Sistemático Objetivo Ético Hábil para el trabajo en equipo

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

ASIGNATURA DE HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>El alumno desarrollará un dictamen de la auditoría informática que contenga los siguientes elementos:</p> <ul style="list-style-type: none"> • Áreas auditadas. • Hallazgos detectados. • Estándares utilizados en cada área de la organización. • Recomendaciones generales para la atención de cada uno de los hallazgos. • Conclusiones. 	<ol style="list-style-type: none"> 1. Comprender los hallazgos de la auditoría informática. 2. Analizar las propuestas de mejora de la auditoría. 3. Comprender las características específicas de los tipos de licenciamientos existentes de software. 4. Reconocer las normas y estándares aplicables al software y hardware. 5. Comprender las diferentes técnicas a los sistemas informáticos. 	<p>Lista de cotejo Rúbrica</p>

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


ASIGNATURA DE HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
Análisis de casos Equipos colaborativos	Equipo de Cómputo Cañón Internet Herramientas ofimáticas Ejemplos de formatos de auditoría informática.

ESPACIO FORMATIVO


Aula	Laboratorio / Taller	Empresa
X		

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


ASIGNATURA DE HACKING ÉTICO

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

Capacidad	Criterios de Desempeño
Planear proyectos de servicios e infraestructura de redes digitales a través del uso de metodologías de gestión, para definir los parámetros que lleven a la implementación de soluciones tecnológicas.	Entrega un plan de trabajo que incluye lo siguiente: <ul style="list-style-type: none"> • Definición de parámetros del proyecto. • Matriz de riesgos. • Actividades a desarrollar. • Responsables. • Tiempos asignados a cada tarea. • Plan de contingencia. • Presupuesto del proyecto (necesidades de financiamiento)
Ejecutar proyectos de servicios e infraestructura de redes digitales a través del uso de metodologías de gestión, para implementar soluciones tecnológicas que atiendan las necesidades de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: <ul style="list-style-type: none"> • Lista de verificación de los siguientes parámetros: Tiempo, recursos humanos, recursos económicos y recursos tecnológicos. • Bitácora de ejecución
Diagnosticar problemas de infraestructura y servicios lógicos de red a partir de los requerimientos de la empresa, para desarrollar estrategias que permitan su mitigación.	Entrega un reporte técnico que incluya lo siguiente: <ul style="list-style-type: none"> • Análisis del contexto del negocio. • Listado requerimientos funcionales y no funcionales. • Análisis de la situación actual de la infraestructura y servicios lógicos de red.
Determinar soluciones y servicios lógicos de red a partir de los requerimientos y recursos de la empresa, para implementar plataformas digitales de tecnologías de la información.	Entrega una propuesta de solución que incluye lo siguiente: <ul style="list-style-type: none"> • 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. • Definición de Indicadores Clave de Desempeño.
Implementar servicios lógicos de red a través de la aplicación de métricas, normas y estándares vigentes, para ofrecer soluciones en la comunicación y colaboración digital de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: <ul style="list-style-type: none"> • Planeación para la implementación. • Línea base del servicio. • Bitácora de implementación. • Pruebas de la implementación. • Hojas de estándares vigentes

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


Capacidad	Criterios de Desempeño
<p>Evaluar proyectos de servicios e infraestructura de redes digitales mediante la aplicación e interpretación de métricas, para determinar áreas de oportunidad en plataformas digitales de tecnologías de la información.</p>	<p>Entrega un reporte técnico que incluye lo siguiente:</p> <ul style="list-style-type: none"> • Análisis de información de monitoreo e incidentes. • Nivel de cumplimiento de Indicadores Clave de Desempeño.
<p>Monitorear soluciones y servicios lógicos de red mediante la aplicación de técnicas y herramientas, para controlar los parámetros establecidos.</p>	<p>Entrega reportes periódicos que incluyen lo siguiente:</p> <ul style="list-style-type: none"> • Informes de desempeño del proyecto. • Solicitudes de cambio • Estrategia de mitigación de riesgos. • Bitácora de eventos. • Propuesta de acciones de mejora. <p>Entrega Actualización del plan de desarrollo del proyecto.</p>

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


ASIGNATURA DE HACKING ÉTICO

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Mario G. Piattini Velthuis, Félix O. García Rubio, Ignacio García Rodríguez de Guzmán y Francisco J. Pino	2018	<i>Calidad de Sistemas de Información 4 edición ampliada y actualizada</i>	Madrid	España	RA-MA Editorial ISBN: 9789587629163
Zahran, Mohamed	2019	<i>Heterogeneous Computing Hardware and Software Perspectives</i>	Nueva York	Estados Unidos	ACM Books ISBN-13 : 978-1450360975
Chicano Tejada, Ester	2014	<i>Auditoria de Seguridad Informática</i>	Antequera	España	IC Editorial ISBN: 9788415457312
Gutiérrez del Mora, Leonardo	2013	<i>Curso Ciberseguridad y Hacking Ético</i>	Sevilla	España	Punto Rojo Libros, S.L ISBN-13 : 9788416068531
Mario G. Piattini Velthuis, Félix O. García Rubio, Ignacio García Rodríguez de Guzmán y Francisco J. Pino	2018	<i>Calidad de Sistemas de Información 4 edición ampliada y actualizada</i>	Madrid	España	RA-MA Editorial ISBN: 9788499647333

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

Autor	Año	Título del Documento	Ciudad	País	Editorial
Romero Castro, Martha I., Figueroa Mora, Grace L., Vera Navarrete, Denisse S. Alava Cruzatty, , Jose E., Parrales Anzules, Galo R., Alvarado Mero, Christian J., Murillo Quimiz, Angel L., Castillo Merino, Miriam A.	2018	<i>Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades</i>	Manabi	Ecuador	3Ciencias ISBN: 9788494930614

ELABORÓ:	Comité de Directores de la Carrera de Ingeniería en Redes Inteligentes y Ciberseguridad	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	