


ASIGNATURA DE CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

1. Competencias	Dirigir e implementar proyectos de negocios digitales y soluciones de entornos virtuales a través del desarrollo de aplicaciones progresivas, herramientas de inteligencia en los negocios y desarrollo avanzado inmersivo / multisensorial considerando las necesidades del cliente, la interpretación de los datos y la normatividad aplicable para contribuir a la evolución digital de las organizaciones en el marco global.
2. Cuatrimestre	Noveno
3. Horas Teóricas	24
4. Horas Prácticas	36
5. Horas Totales	60
6. Horas Totales por Semana Cuatrimestre	4
7. Objetivo de aprendizaje	El alumno empleará aspectos de ciberseguridad considerando estándares, protocolos, métodos, reglas, herramientas y leyes aplicables para minimizar los riesgos, incidentes y ataques en la información de los negocios digitales.


Unidades de Aprendizaje		Horas		
		Teóricas	Prácticas	Totales
I.	Fundamentos de la ciberseguridad	10	18	28
II.	Estándares y marcos de referencia para la ciberseguridad.	6	4	10
III.	Ciberseguridad en la nube.	8	14	22
Totales		24	36	60

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.
UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	I. Fundamentos de la ciberseguridad
2. Horas Teóricas	10
3. Horas Prácticas	18
4. Horas Totales	28
5. Objetivo de la Unidad de Aprendizaje	El alumno determinará las principales técnicas y herramientas para el intercambio de información segura.

Temas	Saber	Saber hacer	Ser
Fundamentos de la ciberseguridad	<p>Diferenciar los conceptos de: seguridad de la información, seguridad informática y ciberseguridad.</p> <p>Identificar las fases de la ciberseguridad.</p> <p>Explicar los conceptos de Amenazas, Vulnerabilidades, Riesgos, tipos de ataques e ingeniería social.</p> <p>Describir la importancia de la triada CID (confidencialidad, integridad y disponibilidad).</p>		<p>Pensamiento creativo</p> <p>Trabajo colaborativo</p> <p>Asertividad</p> <p>Observador</p> <p>Saber escuchar</p> <p>comunicarse</p> <p>Puntualidad</p> <p>Responsabilidad</p> <p>Honestidad</p> <p>Ética profesional y personal</p> <p>Respeto</p> <p>Liderazgo</p> <p>Iniciativa</p> <p>Proactivo.</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


Temas	Saber	Saber hacer	Ser
Gestión e intercambio seguro	<p>Identificar las Técnicas y Herramientas de protección de datos.</p> <p>Explicar la importancia de Controles de acceso y gestión de identidad.</p> <p>Identificar los principales protocolos de Intercambio de información segura (HTTPS, SSL, FTPS, SSH, IPSEC, SET, SCP, SFTP, SMTPS, IMAPS, OAuth).</p> <p>Describir el proceso para generación de firmas digitales.</p> <p>Explicar los usos y aplicaciones del BlockChain</p>	<p>Seleccionar las herramientas para protección de datos.</p> <p>Demostrar la aplicación de los principales protocolos de intercambio de información segura.</p>	<p>Pensamiento creativo</p> <p>Trabajo colaborativo</p> <p>Asertividad</p> <p>Observador</p> <p>Saber escuchar</p> <p>comunicarse</p> <p>Puntualidad</p> <p>Responsabilidad</p> <p>Honestidad</p> <p>Ética profesional y personal</p> <p>Respeto</p> <p>Liderazgo</p> <p>Iniciativa</p> <p>Proactivo.</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>Elabora y presenta a partir de un caso práctico un portafolio de evidencias que integre:</p> <p>a) Justificación de las herramientas seleccionadas para la protección de datos.</p> <p>b) Pruebas de los protocolos empleados para el Intercambio de información segura.</p> <p>c) Certificados digitales</p>	<p>1. Comprende los conceptos de seguridad de la información, seguridad informática y ciberseguridad.</p> <p>2. Comprende las fases de la ciberseguridad.</p> <p>3. Explica la importancia de Controles de acceso y gestión de identidad.</p> <p>4. Identifica protocolos de Intercambio de información segura.</p> <p>5. Explica el proceso de generación de firmas digitales.</p>	<p>Estudio de casos</p> <p>Lista de cotejo</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
Estudio de casos. Análisis de casos. Práctica demostrativa.	Equipo de cómputo. Internet sistemas operativos y Software especializado

ESPACIO FORMATIVO


Aula	Laboratorio / Taller	Empresa
	X	

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.
UNIDADES DE APRENDIZAJE

1.Unidad de aprendizaje	II. Estándares y marcos de referencia para la ciberseguridad.
2.Horas Teóricas	6
3.Horas Prácticas	4
4.Horas Totales	10
5.Objetivo de la Unidad de Aprendizaje	El alumno evaluará la normativa, aspectos legales y éticos aplicables a los negocios digitales para garantizar el buen uso de los datos personales de los usuarios.

Temas	Saber	Saber hacer	Ser
Estándares y marcos de referencia .	Describir las características de las normas y estándares: - ISO 27000 (ISO 27001 Sistema de Gestión de Seguridad de la Información, ISO 27002, ISO 27005 Gestión de riesgos de seguridad de la información). -Gestión de Ciberseguridad (ISO /IEC 27000, 27032). -Gestión de la Continuidad del Negocio (ISO 22301). -Gobierno de TI (COBIT 5).		Pensamiento creativo Trabajo colaborativo Asertividad Observador Saber escuchar comunicarse Puntualidad Responsabilidad Honestidad Ética profesional y personal Respeto Liderazgo Iniciativa Proactivo.

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


Temas	Saber	Saber hacer	Ser
Aspectos legales y éticos de la ciberseguridad.	<p>Describir las características de la normatividad nacional e internacional en materia de seguridad</p> <ul style="list-style-type: none"> - Ley General de protección de datos Personales de México - Ley de propiedad industrial - Ley federal de derechos de autor - Ley federal de datos personales en posesión de particulares - Código penal federal - Ley general de transparencia y acceso a la información. <p>Identificar el concepto e importancia de política de privacidad.</p> <p>Identificar las diferencias de Políticas de privacidad según su aplicación.</p> <p>Identificar la estructura a considerar en la elaboración de las políticas de privacidad.</p>	<p>Seleccionar las normatividades aplicables al desarrollo de aplicaciones para negocios digitales.</p> <p>Elaborar política de privacidad y confidencialidad de la información</p>	<p>Pensamiento creativo Trabajo colaborativo Asertividad Observador Saber escuchar comunicarse Puntualidad Responsabilidad Honestidad Ética profesional y personal Respeto Liderazgo Iniciativa Proactivo.</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>Elabora y presenta a partir de un caso práctico un portafolio de evidencias que integre:</p> <p>a) Propuesta de política de privacidad.</p> <p>b) Justificación o argumentación de como la política protege los datos personales del usuario.</p> <p>c) Cuadro comparativo de los marcos de referencia</p>	<p>1. Explica las características de las normas y estándares.</p> <p>2. Explica las características de la normatividad nacional e internacional.</p> <p>3. Comprende concepto e importancia de política de privacidad.</p> <p>4. Identifica la estructura a considerar en la elaboración de las políticas de privacidad.</p>	<p>Estudio de casos Lista de cotejo</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
Estudio de casos Análisis de casos Tareas de investigación	Equipo de cómputo. Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		


ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

UNIDADES DE APRENDIZAJE

6. Unidad de aprendizaje	III. Ciberseguridad en la nube.
7. Horas Teóricas	8
8. Horas Prácticas	14
9. Horas Totales	22
10. Objetivo de la Unidad de Aprendizaje	El alumno propondrá un plan de recuperación de desastres para garantizar la continuidad de los servicios en el negocio digital.


Temas	Saber	Saber hacer	Ser
Identificación de vulnerabilidades	<p>Identificar las principales amenazas de ciberseguridad para la nube.</p> <p>Describir la Metodología de análisis de vulnerabilidades. Identificar las herramientas de escaneo y detección de vulnerabilidades en la nube.</p> <p>Identificar herramientas para Seguridad para APIS. Identificar las Tendencias en ciberseguridad.</p>	<p>Realizar pruebas de intrusión, análisis de vulnerabilidades y monitoreo de incidencias.</p> <p>Demostrar la aplicación de herramientas para control de acceso y monitoreo para seguridad en APIS</p>	<p>Pensamiento creativo</p> <p>Trabajo colaborativo</p> <p>Asertividad</p> <p>Observador</p> <p>Saber escuchar</p> <p>comunicarse</p> <p>Puntualidad</p> <p>Responsabilidad</p> <p>Honestidad</p> <p>Ética profesional y personal</p> <p>Respeto</p> <p>Liderazgo</p>
Recuperación de desastres	<p>Describir el proceso para la elaboración del plan recuperación ante desastres por ciberataques para:</p> <ul style="list-style-type: none"> - la nube, - la virtualización - la red. <p>Identificar las herramientas de Hardware y software para gestión y análisis de vulnerabilidades en infraestructura de red.</p>	<p>Formular propuesta de plan de recuperación de desastres</p>	<p>Iniciativa</p> <p>Proactivo.</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
<p>Elabora y presenta a partir de un caso práctico un portafolio de evidencias que integre:</p> <p>a) Reporte de pruebas de intrusión y análisis de vulnerabilidades.</p> <p>b) Propuesta de plan de recuperación de desastres</p> <p>c) A partir de la interpretación elaborar el Diagnóstico del estatus de la seguridad.</p>	<p>1. Explica las principales amenazas de ciberseguridad para la nube.</p> <p>2. Comprende la Metodología de análisis de vulnerabilidades.</p> <p>3. Comprende el proceso para la elaboración del plan recuperación</p>	<p>Estudio de casos</p> <p>Lista de cotejo</p>

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	


CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
Estudio de casos Análisis de casos Práctica demostrativa	Equipo de cómputo. Internet Sistemas operativos y Software especializado

ESPACIO FORMATIVO


Aula	Laboratorio / Taller	Empresa
	X	

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

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


Capacidad	Criterios de Desempeño
Determinar componentes de arquitectura, considerando los requerimientos establecidos, requisitos técnicos y de seguridad, para mejorar la experiencia de usuario.	Entregará propuesta técnica que incluya: a) Informe de levantamiento de requerimientos. b) Requisitos técnicos y de seguridad (hardware, software). c) Diseño (mapeo, vistas, componentes). d) Criterios de medición de experiencia del usuario."
Desarrollar aplicaciones web progresivas considerando los requerimientos establecidos, requisitos técnicos y de seguridad, para mejorar la experiencia de usuario.	Entregará aplicaciones funcionales que incluya: a) Interfaces de usuario multiplataforma. b) Módulos administrativos. c) Consumo de APIS (propias y de terceros). d) Medidas y políticas de seguridad "
Desarrollar proyectos de negocios digitales mediante metodologías ágiles, herramientas tecnológicas orientadas a la distribución de aplicaciones en la nube, modelos de negocio, procesos y métodos de dirección para la venta de productos, contenidos y servicios en línea.	Entregará reporte de seguimiento que considere: a) propuesta de proyecto. b) argumentación del proyecto. c) Seguimiento y control (de avances, solicitudes de cambios, versiones. d) Proceso de despliegue y distribución. e) mecanismos de controles de seguridad. f) Requisitos legales(registros de derechos autor y de propiedad intelectual)"
Controlar el desempeño de los proyectos de negocios digitales mediante evaluación de análisis de datos, técnicas y herramientas de ciberseguridad, técnicas de monitoreo para cumplir con el propósito y alcance del proyecto.	Entregará reporte de medición de la implementación que incluya: a) proceso de la administración del proyecto. b) evaluación de riesgos. c) estadísticas de comportamiento y desempeño. d) Control de pruebas y seguridad. e) Registro de cambios.

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	

CIBERSEGURIDAD APLICADA A LOS NEGOCIOS.

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Chris Moschovitis	2018 ISBN 9781119429517 (Hardcover) ISBN 9781119430056 (ePDF) ISBN 9781119430001 (ePub)	CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS	Hoboken, New Jersey	USA	Wiley & Sons
Charles J. Brooks Christopher Grow Philip Craig Donald Short	2018 ISBN: 978-1-119-36239-5 ISBN: 978-1-119-36243-2 (ebk) ISBN: 978-1-119-36245-6 (ebk)	CYBERSECURITY ESSENTIALS	Indianápolis, Indiana	USA	Wiley & Sons
William "Bo" Rothwell Denise Kinsey	2019 ISBN-13: 978-0-7897-5935-1 ISBN-10: 0-7897-5935-7	Linux Essentials for Cybersecurity		USA	Pearson
Chris Dotson	2019 ISBN: 978-1-492-03751-4	Practical Cloud Security A Guide for Secure Design and Deployment	Sebastopol, CA	USA	O'Reilly

ELABORÓ:	Comité de Directores de la Carrera de Entornos Virtuales y Negocios Digitales	REVISÓ:	Dirección Académica	
APROBÓ:	C. G. U. T. y P.	FECHA DE ENTRADA EN VIGOR:	Septiembre de 2020	