



INFORMACIÓN ESPACIO ACADÉMICO						
Nombre de asignatura	Regulaciones y Delitos Informáticos					
Código	11502003					
Definición de asignatura	Obligatorio	X	Básico		Complementario	
	Electivo		Intrínseco		Extrínseco	
Número de créditos	3	Horas		Semanas	16	
Distribución créditos	HTD	64	HTC	32	HTA	48
	Horas de trabajo cooperativo					
Metodología	El desarrollo del curso se efectuará de manera virtual a través de la plataforma de aprendizaje interactiva Moodle. Se priorizará la lectura de artículos y fragmentos de libros, así como la realización de foros y talleres grupales.					

PROGRAMACIÓN DEL CONTENIDO
CONOCIMIENTOS PREVIOS
-Tecnologías de la Información y las Comunicaciones (TIC).
DESCRIPCIÓN DEL CURSO
<p>El curso Legislación y Delitos Informáticos es de carácter teórico vinculado al núcleo énfasis del programa de Maestría en Gestión y Seguridad de la Información. El curso, de cuatro (04) créditos y dividido en cuatro (04) unidades, ha sido diseñado para ejecutarse en dieciséis (16) semanas.</p> <p>Vivimos en un mundo intrínsecamente relacionado con las nuevas tecnologías, las cuales se han venido impregnando cada vez más en todas las esferas de la existencia social. En este sentido, el derecho, en el desarrollo de su función como regulador de realidades sociales, ha realizado avances legislativos que abordan las nuevas interacciones, tensiones y riesgos existentes en la sociedad de la información; de las cuales no son ajenas las presentadas en los procesos de las organizaciones en los que la información es un activo primordial.</p> <p>El curso Legislación y Delitos Informáticos tiene como objetivo familiarizar al estudiante con la legislación nacional más relevante respecto a los riesgos asociados al tratamiento de la información y la tecnología en el desarrollo de operaciones organizacionales. Desde esta perspectiva, el curso permitirá que el estudiante adquiera nociones conceptuales y normativas relacionadas al derecho y las nuevas tecnologías, la construcción y desarrollo de procesos efectivos respecto a la protección de datos personales y firma digital al interior de las organizaciones, así como la comprensión, identificación y análisis de los delitos informáticos en el ámbito nacional e internacional.</p>





En este sentido, el curso Legislación y Delitos Informáticos pretende dotar a los estudiantes del programa de Maestría en Gestión y Seguridad de la Información de las herramientas jurídicas necesarias para que las estrategias de gestión y seguridad de la Información y proyectos TI que diseñen y formulen, estén alineados a la normatividad nacional.

ÁREAS DE CONOCIMIENTO

Derecho - Derecho Informático - Tecnologías de la Información y las Comunicaciones - Protección de Datos Personales - Firma Digital - Delitos Informáticos

COMPETENCIAS EN FORMACIÓN

- Analizar el impacto de las nuevas tecnologías en la sociedad y en el Derecho.
- Plantear las prácticas necesarias para el cabal cumplimiento del régimen de protección de datos y la aplicación del principio de responsabilidad demostrada en las organizaciones.
- Proponer los procesos necesarios para una correcta implementación y funcionamiento de la firma digital teniendo en cuenta las necesidades de la organización y la legislación nacional.
- Reconocer el funcionamiento de la cibercriminalidad, las diferentes tipologías del ciberdelito, así como las generalidades, conceptos, elementos y características de los delitos informáticos en la legislación penal colombiana.

ESTRUCTURA DEL MÓDULO

UNIDAD 1. Derecho, Sociedad y Nuevas Tecnologías

OBJETIVO DE APRENDIZAJE		TÍTULO DE TEMA
<p>Conocer las nociones básicas del Derecho, la incidencia de las Nuevas Tecnologías en este y en la sociedad, así como las generales del derecho informático.</p>		<p>1. UNIDAD 1. Derecho, Sociedad y Nuevas Tecnologías</p> <p>1.1. Nociones básicas del Derecho</p> <p>1.1.1. Definición de Derecho</p> <p>1.1.2. Fuentes del Derecho</p> <p>1.1.3. Principios generales del Derecho</p> <p>1.1.4. Organización del estado colombiano</p> <p>1.1.5. Bloque de Constitucionalidad</p> <p>1.1.6. Derechos fundamentales</p> <p>1.1.7. Derechos colectivos</p> <p>1.1.8. Derechos sociales</p>
		<p>1.2. Relación entre tecnología, sociedad y Derecho</p> <p>1.2.1. Sociedad de la información</p> <p>1.2.2. La influencia de la tecnología en el Derecho</p> <p>1.2.3. Regulación de las nuevas tecnologías</p>
		<p>1.3. El derecho informático</p> <p>1.3.1. Derecho de la informática</p> <p>1.3.2. Informática jurídica</p>





UNIDAD 2. Protección de Datos Personales y Accountability		
OBJETIVO DE APRENDIZAJE		TÍTULO DE TEMA
<p>Estudiar los aspectos regulatorios principales del régimen de protección de datos personales y la implementación del principio de responsabilidad demostrada (<i>Accountability</i>) en las organizaciones.</p>		<p>2. UNIDAD 2. Protección de Datos Personales y Accountability</p> <p>2.1. Introducción a la Protección de Datos Personales</p> <p>2.1.1. Habeas Data</p> <p>2.1.2. Marco Normativo</p> <p>2.1.2.1. Marco normativo colombiano</p> <p>2.1.2.2. Excepciones a la aplicación de las leyes 1266 de 2008 y 1581 de 2012</p> <p>2.1.3. Conceptos importantes</p> <p>2.1.3.1. Tratamiento</p> <p>2.1.3.2. Autorización</p> <p>2.1.3.3. Políticas de tratamiento de la información</p> <p>2.1.3.4. Aviso de privacidad</p> <p>2.1.3.5. Base de datos</p>
		<p>2.2. El dato personal y los sujetos que intervienen en la protección de datos personales</p> <p>2.2.1. El dato personal</p> <p>2.2.1.1. Concepto de dato personal</p> <p>2.2.1.2. Principios rectores aplicables al dato</p> <p>2.2.1.3. Características del dato personal</p> <p>2.2.1.4. Clasificación de los datos personales</p> <p>2.2.1.5. Datos de niños, niñas y adolescentes</p> <p>2.2.2. Sujetos que intervienen en la protección de datos personales</p> <p>2.2.2.1. Principios rectores aplicables a los sujetos</p> <p>2.2.2.2. Sujetos en la Ley 1266 de 2008</p> <p>2.2.2.2.1. Deberes de los sujetos</p> <p>2.2.2.2.2. Derechos del Titular</p> <p>2.2.2.3. Sujetos en la Ley 1581 de 2012</p> <p>2.2.2.3.1. Deberes de los sujetos</p> <p>2.2.2.3.2. Derechos del Titular</p>





		<p>2.2.2.4. Organismo de control y régimen de sanciones</p> <p>2.3. Procedimientos para el adecuado tratamiento de datos personales y circulación transfronteriza de datos.</p> <p>2.3.1. Procedimientos para el adecuado tratamiento de datos personales (Consultas y trámites)</p> <p>2.3.1.1. Principios relacionados a los procedimientos</p> <p>2.3.1.2. Consultas y reclamos en la Ley 1581 de 2012</p> <p>2.3.1.3. Consultas y reclamos en la Ley 1266 de 2008</p> <p>2.3.2. La circulación transfronteriza de datos</p> <p>2.4. Inventario de bases de datos</p> <p>2.4.1. Conceptos y contexto normativo</p> <p>2.4.2. Ruta del Registro Nacional de Bases de Datos</p> <p>2.5. Principio de responsabilidad demostrada (Accountability)</p> <p>2.5.1. Conceptos importantes</p> <p>2.5.2. Beneficios de la implementación del principio de responsabilidad demostrada</p> <p>2.5.3. Los Administradores de los datos personales</p> <p>2.5.4. ¿Cómo prevenir la vulneración del derecho a la Protección de Datos personales?</p> <p>2.5.5. Concepto de Responsabilidad demostrada</p> <p>2.5.6. Aspectos para tener en cuenta en la implementación de las medidas</p> <p>2.5.7. ¿Qué se debe informar ante la SIC?</p> <p>2.5.8. Aspectos generales sobre el desarrollo de un Programa Integral de Gestión de Datos Personales.</p>
<p>UNIDAD 3. Firma Digital</p>		<p>TÍTULO DE TEMA</p>
<p>OBJETIVO DE APRENDIZAJE</p>		<p>TÍTULO DE TEMA</p>





<p>Comprender las nociones generales, normatividad y la correcta implementación y funcionamiento de las firmas digitales en el contexto colombiano.</p>		<p>3. UNIDAD 3. Firma Digital</p> <p>3.1. Introducción a la regulación de la firma digital</p> <p>3.1.1. Principio de equivalencia funcional</p> <p>3.1.2. Documento electrónico</p> <p>3.1.2.1. Conceptualización de documento</p> <p>3.1.2.2. El mensaje de datos como documento</p> <p>3.1.2.3. Definición de documento electrónico</p> <p>3.1.2.4. Valor legal y probatorio de un documento electrónico</p> <p>3.1.2.5. Características del documento electrónico</p> <p>3.1.2.6. Atributos de seguridad jurídica de los documentos electrónicos</p> <hr/> <p>3.2. La firma electrónica, la firma digital y las entidades de certificación</p> <p>3.2.1. La firma manuscrita</p> <p>3.2.2. Características y elementos de la firma</p> <p>3.2.3. Firma electrónica</p> <p>3.2.4. Firma digital</p> <p>3.2.5. La firma electrónica y la firma digital en Colombia</p> <p>3.2.6. Las entidades de certificación digital</p> <p>3.2.6.1. El tercero de confianza</p> <p>3.2.6.2. Entidades de certificación en Colombia</p> <p>3.2.6.3. Requisitos de funcionamiento</p> <p>3.2.6.4. Clases de entidades de certificación</p> <p>3.2.6.5. Actividades y servicios de las entidades de certificación</p> <p>3.2.6.6. Los certificados digitales</p> <p>3.2.6.7. El servicio de estampado cronológico</p> <hr/> <p>3.3. Parámetros generales de funcionamiento de las firmas digitales y electrónicas y su implementación en las organizaciones.</p>
<p>UNIDAD 4. Delitos Informáticos</p>		





OBJETIVO DE APRENDIZAJE	TÍTULO DE TEMA
Analizar el fenómeno de la cibercriminalidad en el ámbito global y local a través de la identificación los actores que intervienen en el ciberdelito, la cadena criminal asociada a este, las principales modalidades delictivas, y el estudio de las diferentes figuras criminales del delito informático incorporadas en la legislación penal colombiana.	4. UNIDAD 4. Delitos Informáticos
	4.1. Conceptualización del Ciberdelito
	4.2. Comprendiendo el fenómeno del ciberdelito
	4.3. Los Actores del Ciberdelito
	4.4. Ciberdelitos y Criptoactivos
	4.5. Los delitos Informáticos en la legislación colombiana
	4.6. Informática forense

EVALUACIÓN		
TIPO	EVALUACIÓN/ACTIVIDAD	PORCENTAJE
Formativa	Unidad 1. (Foro) Tecnologías emergentes y su incidencia en la sociedad y el derecho.	5%
	Unidad 1. (Taller) Estudio de caso sobre la 'Constitución Digital' aprobada en la Unión Europea.	10%
	Unidad 2. (Taller) Análisis de aviso de privacidad.	20%
	Unidad 3. (Taller) Tabla niveles de confianza y tipos de firma.	20%
	Unidad 4. (Taller) Estudio de caso. Tipologías y tipos penales.	10%
	Unidad 4. (Taller) Tabla tipologías y delitos informáticos.	15%
Estudio autónomo	Lectura de las unidades y revisión de los videos y bibliografía recomendada.	10%
Tutorías	Revisión de clases magistrales virtuales	10%
Total del curso		100 %

BIBLIOGRAFÍA	
1	Monroy, M. (2018). <i>Introducción al Derecho</i> . Temis.
2	Aranda, F. (2021). <i>Derecho y las nuevas tecnologías: La influencia de Internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español</i> . Dykinson.





3	Remolina, N. (2013). <i>Tratamiento de datos personales: Aproximación internacional y comentarios a la Ley 1581 de 2012</i> . Legis.
4	Remolina, N., Tenorio, M., Quinterio, G. (2018). <i>La responsabilidad demostrada en las funciones misionales de la registraduría nacional del estado civil</i> . Temis.
5	Peña, D. (2015). <i>De la firma manuscrita a las firmas electrónica y digital</i> . Universidad Externado de Colombia.
6	Rincón, E., Mendieta, C. (2021). <i>Aspectos teórico-prácticos de la firma digital en Colombia y su referente en Latinoamérica</i> . Universidad del Rosario.
6	Suarez, A. (2016). <i>Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009</i> . Universidad Externado de Colombia.
8	Posada, R., Zúñiga, L. (2017). <i>Los cibercrímenes : un nuevo paradigma de criminalidad : un estudio del título VII bis del Código penal colombiano</i> . Grupo editorial Ibañez.

		ORGANIZACIÓN / TIEMPOS															
PROGRAMA SINTÉTICO		SEMANAS ACADÉMICAS															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.	UNIDAD 1. Derecho, Sociedad y Nuevas Tecnologías	X	X	X													
2.	UNIDAD 2. Protección de Datos Personales y Accountability				X	X	X	X	X								
3.	UNIDAD 3. Firma Digital									X	X	X					
4.	UNIDAD 4. Delitos Informáticos												X	X	X	X	X

ELABORÓ: Oscar Andrés Doncel Brito
27/10/2022

