DIPLOMADO "CIBERSEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGO"

- **Introducción del programa**

Las TIC – Tecnologías de la Información y la Comunicación han revolucionado todos los sectores productivos de la sociedad, hasta el punto de generar un nuevo subsistema económico, la llamada Economía Digital.

Bajo el contexto anterior, la ciberseguridad se ha convertido en un elemento sustancial para asegurar no solo la confidencialidad, autenticidad e integridad de la información, sino también asegurar la supervivencia y continuidad de los negocios empresariales y de los gobiernos.

Conocer de ciberseguridad es una necesidad para cualquier profesional, el presente diplomado pretende que generar nuevas competencias que aseguren que cualquier persona pueda estar calificada para asumir los retos de la seguridad digital en un mundo cada vez más digital y transfronterizo.

- **Objetivo del programa**

Este diplomado busca presentar a los estudiantes el estado de la ciberseguridad mundial, junto con los principales componentes y conceptos sobre la ciberseguridad, la ciberguerra y las ciberoperaciones, su funcionamiento, mecanismos jurídicos y una aproximación a los riesgos y retos para las empresas y los gobiernos.

- **Estructura del Programa – Módulos**
- Conceptos sobre ciberseguridad
- ¿Qué es la ciberseguridad? ¿Qué lo compone?
- Qué es un ciberataque ¿Cómo funciona?
- Diferencias con la ciberguerra y la ciberdefensa
- Componentes, manifestaciones de las ciberarmas
- Diferencia entre seguridad de la información, seguridad digital, seguridad de las aplicaciones.
- El ciberespacio como dominio de poder y de la guerra digital. Geopolítica de la ciberseguridad y la ciberguerra
- Ejercicios prácticos

1. Historia de los ciberataques y ciberoperaciones

- Tipos de ciberataques y su clasificación
- Ataques cibernéticos que han sucedido en la historia
- Ataques digitales, híbridos y asimétricos
- Principales grupos armados cibernéticos
- Rol de los Estados
- Rol de los grupos de personas / individuos

- Rol de las empresas

3. Fundamentos jurídicos de la ciberseguridad
- Convenio de Budapest y sus protocolos
- Constitución Unión Internacional de Telecomunicaciones
- Línea de Derecho de las Ciberoperaciones – Manual de Taillinn
- Institucionalidad y Conpes de Ciberseguridad en Colombia
- Normativa Superfinanciera
- Normativa de Gobierno Digital – Ciberseguridad
- Otra normativa de ciberseguridad
- Modelo de Seguridad y Privacidad de la Información para el Estado colombiano
- Comparativo de normativa de ciberseguridad en la región
- Reglas para la conducción de las ciberoperaciones

4. Protección de datos
- Introducción y tendencias. Caso colombiano
- Introducción, concepto y evolución histórica de la protección de datos
- Evolución jurisprudencial
- Tendencias regulatorias
- Bases legales para el tratamiento de datos personales en el ordenamiento colombiano
- Conceptos
- Principios
- Partes (responsable, encargado) y sus obligaciones
- Derechos de los titulares
- Autoridad y modelos en el derecho comparado
- Régimen aplicable en circulación y transferencia de datos
- Aplicación de la ley colombiana a empresas extranjeras
- Circulación internacional de datos personales
- Modelos regulatorios internacionales
- Unión Europea
- California
- China
- Hábeas data en el sector financiero
- Seguridad de la información. Buenas prácticas nacionales e internacionales.
- Certificación ISO
- Regulaciones sectoriales internacionales
- Seguridad de la información y gestión de incidentes

5. Delitos informáticos
- Problemática de los delitos informáticos: delitos transfronterizos
- Normativa sobre delitos informáticos en el Código Penal Colombiano
- La prueba en los delitos informáticos
- Peritaje para delitos informáticos
- Canales de atención para delitos informáticos y mecanismo de cooperación internacional 24/7
- Ejercicios prácticos

6. Gestión del riesgo de la seguridad digital
- Estándares familia ISO 27000
- Estándares NIST
- Niveles de madurez de la ciberseguridad
- El Plan de Ciberseguridad
- ¿Qué hacer en caso de ciberataque?

- Controles físicos
- Controles lógicos
- Monitoreo y sus reglas
- Supervisión del acceso no autorizado a sistemas y redes
- Auditorías y pruebas de impacto (IS0 27001:2013) (ISO 27032:2012).
- Rol del abogado
- Rol del técnico
- Verificación de riesgos
- Continuidad del negocio

7. Prospectiva de la ciberseguridad y la protección de datos

- Inteligencia artificial para la ciberseguridad
- Controles de identidad y credenciales
- Protección de datos en las nuevas tecnologías

- **Dirigido a**

Este programa está dirigido a todos aquellos profesionales de diversas áreas que estén interesados en comprender el estado de la ciberseguridad mundial, junto con los principales componentes y conceptos sobre la ciberseguridad, la ciberguerra y las ciberoperaciones, su funcionamiento, mecanismos jurídicos y una aproximación a los riesgos y retos para las empresas y los gobiernos.

- **Horario y Lugar**

Todos los jueves, de 7:00 a.m. a 1:00 p.m. (con visitas presenciales cada 15 días a la universidad)

- **Inversión.** $3.000.000
- **Fecha de inicio: 05/05/2022**
- **Fecha fin: 15/09/2022**
- **Duración: 96 horas**
- **Inscríbase en: https://www.uexternado.edu.co/programa/derecho/diplomado-seguridad-digital/**

Contáctanos
Departamento de Derecho de las Telecomunicaciones
Teléfonos (601) 3537000, 3420288 y 3419900
Ext. 1105-1106.
Bogotá, Colombia.
esdercom@uexternado.edu.co