**Plan de estudios**

El Diplomado se subdivide en tres (3) módulos que van proporcionando los conocimientos requeridos para involucrarse en la temática:

**MODULO 1 – RIESGOS (24 horas):** Presentar y contextualizar las temáticas asociadas con riesgos cibernéticos, la normatividad y el compliance, así como el impacto organizacional y buen gobierno en materia de cumplimiento.

a. **Introducción – impacto organizacional (2 horas):** La mejora del MPD (Modelo de Prevención de Delitos o Modelo de Organización y Control) y de la imagen de la empresa.
b. **Normas técnicas (4 horas):** ISO 31000:2018, ISO 31010:2019, ISO/IEC 27005:2018, ISO 19600:2014.
c. **Metodologías de gestión del riesgo (4 horas):** Metodologías aplicadas (mapa de riesgos, identificación de amenazas, vulnerabilidades y riesgo.
d. **Herramientas de Gestión del Riesgo (4 horas):** Aplicación y uso de herramientas de gestión del riesgo.
e. **Ética, corrupción, gobierno corporativo (10 horas):** Contexto y tendencias del compliance / cumplimiento y el gobierno corporativo, investigaciones internas, diseño de una línea ética o canal de denuncia (whistleblowing), reporte del incumplimiento a la Alta Dirección, diseño de un sistema de sanciones disciplinario, responsabilidad individual por los delitos de la empresa, compliance penal ISO 19601:2018.

**MODULO 2. LEGISLACIÓN EN CIBERSEGURIDAD (42 horas)**: Presentar y contextualizar las tipologías y modalidades asociadas al cibercrimen, así como la legislación aplicable en materia de compliance.

a. **Tipología cibercrimen - prevención de delitos (12 horas):** Tipologías de cibercrimen y su incidencia en las organizaciones (contexto y evolución), concepto de modelo de prevención de delitos o criminal compliance, distinción de otros fenómenos similares: buen gobierno corporativo, responsabilidad social corporativa, business ethics, relación entre los modelos de prevención de delitos y otras normativas sectoriales como la Ley de Protección de Datos, entre otras, marcos de referencia internacional UE, EEUU, ISO/IEC 27701:2019, ISO/IEC 29100:2011.
b. **Modalidades (4 horas):** Espionaje empresarial, Fuga de Datos empresariales, brechas, reputación financiera.
c. **Ciberlavado, criptoactivos (4 horas):** Tendencias actuales y retos.
d. **Protección de datos y derecho penal (10 horas):** Análisis e implicaciones de la normatividad vigente, historia legislativa - responsabilidad penal de las empresas, descripción del régimen vigente, reflexiones sobre la incidencia de la nueva regulación en la teoría general del delito y en el modelo de Estado.
e. **Cómo protegerse (detección, reacción, prevención, gestión) – (12 horas):** Hacking ético, gestión de vulnerabilidades e ingeniería inversa, metodología de auditoria y test de intrusión, técnicas de hacking y test de intrusión, gestión de vulnerabilidades, origen de la continuidad del negocio (CN), el ciclo de vida de la gestión de la continuidad del negocio (GCN), componentes claves de un sistema de GCN, implementación de un SGCN, gestión de crisis y respuesta ante incidentes, sistema de gestión de la continuidad de negocio (ISO 22301:2019).

**MODULO 3. CIBERSEGURIDAD (24 horas):** Presentar y contextualizar acerca de los estándares asociados a la ciberseguridad y la noción de ciber resiliencia.

conviene protegerse, desarrollo seguro de aplicaciones (SSLDC), securización de

a. **Lo que debe tener una organización para mantenerse (8 horas):** La transformación digital de las empresas y la gestión de la ciberseguridad, el mapa de riesgos digitales frente al que aplicaciones web modernas.
b. **Basura electrónica e impacto (2 horas):** Tendencias actuales y retos.
c. **Estándares en ciberseguridad (8 horas):** Contexto, estándares ISO/IEC 27932, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27100. ISO/IEC 27103, protección de infraestructura crítica cibernética, ciber resiliencia, otros marcos de referencia.
d. **Ciber resiliencia y sistemas resilientes (6 horas):** Definiciones de ciber resiliencia, marco NIST Special Publication 800-160, gobernanza, dominios y principios de ciber-resiliencia, técnicas y aproximaciones, ciclo de vida, prácticas y procesos, evaluación de la madurez.