Diplomado
Ciberseguridad y Compliance

Modalidad presencial (bajo el modelo de Presencialidad Asistida por Tecnología PAT)

PRESENTACIÓN

Uno de los temas claves en la actualidad para la estrategia de negocios y la trasformación digital de las organizaciones es la Ciberseguridad, debido a la interconexión y uso masivo del internet y tecnologías derivadas de la cuarta revolución por parte de las personas y las organizaciones.

Por ello, todas las organizaciones sin importar su tamaño y el sector al que estén vinculadas, deben hacer un esfuerzo por proteger sus infraestructuras, garantizar la fiabilidad de sus datos, la prestación efectiva de sus servicios y mitigar los riesgos cibernéticos, lo que implica para éstas, afrontar desafíos en materia de ciberseguridad, fomentando la concienciación y el desarrollo de competencias en torno a la importancia de la formación en materia de cumplimiento (compliance), el buen gobierno (ética y anticorrupción), como un control efectivo para cerrar la brecha de acceso a activos importantes de las organizaciones como la información por parte de ciberdelincuentes, así como los costos por daños asociados a sanciones por incumplimiento a las regulaciones y las débiles implementaciones de las recientes normas técnicas tales como: ISO 19600:2014, ISO 31000:2018, ISO 31010:2019, ISO/IEC 27005:2018, entre otras.

Datos relevantes para las organizaciones según el último Informe Global de Riesgos del Foro Económico Mundial (2019):

- De los 10 principales riesgos mundiales en términos de probabilidad en la posición 4 está el fraude o robo de datos y en la 5 los ataques cibernéticos.
- Habrá un incremento en los riesgos de ataques cibernéticos entre el 2019 y 2020, lo que conducirá al robo de dinero y datos (un 82 %) y a la interrupción de las operaciones (un 80 %).
- De 10 principales riesgos mundiales en términos de impacto en la posición 7 están los ataques cibernéticos y en la 8 el colapso de la infraestructura crítica de la información.
- El "fraude y robo de datos masivo" se ubicó en el número cuatro de riesgo mundial por probabilidad, en un lapso de 10 años, con los "ataques cibernéticos" situados en el número cinco.

OBJETIVOS DEL PROGRAMA

GENERAL

El Diplomado en Ciberseguridad y Compliance pretende dotar a los asistentes de conocimiento y herramientas que le permitan aportar en la planeación, gestión y disposición de controles efectivos en materia de ciberseguridad y cumplimiento en las organizaciones, tanto desde la perspectiva estratégica como técnica y jurídica.

ESPECÍFICOS

- Conocer las tipologías, técnicas y métodos que tienen los autores de un ciberataque, así como las amenazas que enfrentan las organizaciones en el entorno digital.

- Generar conciencia en torno a la importancia de involucrar a las distintas áreas de las organizaciones en la responsabilidad de la gestión de los riesgos digitales.

PERFIL DEL INTERESADO

El Diplomado en Ciberseguridad y Compliance está dirigido a aquellos responsables de la planeación, gestión y disposición de controles efectivos en materia de ciberseguridad en las organizaciones tanto desde la perspectiva estratégica como técnica y jurídica. Igualmente, está dispuesto para aquellos profesionales, estudiantes o interesados en adquirir conocimientos en la materia.

METODOLOGÍA

Durante la formación se abordarán desde un punto de vista global, actual y práctico las amenazas y vulnerabilidades en materia de ciberseguridad y compliance que afectan hoy en día a las organizaciones, mediante el desarrollo de clases magistrales y actividades teórico-prácticas (individuales y grupales).

Para fortalecer las competencias para el análisis, gestión y respuesta en las organizaciones, se desarrollarán casos de uso y se analizarán escenarios controlados en ambientes virtuales mostrando fundamentos en incidentes cibernéticos (recopilación de información, ataques de Denegación de Servicio (DoS), entre otros) y sus respectivos controles (metodologías de desarrollo seguro, seguridad perimetral, entre otros), todo alienado con los estándares y buenas prácticas internacionales.

Módulo	Contenido	Intensidad
1 RIESGOS	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. • **Introducción – impacto organizacional:** La mejora del MPD (Modelo de Prevención de Delitos o Modelo de Organización y Control) y de la imagen de la empresa. • **Normas técnicas:** ISO 31000:2018, ISO 31010:2019, ISO/IEC 27005:2018, ISO 19600:2014, OCTAVE, actualización orange book, NIST. • **Metodologías de gestión del riesgo:** Metodologías aplicadas (mapa de riesgos, identificación de amenazas, vulnerabilidades y riesgo. • **Herramientas de Gestión del Riesgo:** Aplicación y uso de herramientas de gestión del riesgo. • **Ética, corrupción y cumplimiento normativo:** Contexto y tendencias del compliance / cumplimiento, 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. • **Introducción a la ciberseguridad en la gestión de riesgos corporativos e institucionales:** Aplicados a activos intangibles digitales, activos intangibles no digitales, infraestructuras físicas y digitales, personas de interés, relaciones y redes de información, procesos productivos y de gobierno, acceso a datos privilegiados, valorización de operaciones, reputación, personas de interés, marca y reputación y trazabilidad de operaciones.	24 Horas
2 LEGISLACIÓN	Presentar y contextualizar las tipologías y modalidades asociadas al cibercrimen, así como la legislación aplicable en materia de compliance. • **Tipología cibercrimen - prevención de delitos:** 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. • **Ciberlavado, criptoactivos:** Tendencias actuales y retos. • **Modalidades:** Espionaje empresarial, Fuga de Datos empresariales, brechas, reputación financiera. • **Protección de datos , peritaje informático y derecho penal:** 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. • **Cómo protegerse (detección, reacción, prevención, gestión):** 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, 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), evidencia digital.	42 Horas
3 CIBERSEGURIDAD	Presentar y contextualizar acerca de los estándares asociados a la ciberseguridad y la noción de ciber resiliencia. • **Lo que debe tener una organización para mantenerse:** La transformación digital de las empresas y la gestión de la ciberseguridad, el mapa de riesgos digitales frente al que conviene protegerse, desarrollo seguro de aplicaciones (SSLDC), securización de aplicaciones web modernas. • **Basura electrónica e impacto:** Tendencias actuales y retos. • **Estándares en ciberseguridad:** Contexto, estándares ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27100. ISO/IEC 27103, NIST, protección de infraestructura crítica cibernética, ciber resiliencia, otros marcos de referencia. • **Ciber resiliencia y sistemas resilientes:** 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. • **Casos de uso de la ciberseguridad aplicada a la empresa y a las instituciones públicas.** • **Propios de la actividad:** Propiedad intelectual y patentes, propuestas comerciales, licitaciones y contratos, bases de clientes, contingencias y procesos legales, información estratégica, partners y acuerdos estratégicos, procesos de expansión (M&A e internacionalización), estructuración/consolidaciones filiales, procesos de Due Diligence, negociaciones, procesos de gobierno, acceso a información privilegiada. • **Stakeholders:** Organización interna, accionistas, consejeros, directivos clave, empleados. Colaboradores externos: proveedores, consultores, asesores, clientes, asociaciones, reguladores, etc. • **Marca / Reputación:** Monitorización de la comunicación y la publicidad, evolución de la percepción de clientes y mercados, impacto en Resultados, valor de la marca, trasparencia en la gestión territorial, etc.	24 Horas

EQUIPO DOCENTE
Expertos en esta área del conocimiento

SANDRA PATRICIA CRISTANCHO BOTERO
COORDINADOR ACADÉMICO

Ingeniera de sistemas, Especialista en Sistemas de Gestión Integrados de Calidad, en formación en Seguridad Informática MgSI, certificada en Oracle y en plataformas Cloud de Google. Desde el año 2011 se encuentra vinculada a la Facultad de Ingeniería de la Universidad Ean, donde actualmente se desempeña como directora del programa de Ingeniería de Sistemas.

JOSE RAMÓN AGUSTINA
DOCENTE

Experto español en ciberseguridad y compliance. Abogado y consultor independiente, Doctor europeo en Derecho por la Universitat Pompeu Fabra. Actualmente es catedrático acreditado en Derecho Penal y Criminología de la Facultad de Derecho y Empresa de la Universitat Abat Oliba CEU.

Ha ejercido durante cuatro años como magistrado suplente en la Audiencia Provincial de Barcelona (2010-2013), siendo magistrado ponente de más de 300 resoluciones judiciales. Con una tesis sobre delincuencia intra-empresarial y sus formas de prevención y control interno, ha realizado diversas estancias de investigación en EE. UU. y Reino Unido.

CORONEL (RA) FREDY BAUTISTA
DOCENTE

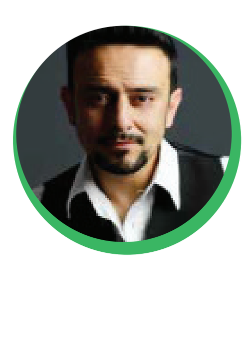
Exdirector del Centro Cibernético Policial, consultor en TI y ciberseguridad. Docente y experto en ciberseguridad, investigación de cibercrimen y perito en informática.

Estudió Administración de Laboratorios de Informática Forense en University of North Texas, Dallas EE. UU. (2007). Especialización en Crimen Organizado, Corrupción y Terrorismo de la Universidad Salamanca, Salamanca España (2009).

ESTHER ÁLVAREZ GONZÁLEZ
DOCENTE

Doctora en Sistemas de Información en la Empresa de Departamento GIO de la Universidad Politécnica de Madrid. Experta en desarrollo de capacidades en ciberseguridad.

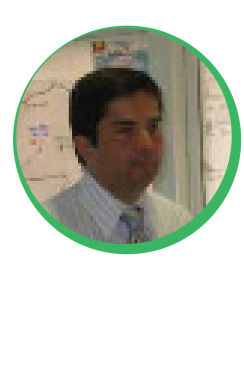
Ingeniera de Telecomunicaciones, experta en sistemas de información en empresas y en desarrollo de capacidades en ciberseguridad, entre otros. Cuenta con un Computing for Data Analysis, JOHNS HOPKINS UNIVERSITY, superado con mención especial (2013).



JOSHSUA J. GONZÁLEZ DÍAZ
DOCENTE

Asesor para la delegatura de riesgo operacional y ciberseguridad – Super Financiera de Colombia. Experto en Gestión de Riesgos e incidentes cibernéticos, hacking ético y computación forense.

Es Ingeniero de Sistemas de la Pontifica Universidad Javeriana. Especialista en Seguridad de la Información de la Universidad de los Andes. Especialista en Derecho Informático y magister en Seguridad de la Información.



JUAN CARLOS LOBO
DOCENTE

Administrador de Empresas de la Universidad Ean, experto y docente en sistemas de gestión, seguridad y privacidad de la información, crisis, continuidad, riesgos, compliance y ciberseguridad.

Certificaciones:
- ERCA- FUTURE BUILDERS. Auditor Líder ISO 45001:2018. 2018
- FUTURE BUILDERS. ISO/IEC 17021-1:2015, ISO/IEC TS 17021-1:2016 y ISO/IEC TS 17021-3:2017
- PECB. ISO 31000 Risk Manager. 2018
- IRCA. SGS. Auditor Líder ISO 9001:2015. 2017
- IRCA. SGS. Auditor Líder ISO 27001:2013. 2017
- ERCA- FUTURE BUILDERS. Tutor, Auditor Líder / Implementador ISO 22301:2012. 2016.

BAYRON PRIETO CASTELLANOS
DOCENTE

Exdirector del laboratorio de informática forense – Superintendencia de Industria y Comercio. Docente y experto en riesgos informáticos, prueba digital y protección de datos.

Ingeniero de Sistemas, con Especialización en Administración de Riesgos Informáticos de la Universidad Externado de Colombia (2011 – 2012). Con Maestría en Negocios Internacionales y en Business Administration de EUDE Business School (2014 – 2015). Certificado como Examinador Forense por Access Data (ACE) (2014) y Auditor Interno de Calidad (NTCGP 1000:2009 – ISO 9001: 2008) (2013).

INVITADOS ESPECIALES
Centro Criptológico Nacional de España (CCN CERT)

Durante el desarrollo del módulo 1 y 3 del Diplomado, se tendran conferencias con profesionales y expertos del Centro Criptológico Nacional (CCN CERT de España), reconocido a nivel mundial por el desarrollo de capacidades en ciberseguridad, formación y expedición de las guías CCN-STIC de referencia para organismos públicos y privados, para la adecuada gestión y respuesta a incidentes cibernéticos en las organizaciones, permitiendo afrontar de manera activa las ciberamenazas.

RECURSOS TECNOLÓGICOS

Uso de la plataforma Webex. Todos los docentes y estudiantes, deberántener un buen acceso a internet, sonido y cámara para poder facilitar las sesiones.

CERTIFICADOS

La Universidad Ean expide un certificado por participación a quienes asistan al 80% de las sesiones programadas. Los certificados se generan y entregan el día de cierre del programa únicamente a aquellos participantes que hayan cumplido con el mínimo requerido en la presente propuesta en la sesión inmediatamente anterior a la finalización.

DURACIÓN

90 horas