Diplomado en
Liderazgo y Gerencia en Ciberseguridad

Presencial apoyado en el modelo PAT

PRESENTACIÓN

El Diplomado en Liderazgo y Gerencia en Ciberseguridad permitirá fortalecer las capacidades de gerentes de organizaciones frente a la respuesta constante dinámica de la transformación digital. El programa de educación continua permite transferir capacidades tácticas y estratégicas para desempeñar el liderazgo en la proyección e implementación de nuevas ideas de diseño de la seguridad cibernética, generando así, que los futuros egresados cuenten con las capacidades generales para poder orientar y diseñar futuras actividades gerenciales en el campo de la ciberseguridad.

La curva de ascenso del cibercrimen y los ciberataques creció de un incremento del 15%, en la comparación con los datos de Cybersecurity 2022:

- Con relación a esta curva, el incremento del costo va a ser fue de 10.5 trillones de dólares en promedio para el 2025
- Los negocios y los startups van a vincularse en el mundo digital con sus áreas de TI y se propagarán rápidamente hacia 2023.
- Se crearán cerca de 3,5 millones de vacantes posicionales a nivel global dentro del nuevo liderazgo de ciberseguridad.

Los negocios internacionales requieren cada vez mayor confianza y credibilidad sobre las decisiones estratégicas en transformación digital segura.

OBJETIVOS DEL PROGRAMA

GENERAL

Generar estrategias y acciones de prevención y protección frente a retos, amenazas corporativas, y riesgos cibernéticos. Enfocadas en la implementación de tecnologías emergentes; que le va a permitir al egresado garantizar un bagaje con relación a la toma de decisiones de gestión y gobernabilidad de las áreas de la ciberseguridad.

ESPECÍFICOS

- Comprender la importancia de temáticas esenciales que permiten visibilizar el campo de la ciberseguridad en el mundo organizacional.
- Establecer una dinámica de entendimiento frente a los principales fenómenos de las amenazas cibernéticas y el Cibercrimen.
- Focalizar una actividad visionaria y prospectiva en miras de resolver la convergencia de escenarios más difíciles y tecnológicamente más modificados.
- Resolver tareas de manera estratégica y táctica ante los diferentes escenarios de crisis o de manejo de la comunicación ante las partes interesadas.

PERFIL DEL INTERESADO

Perfiles de Gerentes de organizaciones CEO, directores de Seguridad Informática o Seguridad en la Información CISO, jefes o directores de Tecnología CTO, directores o Responsables de la Información CIO, directores o Gerentes de Grupos de Tecnología, protección de los datos y Riesgos COO, involucra perfiles técnicos, estratégicos, tácticos y operativos en organizaciones.

El Diplomado de Liderazgo y Gerencia de la Ciberseguridad está dirigido a los líderes de proceso estratégico, operacional y táctico sobre los principales elementos de la ciberseguridad bajo un esquema de la evaluación crítica y análisis de los proyectos principales en ciberseguridad, al interior de las organizaciones.

METODOLOGÍA

Frente a la transferencia de conocimiento, el estudiante despertará su lado crítico durante 50 horas técnicas sobre los principios marcos de trabajo de ciberseguridad, para poder crear y redisañar nuevos paradigma en donde se impulsen actividades prácticas para poder medir la capacidad de análisis ante una amenaza o riesgo cibernético.

En esa misma vía se realizará un componente académico e mediante la ilustración gráfica, consiscente y creativo para desarrollar su la forma no convencional de pensamiento estratégico, que también contenga 40 horas de estudio o trabajo independiente basado análisis de estrategia, casos de estudio, elementos asincronos y aprendizaje en donde el componente esencial sea la evaluación de su pensamiento frente a la ciberseguridad.

Análisis de contextos: Los cuales le van a permitir al estudiante concretizar hechos conocidos, diferente a los desconocidos para descubrir nuevos paradigmas frente a la implementación de la ciberseguridad.

Apreciación y Análisis: Determinar mediante resultados de ejercicios prácticos, la importancia de la táctica y la estrategia frente a la implementación o no de una tecnología emergente y los riesgos que de esta se derivan.Resultados y ciclo de vida del aprendizaje: Determinar mediante esta metodología: y la combinación de las técnicas gamificadas, la evolución y crecimiento de la actividad de toma de decisiones frente a un evento de ciberseguridad, incidente, riesgo o vulnerabilidad.

Módulo	Contenido	Intensidad
1 CIBERCRIMEN: RIESGOS CIBERNÉTICOS Y AMENAZAS	• Conocimiento teórico práctico de la ciberseguridad y la intersección con la Seguridad Digital, amplificadores de conocimiento en riesgos cibernéticos críticos de la industria 4.0 y las tecnologías emergentes. • El nuevo paradigma del Cibercrimen 4.0: Tipos y clasificación de las víctimas del cibercrimen, organizaciones del crimen emergente, nuevas tecnologías de la ciberdelincuencia, mercados y economías emergentes. EJ. Organización del Ransomware como Economía emergente criminal. • Conductas del adversario estratégico: Técnicas utilizadas por el atacante, derivación del metaverso delincuencial. • Herramientas (Tool Box) táctico: Revisión actual de la intersección de la seguridad digital y la implicación de la ciberseguridad como un eje dinámico y disruptivo, mecanismos de evolución sostenible ante los amenazas avanzadas emergentes y agentes provocadores. • Arcoíris de Metodologías y buenas prácticas: Textura de la convencionalidad del riesgo, frente al riesgo cibernético, definiciones y posturas académicas internacionales bajo un esquema abierto para el elección de marcos de trabajo que sean perdurables en el tiempo. (Investigación del Cibercrimen).	**21 horas**
2 LIDERAZGO ESTRATÉGICO DE LA CIBERSEGURIDAD	Presentar y contextualizar acerca de Assesment Organizacional en Ciberseguridad y la noción del liderazgo aplicado a la Ciberseguridad. • Lo que debe tener una organización para mantenerse (Assurance): 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. • **Componente Táctico de la Ciberseguridad:** Aproximación a la Gobernabilidad y Gobernanza de los sistemas de información y la articulación de componentes resolutivos frente a la amenaza. • **Visión de Gestión de Incidentes y Equipos de Seguridad Cibernética:** Alineación de mejores prácticas para el enfoque del nuevo diseño de ciberseguridad. Enfoque de transparencia, simulaciones adversariales y protección de la fábrica de datos.	**27 horas**
3 CIBERSEGURIDAD RESILIENTE Y COMUNICACIÓN ESTRATÉGICA	• **Ciber resiliencia y sistemas** resilientes (Enfoque de infraestructuras Críticas): 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** • Instituciones públicas, las juntas directivas en Ciberseguridad - c. Insurtech: Retos frente a la celebración de pólizas en Ciberseguridad en las Organizaciones - d. Aplicabilidad y gestión mejora de la Certificación PCI para Instituciones Financieras. - **Threat Intelligence y Hunting Estratégico:** Buenas prácticas y marcos de trabajo gerenciales para abordar las amenazas avanzadas persistentes, diagrama Who am I y who protect me, frente los elementos novedosos de la transformación digital de mi adversario. - **Marca / Reputación:** Monitorización de la comunicación y la publicidad, evolución de la percepción de clientes y mercados, impacto en Resultados, valor de la marca, transparencia en la gestión territorial o transfronteriza de la información etc.	**27 horas**
4 TRANSVERSAL PROYECTO	• **Planeación de un proyecto visionario de la ciberseguridad estratégica en organizaciones.**	**18 horas**

EQUIPO DOCENTE

Expertos en esta área del conocimiento

EMANUEL ORTIZ RUIZ
COORDINADOR ACADÉMICO

Docente de Ciberseguridad Universidad Ean

SANDRA PATRICIA CRISTANCHO
DOCENTE

Directora del Programa de Sistemas – Universidad Ean

Ingeniera de sistemas, Especialista Y Líder de 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. Directora del Proyecto Hackers Wanted colderado por la Organización de Estados Americanos OEA.

JANET GARCIA
DOCENTE

Líder Investigadora y Analista de Delitos Informáticos - Policía Judicial C.T.I. Fiscalía General de la Nación Colombia, servidora pública con una trayectoria de 28 años de experiencia, especialista en Procesamiento y Análisis de la Escena del Crimen, Ponente nacional e internacional en delitos cometidos en los entornos digitales, Analista de Información y Contexto en Delitos Informáticos, Formadora de la Dirección de Altos Estudios de la Fiscalía General de la Nación de Colombia, seleccionada dentro del top de las 25 Mujeres que se visibilizan en Ciberseguridad para Latinoamérica, otorgado por Womcy LATAM.

DIANA PATRICIA ROJAS
DOCENTE

Magister en Ciberseguridad y ciberdefensa, especialista en Seguridad informática, Certificada en PMP, SCRUM Master, Auditor Líder ISO 27001, Auditor ISO 22301, ITIL® Intermediate Certificate in Operational Support and Analysis (ITIL OSA), ITIL® Foundation Certificate in IT Service Management (ITIL V3), amplia experiencia en área de tecnología del sector financiero, Comunicaciones público y privado, Desarrollo de Software con énfasis en procesos, operaciones, administración, Arquitectura Empresarial, Arquitectura TI, gerencia de proyectos desde el diseño, desarrollo, implementación y administración de sistemas de información, elaboración y cumplimiento de presupuestos. Habilidad en el montaje y puesta en marcha de proyectos de renovación tecnológica e implementación de nuevos productos y servicios. Con trayectoria en el campo financiero, público en seguridad de la Información, riesgos tecnológicos, seguridad digital, ciberseguridad y fusión bancaria. Habilidad en el manejo y control de procesos administrativos de contratación, presupuestos, relacionados con tecnología, experiencia en manejo de grupos técnicos y orientado a resultados, capacidad de liderazgo, pensamiento estratégico, construcción y desarrollo al cumplimiento de objetivos, trabajo bajo presión, adaptabilidad al cambio

JUAN CARLOS LOBO
DOCENTE

Administrador de Empresas de la Universidad Ean, Líder 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

MANUEL SANCHEZ RUBIO
DOCENTE

Cierrefico titular del Instituto Nacional Técnica Aeroespacial (Ministerio de Defensa). Además, ejerce como codirector de la Cátedra DARS de ciberinteligencia y es investigador principal del grupo Cibersecuritics de UNIR. Es Codirector de varias Cátedras de ciberseguridad y Ciberinteligencia. Investigador Principal del grupo de investigación Cibersecuritics, y también formador a distintas unidades de Guardia Civil, Policía Nacional y Ejército. Tiene concedidas las medallas al Mérito Policial, la Cruz al Mérito de la Guardia Civil y la Cruz al Mérito Aeronáutico. En el ámbito aeronáutico, lleva más de 25 años en Ensayos en Vuelo y Armamento así como en telemedida, telecomando e instrumentación embarcada.

DAVID JIMENEZ FERNANDEZ
DOCENTE

Es Ingeniero en Informática por la Universidad Politécnica de Madrid, (España), posee más de 20 años de experiencia en el sector IT, es Experto en Ciberseguridad, Perito Judicial Informático/Forense y actualmente se desempeña como Director de desarrollo de negocio en soluciones y servicios de ciberseguridad. Auditor de seguridad de la información en RGPD , ENS, ISO 27001, PCIDSS y Derecho Tecnológico. Tiene amplia experiencia como Asesor técnico y jurídico especializado contra el Cibercrimen. En su trayectoria profesional ha trabajado para empresas y multinacionales de Ciberseguridad Europeas y ha participado en conferencias en Ciberseguridad en Europa y en el continente americano.

RECURSOS TECNOLÓGICOS

Uso de la plataforma Webex. Todos los docentes y estudiantes deberán tener 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 únicamente a aquellos participantes que hayan cumplido con la cantidad mínima de horas según requerido en la presente propuesta.

DURACIÓN

144 horas