



Cursos Superiores

Curso Superior en Ciberseguridad Industrial



INESEM
BUSINESS SCHOOL

INESEM BUSINESS SCHOOL

Índice

Curso Superior en Ciberseguridad Industrial

1. Sobre INESEM

2. Curso Superior en Ciberseguridad Industrial

[Descripción](#) / [Para que te prepara](#) / [Salidas Laborales](#) / [Resumen](#) / [A quién va dirigido](#) /

[Objetivos](#)

3. Programa académico

4. Metodología de Enseñanza

5. ¿Por qué elegir INESEM?

6. Orientación

7. Financiación y Becas

SOBRE INESEM BUSINESS SCHOOL



INESEM Business School como Escuela de Negocios Online tiene por objetivo desde su nacimiento trabajar para fomentar y contribuir al desarrollo profesional y personal de sus alumnos. Promovemos ***una enseñanza multidisciplinar e integrada***, mediante la aplicación de ***metodologías innovadoras de aprendizaje*** que faciliten la interiorización de conocimientos para una aplicación práctica orientada al cumplimiento de los objetivos de nuestros itinerarios formativos.

En definitiva, en INESEM queremos ser el lugar donde te gustaría desarrollar y mejorar tu carrera profesional. ***Porque sabemos que la clave del éxito en el mercado es la "Formación Práctica" que permita superar los retos que deben de afrontar los profesionales del futuro.***

Curso Superior en Ciberseguridad Industrial



DURACIÓN	250
PRECIO	460 €
MODALIDAD	Online

Entidad impartidora:



INESEM
BUSINESS SCHOOL

Programa de Becas / Financiación 100% Sin Intereses

Titulación Cursos Superiores

- Titulación Expedida y Avalada por el Instituto Europeo de Estudios Empresariales “Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad.”

Resumen

La globalización de procesos industriales bajo control de sistemas automatizados e informatizados requiere de técnicos cualificados capaces de gestionar la ciberseguridad de estas instalaciones, ya que el sector industria tiene a contar todos con este tipo de controles. Este curso se prepara para poder hacer frente a las necesidades de seguridad de los sistemas de control industrial SCADA presentes en prácticamente todas las industrias o hacer frente a la implantación de nuevos sistemas bajo criterios de seguridad adecuados. A través del estudio con Inesem serás capaz de alcanzar los conocimientos requeridos para gestionar la seguridad de un sistema informático en entornos de automatización industrial.

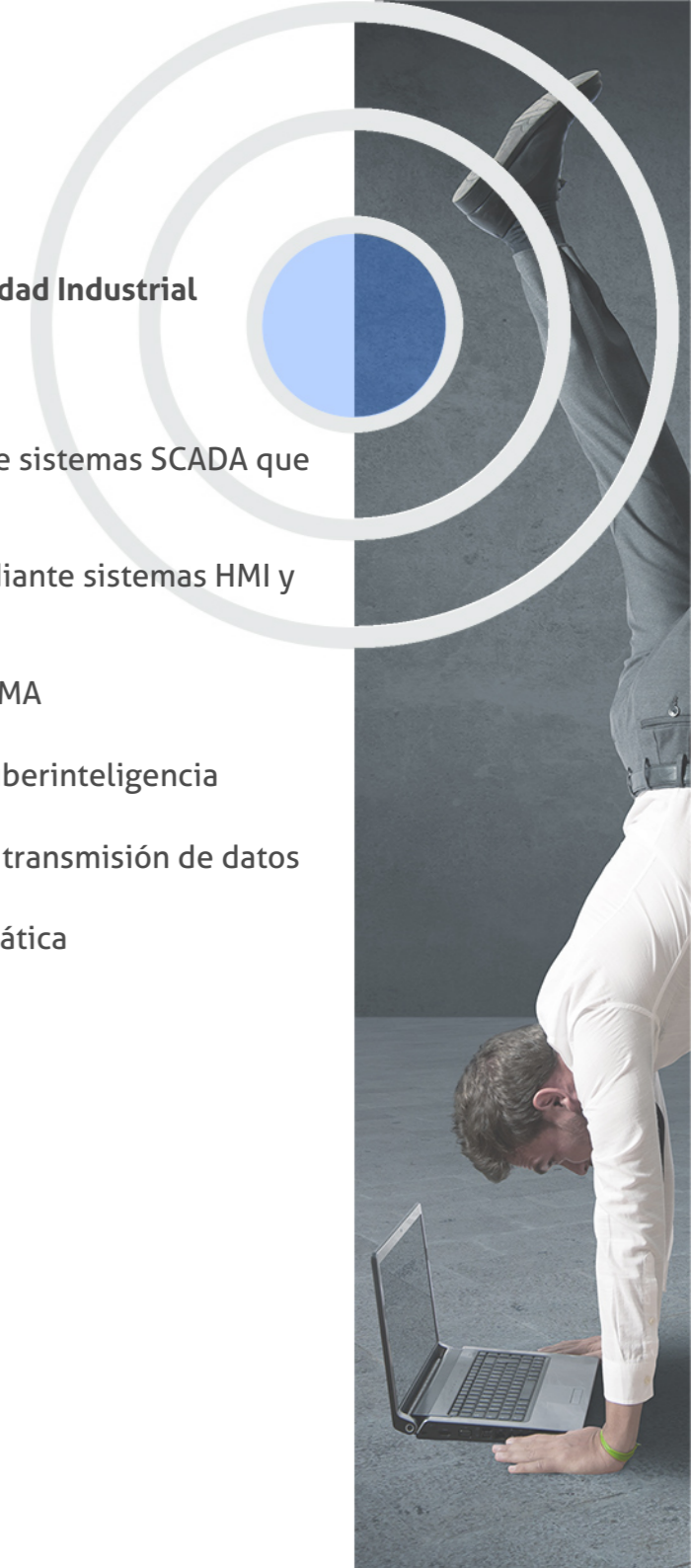
A quién va dirigido

El Curso en Ciberseguridad Industrial está dirigido a cualquier profesional del sector, como técnicos, ingenieros o profesionales TIC que quieran convertirse en experto en la implantación de sistemas de control y seguridad automatizados en producción industrial SCADA y conocer y aplicar la Ciberseguridad y Ciberinteligencia.

Objetivos

Con el Cursos Superiores **Curso Superior en Ciberseguridad Industrial** usted alcanzará los siguientes objetivos:

- Conocer los componentes, características y tipos de sistemas SCADA que existen en el mercado actual
- Desarrollar y profundizar en la monitorización mediante sistemas HMI y SCADA
- Conocer, diseñar e implementar procesos con GEMMA
- Profundizar en los conceptos de ciberseguridad y ciberinteligencia
- Desarrollar y diseñar sistemas seguros de acceso y transmisión de datos
- Prevenir y detectar incidentes de seguridad informática





¿Y, después?

Para qué te prepara

El Curso en Ciberseguridad Industrial te prepara para conocer y profundizar en la monitorización en sistemas HMI y SCADA y gestionar la ciberseguridad y ciberinteligencia para detectar y prevenir incidentes en la seguridad informática. Podrás diseñar e implementar sistemas seguros de acceso y transmisión de datos y procesos con GEMMA, convirtiéndote en un experto en el control y gestión de datos en el sector industrial.

Salidas Laborales

Una vez finalizado el Curso en Ciberseguridad Industrial podrás trabajar en empresas de producción industrial o empresas tecnológicas, donde existe una demanda real de perfiles profesionales como Experto en monitorización con sistemas HMI y SCADA, Analista de Seguridad Informática o Consultor de Ciberseguridad en Entornos Industriales, por lo que podrás poner en práctica lo aprendido en este curso optando a puestos de mayor responsabilidad.

¿Por qué elegir INESEM?



Módulo 1. **Sistemas hmi y scada en procesos industriales**

Módulo 2. **Ciberseguridad: normativa, política de seguridad y ciberinteligencia**

Módulo 3. **Herramientas, técnicas de ciberseguridad y sistemas siem**

Módulo 4. **Ciberseguridad aplicada a inteligencia artificial (ia), smartphones, internet de las cosas (iot) e industria 4.0**

Módulo 1.

Sistemas hmi y scada en procesos industriales

Unidad didáctica 1.

Fundamentos de sistemas de control y supervisión de procesos: scada y hmi

1. Contexto evolutivo de los sistemas de visualización
2. Sistemas avanzados de organización industrial: ERP y MES
3. Consideraciones previas de supervisión y control
4. El concepto de "tiempo real" en un SCADA
5. Conceptos relacionados con SCADA
6. Definición y características del sistemas de control distribuido
7. Sistemas SCADA frente a DCS
8. Viabilidad técnico económica de un sistema SCADA
9. Mercado actual de desarrolladores SCADA
10. PC industriales y tarjetas de expansión
11. Pantallas de operador HMI
12. Características de una pantalla HMI
13. Software para programación de pantallas HMI
14. Dispositivos tablet PC

Unidad didáctica 2.

El hardware del scada: mtu, rtu y comunicaciones

1. Principio de funcionamiento general de un sistema SCADA
2. Subsistemas que componen un sistema de supervisión y mando
3. Componentes de una RTU, funcionamiento y características
4. Sistemas de telemetría: genéricos, dedicados y multiplexores
5. Software de control de una RTU y comunicaciones
6. Tipos de capacidades de una RTU
7. Interrogación, informes por excepción y transmisiones iniciadas por RTU´s
8. Detección de fallos de comunicaciones
9. Fases de implantación de un SCADA en una instalación

Unidad didáctica 3.

El software scada y comunicación opc ua

1. Fundamentos de programación orientada a objetos
2. Driver, utilidades de desarrollo y Run-time
3. Las utilidades de desarrollo y el programa Run-time
4. Utilización de bases de datos para almacenamiento
5. Métodos de comunicación entre aplicaciones: OPC, ODBC, ASCII, SQL y API
6. La evolución del protocolo OPC a OPC UA (Unified Architecture)
7. Configuración de controles OPC en el SCADA

Unidad didáctica 4.

Planos y croquis de implantación

1. Símbolos y diagramas
2. Identificación de instrumentos y funciones
3. Simbología empleada en el control de procesos
4. Diseño de planos de implantación y distribución
5. Tipología de símbolos
6. Ejemplos de esquemas

Unidad didáctica 5.

Diseño de la interfaz con estándares

1. Fundamentos iniciales del diseño de un sistema automatizado
2. Presentación de algunos estándares y guías metodológicas
3. Diseño industrial
4. Diseño de los elementos de mando e indicación
5. Colores en los órganos de servicio
6. Localización y uso de elementos de mando

Unidad didáctica 6.

Gemma: guía de los modos de marcha y parada en un automatismo

1. Origen de la guía GEMMA
2. Fundamentos de GEMMA
3. Rectángulos-estado: procedimientos de funcionamiento, parada o defecto
4. Metodología de uso de GEMMA
5. Selección de los modos de marcha y de paro
6. Implementación de GEMMA a GRAFCET
7. Método por enriquecimiento del GRAFCET de base
8. Método por descomposición por TAREAS: coordinación vertical o jerarquizada
9. Tratamiento de alarmas con GEMMA

Unidad didáctica 7.

Módulos de desarrollo

1. Paquetes software comunes
2. Módulo de configuración Herramientas de interfaz gráfica del operador
3. Utilidades para control de proceso
4. Representación de Trending
5. Herramientas de gestión de alarmas y eventos
6. Registro y archivado de eventos y alarmas
7. Herramientas para creación de informes
8. Herramienta de creación de recetas
9. Configuración de comunicaciones

Unidad didáctica 8.

Diseño de la interfaz en hmi y scada

1. Criterios iniciales para el diseño
2. Arquitectura
3. Consideraciones en la distribución de las pantallas
4. Elección de la navegación por pantallas
5. Uso apropiado del color
6. Correcta utilización de la Información textual
7. Adecuada definición de equipos, estados y eventos de proceso
8. Uso de la información y valores de proceso
9. Tablas y gráficos de tendencias
10. Comandos e ingreso de datos
11. Correcta implementación de Alarmas
12. Evaluación de diseños SCADA

Módulo 2.

Ciberseguridad: normativa, política de seguridad y ciberinteligencia

Unidad didáctica 1.

Ciberseguridad y sociedad de la información

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

Unidad didáctica 2.

Normativa esencial sobre el sistema de gestión de la seguridad de la información (sgsi)

1. Estándares y Normas Internacionales sobre los SGSI. ISO
2. Legislación: Leyes aplicables a los SGSI

Unidad didáctica 3.

Política de seguridad: análisis y gestión de riesgos

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

Unidad didáctica 4.

Ingeniería social, ataques web y phishing

1. Introducción a la Ingeniería Social
2. Recopilar información
3. Herramientas de ingeniería social
4. Técnicas de ataques
5. Prevención de ataques
6. Introducción a Phising
7. Phising
8. Man In The Middle

Unidad didáctica 5. Ciberinteligencia y ciberseguridad

1. Ciberinteligencia
2. Herramientas y técnicas de ciberinteligencia
3. Diferencias entre ciberinteligencia y ciberseguridad
4. Amenazas de ciberseguridad

Unidad didáctica 6. Métodos de inteligencia de obtención de información

1. Contextualización
2. OSINT
3. HUMINT
4. IMINT
5. Otros métodos de inteligencia para la obtención de información

Unidad didáctica 7. Ciberinteligencia y tecnologías emergentes

1. Tecnologías emergentes
2. Desafíos y oportunidades de la ciberinteligencia en las tecnologías emergentes
3. Análisis de amenazas avanzado
4. Usos de las tecnologías emergentes en la ciberinteligencia

Módulo 3. Herramientas, técnicas de ciberseguridad y sistemas siem

Unidad didáctica 1. Comunicaciones seguras: seguridad por niveles

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

Unidad didáctica 2. Criptografía

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4. Criptografía de clave privada o simétrica
5. Criptografía de clave pública o asimétrica
6. Algoritmos criptográficos más utilizados
7. Funciones hash y los criterios para su utilización
8. Protocolos de intercambio de claves
9. Herramientas de cifrado

Unidad didáctica 3.

Aplicación de una infraestructura de clave pública (pki)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

Unidad didáctica 4.

Sistemas de detección y prevención de intrusiones (ids/ips)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

Unidad didáctica 5.

Implantación y puesta en producción de sistemas ids/ips

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

Unidad didáctica 6.

Introducción a los sistemas siem

1. ¿Qué es un SIEM?
2. Evolución de los sistemas SIEM: SIM, SEM y SIEM
3. Arquitectura de un sistema SIEM

Unidad didáctica 7.

Capacidades de los sistemas siem

1. Problemas a solventar
2. Administración de logs
3. Regulaciones IT
4. Correlación de eventos
5. Soluciones SIEM en el mercado

Módulo 4.

Ciberseguridad aplicada a inteligencia artificial (ia), smartphones, internet de las cosas (iot) e industria 40

Unidad didáctica 1.

Ciberseguridad en nuevas tecnologías

1. Concepto de seguridad TIC
2. Tipos de seguridad TIC
3. Aplicaciones seguras en Cloud
4. Plataformas de administración de la movilidad empresarial (EMM)
5. Redes WiFi seguras
6. Caso de uso: Seguridad TIC en un sistema de gestión documental

Unidad didáctica 2.

Ciberseguridad en smartphones

1. Buenas prácticas de seguridad móvil
2. Protección de ataques en entornos de red móvil

Unidad didáctica 3.

Inteligencia artificial (ia) y ciberseguridad

1. Inteligencia Artificial
2. Tipos de inteligencia artificial
3. Impacto de la Inteligencia Artificial en la ciberseguridad

Unidad didáctica 4.

Ciberseguridad e internet de las cosas (iot)

1. Contexto Internet de las Cosas (IoT)
2. ¿Qué es IoT?
3. Elementos que componen el ecosistema IoT
4. Arquitectura IoT
5. Dispositivos y elementos empleados
6. Ejemplos de uso
7. Retos y líneas de trabajo futuras
8. Vulnerabilidades de IoT
9. Necesidades de seguridad específicas de IoT

Unidad didáctica 5.

Seguridad informática en la industria 40

1. Industria 4.0
2. Necesidades en ciberseguridad en la Industria 4.0

metodología de aprendizaje

La configuración del modelo pedagógico por el que apuesta INESEM, requiere del uso de herramientas que favorezcan la colaboración y divulgación de ideas, opiniones y la creación de redes de conocimiento más colaborativo y social donde los alumnos complementan la formación recibida a través de los canales formales establecidos.



Con nuestra metodología de aprendizaje online, el alumno comienza su andadura en INESEM Business School a través de un campus virtual diseñado exclusivamente para desarrollar el itinerario formativo con el objetivo de mejorar su perfil profesional. El alumno debe avanzar de manera autónoma a lo largo de las diferentes unidades didácticas así como realizar las actividades y autoevaluaciones correspondientes.

El equipo docente y un tutor especializado harán un *seguimiento exhaustivo*, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

Nuestro sistema de aprendizaje se fundamenta en *cinco pilares* que facilitan el estudio y el desarrollo de competencias y aptitudes de nuestros alumnos a través de los siguientes entornos:

Secretaría

Sistema que comunica al alumno directamente con nuestro asistente virtual permitiendo realizar un seguimiento personal de todos sus trámites administrativos.

Campus Virtual

Entorno Personal de Aprendizaje que permite gestionar al alumno su itinerario formativo, accediendo a multitud de recursos complementarios que enriquecen el proceso formativo así como la interiorización de conocimientos gracias a una formación práctica, social y colaborativa.

Revista Digital

Espacio de actualidad donde encontrar publicaciones relacionadas con su área de formación. Un excelente grupo de colaboradores y redactores, tanto internos como externos, que aportan una dosis de su conocimiento y experiencia a esta red colaborativa de información.

Webinars

Píldoras formativas mediante el formato audiovisual para complementar los itinerarios formativos y una práctica que acerca a nuestros alumnos a la realidad empresarial.

Comunidad

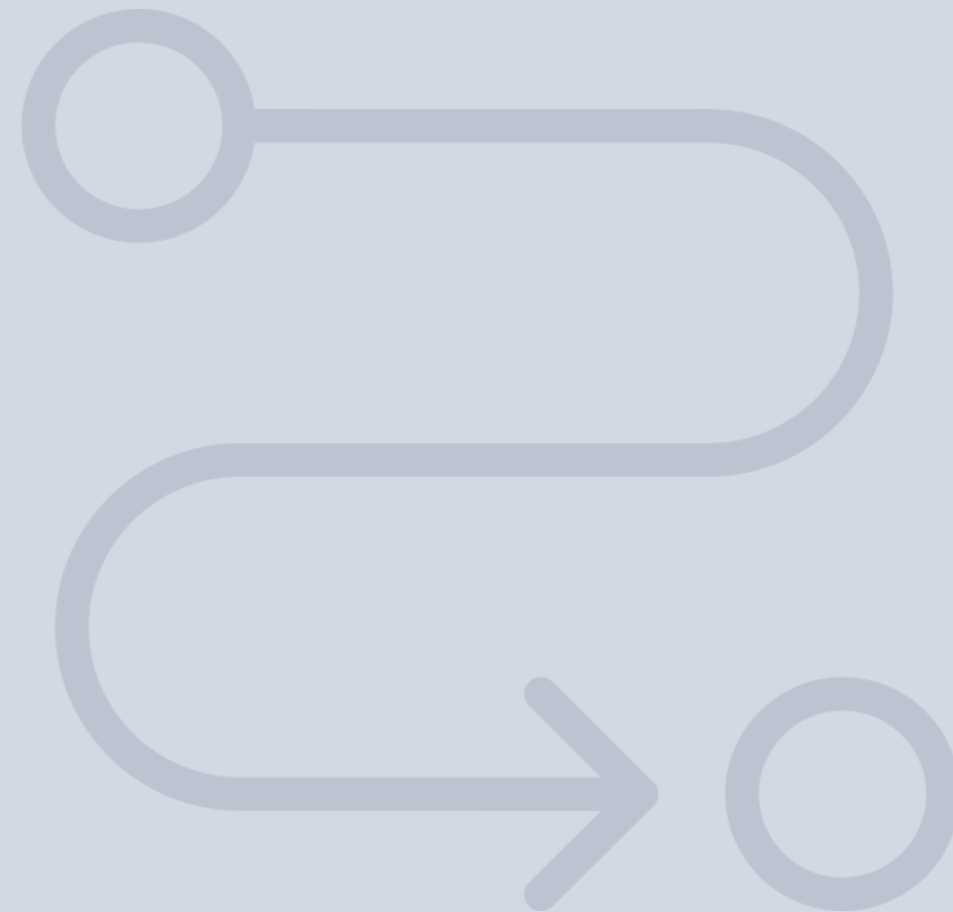
Espacio de encuentro que permite el contacto de alumnos del mismo campo para la creación de vínculos profesionales. Un punto de intercambio de información, sugerencias y experiencias de miles de usuarios.





SERVICIO DE **Orientación** de Carrera

Nuestro objetivo es el asesoramiento para el desarrollo de tu carrera profesional. Pretendemos capacitar a nuestros alumnos para su adecuada adaptación al mercado de trabajo facilitándole su integración en el mismo. Somos el aliado ideal para tu crecimiento profesional, aportando las capacidades necesarias con las que afrontar los desafíos que se presenten en tu vida laboral y alcanzar el éxito profesional. Gracias a nuestro Departamento de Orientación de Carrera se gestionan más de 500 convenios con empresas, lo que nos permite contar con una plataforma propia de empleo que avala la continuidad de la formación y donde cada día surgen nuevas oportunidades de empleo. Nuestra bolsa de empleo te abre las puertas hacia tu futuro laboral.



Financiación y becas

En INESEM

Ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización del pago de matrículas,

todo ello
100%
sin intereses.

INESEM continúa ampliando su programa de becas para acercar y posibilitar el aprendizaje continuo al máximo número de personas. Con el fin de adaptarnos a las necesidades de todos los perfiles que componen nuestro alumnado.



20%	Beca desempleo	Para los que atraviesen un periodo de inactividad laboral y decidan que es el momento idóneo para invertir en la mejora de sus posibilidades futuras.
15%	Beca emprende	Nuestra apuesta por el fomento del emprendimiento y capacitación de los profesionales que se han aventurado en su propia iniciativa empresarial.
10%	Beca alumnos	Como premio a la fidelidad y confianza de los alumnos en el método INESEM, ofrecemos una beca a todos aquellos que hayan cursado alguna de nuestras acciones formativas en el pasado.

Cursos Superiores

Curso Superior en Ciberseguridad Industrial

Impulsamos tu carrera profesional



INESEM
BUSINESS SCHOOL

www.inesem.es



958 05 02 05 formacion@inesem.es

Gestionamos acuerdos con más de 2000 empresas y tramitamos más de 500 ofertas profesionales al año.

Facilitamos la incorporación y el desarrollo de los alumnos en el mercado laboral a lo largo de toda su carrera profesional.