CONSULTOR EN CIBERSEGURIDAD CON CERTIFICACION INTERNACIONAL

PRESENTACION DEL PLAN FORMATIVO COMO CONSULTOR EN CIBERSEGURIDAD CON CERTIFICACION INTERNACIONAL:

Este plan formativo como Consultor en Ciberseguridad con Certificación Internacional, proporciona al estudiante los conocimientos necesarios para implantar y aplicar las técnicas de Ciberseguridad corporativas en cualquier organización independientemente de su tamaño, avalado con las tres certificaciones internacionales siguientes:

- **ISO/IEC 27002 Seguridad de la Información Certificación EXIN Foundation.**
- **CYBER&IT Certificación EXIN Foundation.**
- **ETHICAL HACKING Certificación EXIN Foundation.**

La seguridad de la información, en su sentido más amplio, es una de las mayores preocupaciones de empresas y gobiernos, que han incrementado sus inversiones en protección y detección de manera exponencial en el último lustro. Cualquier dispositivo conectado a Internet es susceptible de ser comprometido si no cuenta con las medidas de seguridad necesarias. De hecho, los robos de información cada vez van más encaminados a portátiles, teléfonos móviles o tabletas electrónicas, más que a bases de datos centralizadas. La razón es que suelen estar menos protegidos y poseen información que podría comprometer todo un país.

El plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** ofrece una formación especializada de primer nivel donde los alumnos adquieren las habilidades, aptitudes y conocimientos avanzados necesarios para desempeñar sus funciones profesionales de consultoría eficazmente en el ámbito de la ciberseguridad.

DESARROLLO DEL PLAN FORMATIVO COMO CONSULTOR EN CIBERSEGURIDAD CON CERTIFICACION INTERNACIONAL

Modalidad de formación: Formación **e-learning personalizada y orientada a objetivos**, con profesores consultores de reconocido prestigio internacional en el ámbito de la Ciberseguridad. Los profesores personalizan la formación en base a los conocimientos previos y tiempo de estudio disponible por el alumno. Es una formación avanzada orientada a la práctica de las técnicas de ciberdefensa y ciberataques de situaciones reales.

Estimación de horas para su realización: 360 horas.

Subvenciones: Este plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** se puede subvencionar a través de los seguros sociales de las empresas por la **Fundación Tripartita**. También se puede subvencionar por diferentes instituciones tanto públicas como privadas para el fomento de las Tecnologías de la Información y la Comunicación a nivel de formación e investigación. Para consultar estas subvenciones y ayudas, no dude en ponerse en contacto con **INTECSSA** llamando al departamento de atención al cliente **+34 91 503 01 35**, o por e-mail a la dirección **depcomercial@intecssa.com.**

Tiempo ilimitado de conexión a la plataforma e-learning

Flexibilidad horaria y geográfica. Formación desde cualquier lugar del mundo y en cualquier momento las 24 horas del día y los 7 días de la semana.

Idioma del curso: Se puede estudiar tanto en español como en inglés.

Profesores: Profesores **certificados** y consultores en formación de tecnologías y metodologías de ciberseguridad, que nos permite garantizar los mejores resultados de aprendizaje. Los profesores personalizan la formación de acuerdo con el nivel de conocimientos de cada alumno.

Contenidos y Documentación: Nuestros contenidos son revisados por nuestro departamento técnico periódicamente, y puestos al día en base a las tendencias de mercado más innovadoras. De igual forma, nuestro departamento de formación selecciona los manuales y materiales a entregar a los alumnos con un criterio profesional y adecuado al contenido y nivel del curso.

Exámenes: Para obtener el diploma correspondiente, el alumno deberá superar al menos el 70% de las pruebas de evaluación y aprendizaje realizadas.

Bolsa de Trabajo: Bolsa de trabajo propia del **Instituto Inertia de Sistemas y Software Avanzado (INTECSSA)** a disposición de los alumnos. Selección de candidatos para las empresas clientes con participación activa del alumno. **Orientación laboral** mediante un individualizado "**Plan de carrera profesional**".

Diploma: Tras la finalización del plan formativo como **Consultor en Ciberseguridad con Certificación Internacional**, se otorga el diploma acreditando los conocimientos adquiridos por el alumno con gran prestigio en el ámbito empresarial. Tras la superación de los exámenes de certificación, el alumno obtendrá la certificaciones oficiales correspondiente.

DESTINATARIOS:

El plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** está especialmente dirigido a:

- Consultores y/o profesionales que quieran prepararse para obtener las certificaciones siguientes:
    - ISO/IEC 27002 Seguridad de la Información Certificación EXIN Foundation.
    - CYBER&IT Certificación EXIN Foundation.
    - ETHICAL HACKING Certificación EXIN Foundation.
- Titulados superiores o medios en informática, telecomunicaciones o similar.

- Personas con experiencia previa en programación y desarrollo de software, así como conocimientos de administración de sistemas operativos y administración de redes.

- También está dirigido a todas aquellas personas que quieran cambiar de rumbo profesional y formarse cómo expertos en técnicas de ciberseguridad corporativa.

OBJETIVOS:

Los tiempos cambian, y los modos de acceder a la información también. **Sería ilógico pensar en sistemas de defensa tradicionales como respuesta a las nuevas amenazas**, las cuales avanzan a la par que la tecnología. Las Amenazas Persistentes Avanzadas (APT por sus siglas en inglés) poseen dos características definitorias: **son muy difíciles de detectar**, puesto que han sido diseñadas de manera *ad-hoc* para un objetivo concreto, y **pueden constituirse por varios módulos que infectan los dispositivos de manera diferente** y a priori, sin relación entre sí, pero nada más lejos de la realidad.

Se suele decir que **una cadena es tan segura como lo es su eslabón más débil.** Esta premisa la conocen los atacantes y, como sus intenciones han cambiado, ya no son sólo adolescentes en sus casas intentando ver hasta dónde pueden llegar, al más puro estilo *Juegos de Guerra*, sino que son ejércitos organizados, con objetivos claramente definidos y además, respaldados por presupuestos millonarios. Si juntamos estos datos con el hecho de que formamos parte de un entorno basado en datos estadísticos, es cuestión de tiempo que estos ataques obtengan resultados con graves consecuencias. A las puertas de 2018, **es necesario que los consejos de administración de las organizaciones o las más altas instancias de nuestros organismos públicos adopten la ciberseguridad como una preocupación real**. Ese será el primer paso para afrontar las soluciones de manera estratégica.

El plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** tiene por objetivo la excelencia de una formación alineada con las necesidades reales de las empresas y organismos públicos que hoy día deben afrontar los riesgos y amenazas provenientes del ciberespacio. Por ello, también incorpora en su programa materias centradas en el estudio y análisis de la seguridad de dispositivos móviles y sistemas de control industrial, dos paradigmas que hoy en día suponen riesgos muy importantes no sólo para ciudadanos y empresas sino también, en el caso de los sistemas de control industrial, para la seguridad nacional.

Por ello, el plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** es sin duda por su contenido, su programa académico, su claustro de profesores y la experiencia del **Instituto Inertia de Sistemas y Software Avanzado (INTECSSA)** en la formación de profesionales del mundo de la ciberseguridad, la mejor opción para afianzar y consolidar una carrera profesional, poniendo a su vez, a disposición de las empresas, la oportunidad de asegurar y proteger el conocimiento global y la información estratégica.

SALIDAS PROFESIONALES:

La demanda laboral de éstos perfiles profesionales se orienta a las organizaciones que necesitan protegerse de las ciberamenazas, y requieren de personal que identifique ataques y debilidades en sus sistemas y redes, y despliegue las medidas más oportunas para asegurarlos durante el ciclo de vida de la seguridad. Este perfil se apoya en mecanismos de ataque y defensa, ensayos y auditorías. Aquí se hallan un número creciente de empresas en sectores críticos empresariales (el financiero, el energético, el de las telecomunicaciones o el del transporte) o públicos (Administraciones Públicas, FF AA o Cuerpos de la Seguridad del Estado).

El plan formativo como **Consultor en Ciberseguridad con Certificación Internacional** está especialmente concebido para trabajar cómo profesionales en los siguientes perfiles:

- Consultor de ciberseguridad.
- Ingeniero o técnico de sistemas seguros.
- Hacker ético.
- Ingeniero o técnico de software seguro.
- Analista de ciberseguridad forense.
- Analista e Ingeniero de malware.

METODOLOGIA APLICADA EN EL PLAN FORMATIVO COMO CONSULTOR EN CIBERSEGURIDAD CON CERTIFICACION INTERNACIONAL:

Durante el desarrollo del plan formativo como **Consultor en Ciberseguridad con Certificación Internacional**, el alumno irá asimilando el contenido teórico de las sesiones de estudio, encontrándose al final de cada una con una serie de ejercicios prácticos que afianzan la teoría, laboratorios de supuestos reales en proyectos en producción, cuestionarios y evaluaciones que pondrán a prueba lo aprendido y servirán para afianzar los conocimientos. Además el alumno tiene un profesor de apoyo que le guiará en todo momento a lo largo de la formación y le resolverá cualquier duda o incidencia que pudiera surgir durante el desarrollo lectivo del mismo.

Los principios sobre los que se basa nuestro método e-learning se relacionan con la practicidad del aprendizaje centrada en el estudiante y en el desarrollo de sus competencias a través de la experiencia. Nuestro principal objetivo es potenciar el impacto en su desarrollo profesional y personal. Para favorecer los estándares de calidad exigibles en un curso técnico de formación del profesorado en TIC, integramos una serie de elementos clave como son: el contenido online que facilita el aprendizaje de conocimientos y habilidades de planificación de tecnologías, procesos y recursos; programas de refuerzo formativo para resolver dudas y ampliar la formación; y casos prácticos para afianzar los conocimientos aprendidos a lo largo de la formación.

El plan formativo como **Consultor en Ciberseguridad con Certificación Internacional**, está realizado con tecnología multimedia aplicando las últimas técnicas didácticas en formación técnica de alto nivel. Durante el curso, el alumno tiene a su disposición el contenido teórico del mismo en formato digital y PDF para su referencia y consulta durante la formación. Este material se puede imprimir para facilitar el estudio al alumno.

DIPLOMA:

El proceso de evaluación es parte inherente del proceso de aprendizaje necesario para la adquisición de las competencias requeridas. Para ello será necesaria la realización de todos y cada uno de los ejercicios, prácticas, test, etc. que se puedan presentar durante la formación, incluyendo los que el profesor pueda añadir. Además se requiere la presentación del proyecto final de curso, finalizado con la competencia que se exige. Finalmente, serán fundamentales las calificaciones obtenidas y la impresión personal del profesor. Cumplidos los términos anteriores, el alumno recibirá el diploma acreditativo de su nivel profesional como **Consultor en Ciberseguridad**. Una vez realizado los exámenes oficiales de Certificación de manera presencial o por internet (EXIN), recibirá la acreditación oficiales siguientes:

- Certificación oficial ISO/IEC 27002 Foundation (EXIN)
- Certificación oficial Cyber&IT Foundation (EXIN)
- Certificación oficial Ethical Hackin (EXIN)

Aquellos alumnos que aun habiendo realizado las actividades prácticas no cumplieran los requisitos de evaluación, recibirán un certificado de matriculación en el plan formativo como **Consultor en Ciberseguridad con Certificación Internacional**.

BOLSA DE EMPLEO:

El Instituto Inertia de Sistemas y Software Avanzado (INTECSSA), cuenta con una amplia Bolsa de Empleo, la cual es un punto de encuentro entre el mundo profesional y el mundo de la formación técnica de calidad. La bolsa de empleo de INTECSSA, proporciona a cualquier empresa la posibilidad de integrar en su plantilla a personal altamente cualificado, formado profesionalmente en nuestra Instituto. Todos los servicios que prestamos son gratuitos y tienen como única finalidad colaborar con las empresas e instituciones de nuestro entorno en la búsqueda de candidatos para cubrir sus necesidades de profesionales cualificados, y así ver satisfechas las aspiraciones de nuestros titulados.

Desde la Bolsa de Trabajo del **Instituto Inertia de Sistemas y Software Avanzado (INTECSSA)**, estamos abiertos a cualquier propuesta de las empresas e instituciones que favorezcan la inserción de nuestros alumnos y fomente las relaciones formación técnica - empresa: presentaciones de empresa, coloquios y seminarios, intercambios internacionales, jornadas de orientación, etc.

ORIENTACION DE INTECSSA A SERVICIOS Y CONSULTORIA:

Nuestra experiencia Internacional en la elaboración y entrega de Programas de Formación y en el Diseño y Desarrollo de Soluciones a Medida, nos permite tener un conocimiento global de las necesidades y competencias que las organizaciones necesitan desarrollar para alcanzar sus objetivos y ser más competitivos.

En un mercado global, las organizaciones y sus políticas de gestión de los RRHH, requieren servicios de consultoría como los que ofrece el **Grupo Inertia Technology** en el mundo; capaces de entender el negocio y dar apoyo a sus estrategias de cambio y gestión del talento en los actuales mercados, tanto multinacionales como locales. En España, el **Instituto Inertia de Sistemas y Software Avanzado (INTECSSA)** como empresa de formación en TI perteneciente al **Grupo Inertia Technology**, desarrolla los siguientes Servicios de Consultoría en Formación:

- Organización y Gestión de la Formación.
- Gestión de Habilidades y Actitudes.
- Diseño y Configuración de Estrategias de Formación y Aprendizaje.
- Consultoría y Desarrollo de Modelos de Formación: (Presencial, e-Learning, Blended, mobile-Learning).
- Gestión del Cambio de Personas.

El Servicio de Outsourcing de Formación tiene como objetivo apoyar a las empresas en las necesidades de formación de sus empleados en Tecnologías de la Información (TI), lo que les permite la adopción de procesos globales y el aprendizaje integrado de gestión y formación.

Ponemos a su disposición un equipo de profesionales adaptado a su proyecto. Nos aseguramos de aportar la experiencia adecuada a las necesidades del proyecto y de mantener un proceso formativo constante, asegurándole así el éxito del mismo y la flexibilidad que esto representa en tiempos y costes.

La metodología de Gestión del **Instituto Inertia de Sistemas y Software Avanzado (INTECSSA)** apoya a la empresa en las diferentes fases del ciclo de formación.

TEMARIO

CONSULTOR EN CIBERSEGURIDAD CON CERTIFICACION INTERNACIONAL

El programa de estudios se estructura alrededor de tres grandes bloques de Fundamentos de Ciberseguridad (Ciberdefensa, Ciberataque e Ingeniería Social) y a continuación el estudio y preparación de las tres certificaciones internacionales:

TECNICAS DE CIBERDEFENSA

- **1: Introducción a la Ciberseguridad**
  - **Conceptos Fundamentales de Ciberseguridad**
  - **Naturaleza del Ciberespacio**
  - **Ámbito de la Ciberseguridad**
  - **Confidencialidad**
  - **Integridad**
  - **Autenticidad**
  - **Trazabilidad**
- **2: Estándares y Normativas de Seguridad de la Información**
  - **Conjunto de normas ISO 27000**
  - **ISO 27032: Ciberseguridad**
- **3: Amenazas a la Ciberseguridad**
  - **Vulnerabilidades**
  - **Amenazas**
  - **Agentes**
  - **Mecanismos de Ataque**
  - **Evaluación y Gestión de Riesgos**
- **4: Incidentes de Ciberseguridad**
  - **Ciberguerra**
  - **Ciberespionaje**
  - **Pasos de un Ataque a la Ciberseguridad**
  - **Footprinting y Reconnaisance**
  - **Escaneo de Redes**
  - **Escaneo de Puertos con Nmap**

TECNICAS DE CIBERATAQUE

- **5: Hacking del Sistema**
  - **Metasploit**
  - **Meterpreter**
  - **Protección de Datos**
- **6: Sniffing de Red**
  - **Sniffers**
  - **ARP Spoofing**
  - **MITM**
  - **Secuestro de Sesiones**
- **7: SQL Injection**
  - **Introducción a SQLi**
  - **Blind SQL Injection**
- **8: Técnicas**
  - **Ciberguerra**
  - **Data Leak Prevention**
  - **Anonimato y Deep Web**
  - **Criptografía**
  - **Demostración: Implementación de una VPN**
  - **Denegación de Servicio Demostración: Implementación de un ataque DoS**
- **9: Malware**
  - **Introducción al Malware**
  - **Troyanos y Backdoors**
  - **Virus y Gusanos**
  - **0-days**
  - **RATs**

GESTION DE LA CIBERSEGURIDAD

- **10: Ingeniería Social**
  - **Introducción a la Ingeniería Social**

- **Hacking con Buscadores**
- **Suplantación de Identidad**
- **Robo de Contraseñas**
- **Phishing**
- **Spear Phishing**
- **Guías para Ciberseguridad**
- **Guías para Usuarios**

11: Principios de Seguridad

- **Controles de Seguridad Técnica para Usuarios Finales**
- **Guías para Organizaciones**
- **Controles de Ciberseguridad**
- **Contramedidas contra Ataques de Ingeniería Social**
- **Políticas**
- **Métodos y Procesos**
- **Personas y Organización**

CERTIFICACIONES INTERNACIONALES

ISO/IEC 27002 Seguridad de la Información Certificación

- **Módulo 1 - Información y seguridad**
  - **El concepto de información**
  - **El valor de la información**
  - **Aspectos de la fiabilidad**
- **Módulo 2 - Amenazas y riesgos**
  - **Amenaza y riesgos**
  - **Relaciones entre amenazas, riesgos y la fiabilidad de la información**
- **Módulo 3 - Enfoque y Organización**
  - **Política de seguridad y organización de la protección de la información**
  - **Componentes**
  - **Gestión de incidentes**
- **Módulo 4 - Medidas**
  - **Importancia de las medidas**
  - **Medidas físicas de seguridad**
  - **Medidas técnicas**

- **Medidas organizativas**

- **Módulo 5 - Redes Legislación y normas**

CYBER&IT Certification EXIN Foundation

- **Módulo 1 - Redes**
  - **TCP / IP**
  - **Protocolos de red**
  - **Equipos de red (switches, routers, NAT, etc.)**
  - **Filtros de red (firewalls, proxies, detección de intrusos, inspección profunda de paquetes, filtrado de contenido)**
  - **Red de almacenamiento (SAN, NAS) Redes ◦ TCP / IP**

- **Módulo 2 - Sistemas**
  - **Arquitectura de la computadora (componentes de hardware)**
  - **Sistemas operativos (gestión de hardware, procesos y usuarios)**
  - **Sistemas cliente-servidor**
  - **Soluciones de cliente ligero (Citrix, etc.)**
  - **Virtualización**

- **Módulo 3 – Bases de Datos**
  - **Tipos de bases de datos**
  - **Integridad de la base de datos**
  - **Directorio de Servicios**
  - **Técnicas de ataque y seguridad**

- **Módulo 4 – Criptografía**
  - **Encriptación simétrica y asimétrica**
  - **Certificaciones**
  - **Infraestructura de Clave Pública**
  - **SSL / TLS**
  - **S / MIME**
  - **VPN**

- **Módulo 5 – Gestión del acceso**
  - **Técnicas de identificación y autenticación**
  - **Autorización**
  - **Protocolos de uso frecuente (SAML, OpenID, OAuth, etc.)**

- **Módulo 6 – Nube**
    - **Tipos de Nube (IaaS, PaaS, SaaS)**
    - **Modelos de implementación (públicos, privados, híbridos)**
    - **Seguridad como servicio**
    - **Acceso en la nube**
    - **Riesgos y medidas específicas**
- **Módulo 7 – Vulnerabilidades**
    - **Seguridad del software**
    - **Malware**
    - **Técnicas de ataque**
    - **Modelos de seguridad disponibles (OWASP, CERT, BSI, FSS, etc.)**

ETHICAL HACKING Certificación EXIN Foundation

- **Módulo 1 – Fundamentos de Ethical Hacking**
    - **Hacking ético**
    - **Principios Básicos**
- **Módulo 2 – Network Sniffing**
    - **Herramientas**
    - **Extraer información**
- **Módulo 3 – Hacking Redes Wireless**
    - **Preparación**
    - **Aircrack-NG**
- **Módulo 4 – Penetración de Sistemas**
    - **Intel Gathering**
    - **Fingerprinting & vulnerabilidades**
    - **Herramientas Software (Nmap, Metasploit)**
    - **Exploitation & Post exploitation**
- **Módulo 5 – Web based Hacking**
    - **Ataques a Base de datos**

- **Ataques del lado Cliente**
- **Ataque del lado Servidor**