Presentación

Actualmente, **IOE Business School** se ha convertido en todo un referente a la hora de hablar de formación de calidad. En nuestros más de veinte años de trabajo no hemos descansado ni un solo momento para proveer a nuestros alumnos de la mejor **oferta educativa**. Es por eso que establecemos y contamos con una amplia cartera de alianzas con las mejores universidades que acreditan nuestros estudios. Además, los profesionales mejor valorados de los diversos sectores se encuentran en nuestras filas. El objetivo es simple y exitoso.

Nuestros egresados se consolidan como los mejores profesionales de sus ámbitos laborales. Con el objetivo claro de seguir formando a los mejores expertos, lanzamos el máster experto en Seguridad Informática. Estos estudios están destinados, sobre todo, a aquellos que quieran destacar en el ámbito de la seguridad en la red de redes.

Este programa enfocado a la Seguridad Informática nace ante una necesidad apremiante de formar profesionales en **seguridad de la información**. El máster en **ciberseguridad** responde a las necesidades actuales que se plantean en el ámbito de los sistemas de información. Cada vez son más las empresas que demandan profesionales capacitados para proteger sus sistemas informáticos y redes. Esto se debe a que son conscientes del **aumento de amenazas** y de la **necesidad de proteger sus sistemas**.

Con este postgrado en Seguridad Informática se pretende proporcionar los conocimientos necesarios. Con ellos se podrán elaborar **estrategias** de actuación desde dos puntos de vista. Es decir, desde el **hacking** y desde el **administrador de redes y sistemas**. De esta manera, el alumno que curse nuestros estudios de **Seguridad Informática** conseguirá un gran desarrollo profesional en el ámbito de la Seguridad Informática.

Formación en el máster en ciberseguridad online

Del mismo modo, un aspecto esencial que también se aborda en este máster en ciberseguridad es el **Hacking Ético**. También se conoce este concepto como **Ethical Hacker**. Consiste, principalmente, en que una persona se convierte en **ciberdelincuente** y simule ataques a una empresa. Además, el **analista de seguridad** que egresa de nuestro postgrado en Seguridad Informática, tiene como objetivo que la empresa conozca el estado real de seguridad.

También se tratarán en este máster de Seguridad Informática de manera detallada, algunos aspectos claves. Éstos nos permitirán realizar esta actividad como, por ejemplo, que se necesita autorización de la empresa.

En el mercado actual, además de tener experiencia profesional, es muy importante contar con conocimientos. Los mismos han de ser sólidos y actualizados, sobre todo en el campo de la ciberseguridad. Con este programa enfocado a la Seguridad Informática el alumno obtendrá las competencias necesarias para desarrollarse personalmente en este campo.

Una oferta puntera de formación con el postgrado de Seguridad Informática online de IOE

Nuestro máster en Seguridad Informática muestra al alumno que para **auditar la seguridad de una empresa** es necesario tener una comprensión general sobre qué es seguridad. Los **auditores de sistemas** están muy demandados en la actualidad, como veremos en el programa de estudios en ciberseguridad. Por tanto, abordaremos que la seguridad es un proceso y no un producto. No resulta posible anticipar cada vector de ataque. Sin embargo, se pueden alcanzar altos niveles de seguridad si se realiza una planificación estratégica adecuada.

Con este programa de estudios de máster en Seguridad Informática, el estudiante conseguirá ayudar a las empresas a alcanzar sus objetivos. Específicamente, aquellos que se enfocan a la seguridad mediante los **instrumentos** necesarios para integrar rasgos de seguridad. Esto se debe aplicar a los muchos aspectos que tiene la red.

Por tanto, la seguridad es un sistema para mejorar el mapa de políticas y los procedimientos. Y, lo que es más importante, mejora los conductores del negocio que hacen que las empresas quieran salvaguardar su activo. Los estudios de Seguridad Informática dan buena cuenta de todo ello.

Entender la seguridad y fomentar la protección de datos

Para entender la seguridad y poder revisarla como sistema, el alumno tiene que ser capaz de identificar cómo se mantiene todo de manera conceptual. En definitiva, la seguridad es un asunto amplio. Abordaremos la cuestión en el desarrollo del programa en Seguridad Informática.

Además, es uno de los pocos en la tecnología de la información que, literalmente, toca todos los aspectos de un negocio. Por lo tanto, la **administración del riesgo** es uno de los factores más importantes en el desarrollo de una estrategia para proteger a la gente, la tecnología y los datos. Para enfocar los esfuerzos de seguridad y hacerlos manejables, ayudar a descomponer los aspectos de seguridad en los cinco pilares de seguridad. Estos son los siguientes:

- Evaluación.
- Prevención.
- Detección.
- Reacción.
- Recuperación.

Aproximación a la seguridad de redes en los estudios de postgrado en Seguridad Informática

La seguridad de la red se ha considerado importante para aquellos que pasan una gran parte de su carrera en este campo. Esta premisa es básica en nuestro postgrado en Seguridad Informática. En la actualidad hemos podido percibir un aumento del interés público. Esta creciente demanda se ha localizado en el último año.

Esto es así debido a acontecimientos que han afectado incluso a la persona técnicamente más experta. Es este un aspecto que estos estudios en ciberseguridad abarcarán ampliamente. La seguridad se ha vuelto más compleja que nunca. Los motivos y las capacidades de los actores amenazantes continúan evolucionando, como veremos en el máster en Seguridad Informática.

Además, el concepto de localización de los datos se está haciendo confuso por conceptos de **Cloud Computing** y redes de datos de contenido y balanceo de carga global.

Hoy en día nos esforzamos por fortalecer a los empleados de todo el mundo con acceso omnipresente a datos importantes. Por ello, cada vez es más importante permanecer constantemente vigilantes sobre la protección de datos y entidades que los utilizan. Esta es una de las metas que cimentan el postgrado en Seguridad Informática de IOE Business School.

¿Cuáles son los objetivos de seguridad en la red?

El máster en Seguridad Informática de IOE Business School se encargará de analizar diferentes perspectivas sobre las redes. Por ejemplo, en el desarrollo de las sesiones, los alumnos del postgrado en seguridad informática podrán ver que, según la persona:

- Los **técnicos de red** podrían considerar que sus redes son el centro del universo.
- La **alta dirección** podría ver la red como una herramienta de negocios para facilitar los objetivos de la empresa.
- Los **usuarios finales** podrían considerar la red solo como una herramienta para que ellos puedan hacer su trabajo. O, posiblemente, como una fuente para la recreación.

No todos los usuarios aprecian su papel de mantener los datos seguros. Atenderemos especialmente a esta premisa en los estudios de ciberseguridad. Desafortunadamente, los usuarios de la red representan una **vulnerabilidad** significativa.

Esto es porque tienen nombres de usuario y contraseñas, que les permiten acceder a la red. Si un usuario está comprometido o un individuo no autorizado obtiene acceso a datos, aplicaciones o dispositivos para los que no debería tener acceso, hay un problema. Como se verá en el programa de Seguridad Informática, la seguridad de red puede incluso fallar como resultado.

En el postgrado en Seguridad Informática haremos hincapié en algo importante. Se trata de recordar el comportamiento de los usuarios. Éste plantea un riesgo para la seguridad. Además, conviene resaltar que la formación de los usuarios es una parte clave de una política de seguridad integral.

Las amenazas actuales de la red

Las amenazas a las que nos enfrentamos hoy en día están cambiando constantemente. De manera continua emergen otras nuevas. Por tanto, como veremos en el programa de estudios de Seguridad Informática, es muy importante tener conocimientos sobre seguridad e la información. En este programa en ciberseguridad los alumnos verán los tipos de adversarios que pueden encontrarse detrás de los ataques.

Estos pueden ser:

- Criminales.
- Estados nacionales.
- Empleados descontentos.
- Cualquier persona con acceso a un dispositivo informático.
- Terroristas.
- Agencias gubernamentales.
- Hackers.
- Competidores.

En el transcurso de nuestro máster en Seguridad Informática veremos que existen diferentes términos para referirse a estos individuos. Por ejemplo:

- Hacker/cracker (criminal hacker).
- Script-kiddie.
- Hactivist.
- Etcétera.

Como profesional de la seguridad y tal y como veremos en los estudios de postgrado en Seguridad Informática lo primero que se quiere es entender al **enemigo**. Es bueno entender las motivaciones e intereses de las personas involucradas en romper todas esas cosas que se pretende proteger.

También es necesario tener una buena comprensión de la red y de los datos para saber qué es vulnerable. Además, conviene saber cuáles pueden ser los objetivos de los actores maliciosos.

En el transcurso de nuestro máster de Seguridad Informática entenderemos que algunos atacantes buscan ganancias financieras. Otros podrían querer la notoriedad que viene de atacar a una empresa bien conocida o marca. A veces los atacantes lanzan sus amplias redes y dañan compañías tanto de forma intencionada como sin pretender hacerlo.

Servicios y Seguridad Informática, palabras clave para formar al nuevo profesional

Los **servicios**, como se abordará en el máster de Seguridad Informática, son los principales puntos de vulnerabilidad para los atacantes. Estos pueden aprovechar los privilegios y capacidades de un servicio para obtener acceso al servidor local o a otros servidores de la red.

Los servicios que no autentican a los clientes, los que utilizan protocolos que no son seguros o los que se ejecutan con demasiados privilegios representan un riesgo especial. Si no se necesita utilizar un determinado servicio, en el transcurso de las sesiones de Seguridad Informática veremos que debería estar deshabilitado. Deshabilitar los servicios innecesarios es un método rápido y sencillo para reducir la superficie de ataque.

Por esta razón, en este programa en ciberseguridad, profundizaremos sobre estos tres puntos:

- Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios. En nuestro máster en Seguridad Informática haremos uso de escáneres de red para averiguar posibles fallos de seguridad.
- Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información. En este caso haremos hincapié en los servicios de máquinas con sistema operativo Windows debido a que se encuentra más extendido.
- Utilización de herramientas de **análisis de tráfico de comunicaciones** para determinar el uso real que hacen los

sistemas de información de los distintos protocolos, servicios y puertos. Aprenderemos a utilizar software que nos permita recabar información sobre el tráfico de la red y a saber interpretarla.

La criptografía para la seguridad de la información

Otro de los puntos fuertes de este programa en ciberseguridad es el ámbito de la **criptografía**. Esta disciplina proporciona niveles adicionales de seguridad a los datos durante el procesamiento, el almacenamiento y las comunicaciones.

A lo largo de los años, los matemáticos y los informáticos desarrollaron una serie de algoritmos cada vez más complejos. Éstos, como comprobarán los alumnos del programa de estudios en Seguridad Informática, estaban diseñados para garantizar:

- La integridad.
- La no-repulsión.
- La confidencialidad.
- La autenticación.

Durante ese mismo periodo, los hackers y los gobiernos dedicaron recursos significativos a socavar esos **algoritmos criptográficos**. Esto llevó a una carrera armada en la criptografía y dio lugar al desarrollo de los algoritmos extremadamente sofisticados que se usan hoy en día. En este máster en Seguridad Informática se examinará la historia de la criptografía, los fundamentos de las comunicaciones criptográficas y los principios de los **criptosistemas de clave privada**.

Los factores de políticas de seguridad, analizados en el postgrado de Seguridad Informática

Cuando definimos las **políticas de seguridad**, en el ámbito del máster en Seguridad Informática, lo hacemos con el objetivo de implantarlas. Al llevarlas al seno de una entidad, tenemos que tener en cuenta los siguientes factores:

- Alcance: conjunto de recursos, instalaciones y procesos de la entidad.
- Objetivos de seguridad que se pretenden alcanzar.
- Información y activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes que se ven involucrados cuando se implantan las medidas de seguridad.
- Definición de directrices de personal.
- Caracterización de medidas, normas y procedimientos de seguridad.
- Gestión de incidencias.
- Planes de contingencia.
- Cumplimiento de las leyes vigentes.
- Definición de consecuencias debidas al incumplimiento de las Políticas de Seguridad.

Como podrán ver los alumnos en este programa en Seguridad Informática, es recomendable también realizar un estudio previo. Éste ha de versar sobre las medidas y criterios definidos en las políticas de seguridad por parte de los asesores legales de la organización.

La correcta implantación de políticas de seguridad, eje vertebrador del postgrado en Seguridad Informática

Por otra parte, en el máster en Seguridad Informática veremos que es necesario dar a conocer cierto tipo de información a los empleados. Deben saber cuáles son los planes, normas y procedimientos adoptados por la organización.

Hay que establecer de forma clara y precisa cuáles son las actuaciones exigidas, las recomendadas y las totalmente prohibidas dentro del sistema de información. También han de saber cómo será el acceso a los distintos recursos de información de la organización, como verán los alumnos del máster en Seguridad Informática. Además, en los procedimientos de seguridad será necesario especificar otra información adicional:

- Personas o departamentos responsables de su ejecución.
- Controles para verificar su correcta ejecución.
- Descripción detallada de las actividades que se deben ejecutar.
- Momento y/o lugar en que deben realizarse.

Como se podrá estudiar en el programa enfocado a la Seguridad Informática, las **políticas de seguridad** constituyen una herramienta valiosa. Con ellas se podrá hacer frente a futuros problemas, fallos de sistemas, imprevistos o posibles ataques informáticos.

Sin embargo, se puede incurrir en una **falsa sensación de seguridad** si las políticas de seguridad no se han implantado correctamente en toda la organización. En consecuencia, la entidad tiene que conseguir una **implantación real y eficaz** de las medidas y directrices definidas. Para ello, como se verá en el máster en Seguridad Informática, será necesario contar con el compromiso de todo el personal de la organización.

Así mismo, la organización debe verificar el nivel de cumplimiento e implantación de las políticas de seguridad. Por tanto, debe realizar **auditorías de seguridad** y **revisiones periódicas**. El máster en ciberseguridad de IOE aborda todas estas cuestiones. Otra medida que contribuye a una adecuada implantación sería la actualización y revisión de las políticas de seguridad cuando sea necesario, manteniendo plenamente vigentes las directrices y medidas establecidas.

Otro punto fuerte del máster en Seguridad Informática: la seguridad física en las instalaciones

Los lugares donde estén situados los equipos con información sensible de la organización tienen que estar protegidos de una manera especial. Por tanto, se han de garantizar los factores de **confidencialidad**, **integridad** y **disponibilidad** de los datos. Estos lugares deben ser zonas dentro del local que eviten futuras incidencias de seguridad. Generalmente, una organización de tamaño mediano o grande dispondrá de una sala especialmente acondicionada.

En ella se podrán ubicar los servidores centrales con todos los ficheros y aplicaciones informáticas. Se debería implantar **un sistema de control de acceso físico** a esta sala, como veremos en el programa en Seguridad Informática. En cualquier caso solo se debe permitir la entrada a personal debidamente autorizado y relacionado con el **Sistema de Información**.

El programa de postgrado en Seguridad Informática se preocupa por la ciberseguridad en el ámbito nacional

Desde hace algunos años, como se estudiará en el programa experto en ciberseguridad, se ha producido un **auge de la seguridad informática desde el punto de vista gubernamental**. El Gobierno de España se ha encargado de crear organismos que se encargan de emitir informes y reportes de acción. Además, en el transcurso del postgrado en Seguridad Informática se verá que también se ha intentado crear un estándar en lo referente a este tipo de seguridad.

Debido, pues, al aumento desmesurado de ataques hacia infraestructuras de los distintos estados, surge la necesidad de crear estrategias, organismos y medidas de control. Su función es impedir, o al menos detectar dichos ataques o intentos de ataque.

En el máster de Seguridad Informática veremos que, mayoritariamente, se ha demostrado a lo largo del año 2013 que estos ataques tienen diferentes orígenes. Con frecuencia, proceden de otros países, cuyas relaciones diplomáticas no están del todo claras. También sucede con países que buscan algo con interés.

Estas cuestiones serán tratadas ampliamente en el marco del programa en ciberseguridad. Nuestro máster en Seguridad Informática aborda la legislación sobre la protección de bienes informáticos y sistemas de información. Y por otro lado, la legislación sobre la protección de datos también es estudiada. Es importante conocer la normativa penal de los comportamientos delictivos asociados a este tipo de protección.

Conocer y comprender la legislación dirigida a la protección de bienes informáticos y sistemas de información será una de las máximas de estos estudios en Seguridad Informática. Del mismo modo, los alumnos dominarán el despliegue de su actividad, en especial la regulación penal de los comportamientos delictivos asociados.

Aspectos legales y regulatorios en la seguridad informática

Este máster en Seguridad Informática pretende que al alumno conozca detalladamente:

- La finalidad de la Ley de Protección de Datos.
- La Ley de Protección de Datos y su Reglamento y aplicación en España.
- La forma en la que se debe aplicar la Ley de Protección de Datos.

La protección de los datos personales de los ciudadanos es un tema de constante actualidad y sensible opinión pública. Como veremos en el programa de estudios en Seguridad Informática, esto ocurre sobre todo en cuanto a la seguridad jurídica que los mismos requieren y por los derechos que se ven afectados.

La sociedad de la información en la que nos movemos en la actualidad y su pretendida libre circulación de datos, choca en muchas ocasiones con el respeto a los derechos personales. Los ciudadanos, como veremos en el máster en Seguridad Informática ven vulnerado su derechos y sus datos personales son utilizados de forma inadecuada.

En el postgrado de Seguridad Informática se atenderá a la legislación española vigente. Ésta trata de proteger dichos derechos. Da cumplimiento a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 25 de octubre de 1995, a través de la **Ley Orgánica de Protección de Datos 15/1999** de 13 de diciembre, desarrollada a su vez por el Reglamento 1720/2007. Con ella, como abordan los estudios en Seguridad Informática, se pretende proteger y garantizar el tratamiento de los datos personales. Además, según el temario del máster de Seguridad Informática, también protege las libertades públicas y los derechos fundamentales de las personas físicas.

En concreto, el postgrado especializado en Seguridad Informática nos indica que se encarga de todo lo relativo al honor e intimidad personal. El contenido de los derechos que se protegen por medio de esta legislación es el mismo que se ha protegido con anterioridad a la introducción de los medios informáticos. Lo que vemos que varía es el modo de protección, según el máster en Seguridad Informática.

Quizá te interese:

- Máster en Ciberseguridad
- Máster en Gestión por Procesos (Sistema ERP)

Objetivos

- Profundizar en el concepto de **seguridad informática**, tanto a nivel de sistemas como de protección de la información.
- Analizar los **distintos tipos de amenazas y vulnerabilidades** a los que se enfrenta un **sistema informático** de una empresa.
- Aprender y conocer los **mecanismos de protección** adecuados con el objetivo de auditar y detectar intrusos.
- Abordar un **modelo de experimentación** para ponerlo en práctica sobre redes que están protegidas y son **inmunes a los ataques**.
- Detectar las **vulnerabilidades** y los **posibles ataques a las redes TCP/IP** de una organización.
- Profundizar detalladamente en las **diferentes técnicas de exploración de puertos**.
- Aprender y aplicar las diferentes **técnicas para la protección de la información** en las redes y **sistemas telemáticos**.
- Ser capaz de proteger la **seguridad inalámbrica** con el fin de que la **seguridad informática** de una empresa se mantenga confiable.
- Estar al tanto de los **ataques más utilizados** junto con la **utilización de herramientas de respuesta** ante estos.
- Implementar y mejorar la **Seguridad Informática** en una organización.

Plan de Estudios

Asignatura 1. **Seguridad informática e implementación en la empresa.**

- Seguridad informática en la empresa.
- Seguridad de los sistemas de información.
- Seguridad y protección de la información empresarial.
- Criptografía.
- Firewalls hardware y software.
- Robustecimiento de sistemas.
- Identificación de servicios.

Asignatura 2. **Organización de la seguridad de la información.**

- Confianza, seguridad y sociedad de la información.
- Tecnología y organización de la seguridad de la información.
- La infrastructura para la construcción de confianza.
- Marco normativo y regulatorio de la seguridad y comercio electrónico.

Asignatura 3. **Ciberseguridad, criptografía y delitos telemáticos.**

- Conceptos sobre seguridad de comunicaciones y criptografía.
- Malware, hacking y ddos.
- Hardening.
- Auditoría y detección de intrusos en el sector empresarial.
- Delitos tipificados y fichas técnicas de los delitos telematicos.

Asignatura 4. **Ataques a redes TCP/IP.**

- Teoría de redes. Protocolo TCP/IP.
- Técnicas de seguimiento, exploración y enumeración.
- Exploración del objetivo.
- Tipos de ataques TCP/IP en las organizaciones.
- Debilidad de los protocolos TCP/IP en las organizaciones.

Asignatura 5. **Ataques a redes inalámbricas. Métodos de penetración wifi.**

- Introducción al ataque a redes.
- Parámetros de estudio. Estructura y topología de redes inalámbricas.
- Equipos inalámbricos wifi a utilizar y relación de rastreos sobre posibles víctimas.
- Fases de ataque a una red inalámbrica.

Asignatura 6. **Técnicas y herramientas de protección de redes para las empresas.**

- Protección a nivel de red.
- Ataques a redes e intrusiones.
- Protección de sistemas.
- Servidores big data y datos en streaming.
- Impacto de las tecnologías Big Data en protección de datos.

Asignatura 7. **La ciberseguridad desde el ámbito judicial.**

- Derecho, deberes y código deontológico del perito informático.
- Evidencias judiciales.
- Organismos relacionados con la ciberseguridad internacionales.
- Organismos relacionados con la ciberseguridad nacionales.
- Aspectos legales y regulatorios.
- Regulación nacional. Lopd y rº de la lopd.

Asignatura 8. **Análisis y auditoría forense.**

- Metodología del cibercrimen.
- Evaluación de la situación.
- Adquisición de evidencias.
- Análisis de evidencias.
- Informe de investigación.

Asignatura 9. **Auditoría del sistema de seguridad.**

- Desarrollo de un plan de políticas de seguridad informática.
- Auditoría del sistema de seguridad y análisis de riesgos.
- La norma iso/iec 27001 e implantacion de un modelo sgsi.
- Cumplimiento y gestión de la seguridad.
- Gestión del riesgo e indicadores de riesgo tecnológico (kri´s).

Asignatura 10. **Infraestructuras críticas.**

- Sistemas de prestación de servicios.
- Líneas de acción estratégicas.
- Los instrumentos de planificación.
- Implantación del sistema nacional de protección de infraestructuras críticas.

Asignatura 11**. Exposición de las pymes a los ciberataques.**

- La vulnerabilidad de las pymes.
- Protección contra los ciberataques en las pymes.
- Métodos de seguridad para combatir ciberataques.
- Mejora de la seguridad en las pymes.

Asignatura 12. **Trabajo fin de Máster.**