MÁSTER EN CIBERSEGURIDAD

Titulación Profesional - **Modalidad:** Online - **Titulación:** IOE - **Duración:** 600 horas

Presentación

Este **Máster Ciberseguridad** desarrollará tareas y funciones relacionadas con la **Seguridad de la Información**. Actualmente, cada vez hay más ciberdelincuencia y está afectando a miles de empresas. Esto supone que las empresas tengan **pérdidas de datos** a causa de la carencia de la protección adecuada. La implantación de **sistemas de seguridad** poco confiables o un uso inadecuado de las tecnologías.

Por tanto, ante este panorama mundial, se hace inminente la necesidad de formar personal capacitado en **máster ciberseguridad** o similares. El **Instituto Nacional de Ciberseguridad** deduce que a este ritmo, en los próximos cinco años se necesitarán casi medio millón de profesionales dedicados a la **ciberseguridad**. Este dato es de algunos países europeos, y no solamente referidos a la seguridad en las redes. Sino también a la **protección de sistemas** y **datos**.

En este sentido, abordaremos también en este **máster ciberseguridad** el **análisis de riesgos**. Cómo distinguir los riesgos y gestionarlos causando los mínimos daños a la seguridad. Estudiaremos para ello la tecnología **ALE** que se valora en la estimación de dos valores cuidadosamente escogidos.

El primero es el **ratio de ocurrencia anual** (ARO) y la **expectativa de pérdida simple** (SLE). En el **máster ciberseguridad** veremos que **ALE= SLE x ARO**. Considerando como **ataque** una situación en la cual la **vulnerabilidad** del sistema se pone en peligro por **una** amenaza. Y, asimismo, asumiendo que cada vulnerabilidad del sistema podría ser explotada por una amenaza.

Hazte especialista en Ciberseguridad online

Por tanto, este **máster ciberseguridad** te proporciona conocimientos sobre la **seguridad informática**. Esta se ha vuelto más compleja que nunca. Ya que los motivos y las capacidades de los actores amenazantes continúan evolucionando. Permitiendo a los malvados a menudo permanecer un paso por delante de los nuestros en el espacio de **seguridad de red**.

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**.

A medida que nos esforzamos por fortalecer a los empleados y estudiantes de **máster ciberseguridad** de todo el mundo con acceso omnipresente a datos importantes. Es cada vez más importante permanecer constantemente vigilantes sobre la **protección de datos y entidades** que los utilizan (individuos, empresas, gobiernos, etc.).

Los **controles de acceso** son primordiales para el **establecimiento de un sistema seguro**. Se basan en la identificación, autenticación, autorización y auditoría. El control de acceso es la administración, el manejo y la implementación de otorgar o restringir el acceso de sujetos a objetos.

La diferencia clave es que la **autenticación** significa que alguien tiene información. Mientras que la **identificación** significa que se demuestra que la información está en posesión del individuo correcto. Como se verá en el **máster ciberseguridad.**

Los profesionales del Máster Ciberseguridad

El **profesional de la seguridad de la información** debería ser consciente de las exigencias de control de acceso. Así como su medio de puesta en práctica para asegurar la confidencialidad, la integridad y la disponibilidad de un sistema. Estos profesionales de **máster ciberseguridad** deben entender el uso de **arquitecturas de control de acceso** distribuidas así como centralizadas.

El profesional de este **máster ciberseguridad** también debería entender las amenazas, vulnerabilidades y riesgos asociados con la **infraestructura del sistema de información** y las medidas preventivas y de investigación que están disponibles para contestar a ellos. Además, el **profesional de InfoSec** debería entender el uso de **herramientas de pruebas de penetración**.

El **control del acceso a sistemas de información y redes asociadas** es necesario para la preservación de su confidencialidad, integridad y disponibilidad. La **confidencialidad** asegura que la información no es revelada a personas o procesos no autorizados. Como aprenderán los participantes de este **máster ciberseguridad**, administramos la integridad por los tres objetivos siguientes:

- **Prevención** de la modificación de información por usuarios no autorizados.
- **Prevención** de la modificación no autorizada o involuntaria de información por usuarios autorizados.
- **Preservación** de la consistencia interna y externa.

En cuanto a las técnicas y herramientas de **protección de redes, sistemas y servicios**, en el **máster ciberseguridad** se muestra que los dispositivos que conforman una red, deben ser protegidos tanto físicamente como lógicamente.

La **política de seguridad** debe especificar todos los detalles sobre qué tipo de servicios, accesos y contraseñas. La política de seguridad debe ser conocida por todas las personas que usan la red y asegurarse de su aplicación.

Dicha política debe ser revisable, apoyada por auditorías internas y externas y se estudiarán en el **máster ciberseguridad**. La **encriptación como medida de seguridad** en todos los servicios y protocolos posibles, debe ser la opción a elegir siempre.

Protocolos y políticas de seguridad en el contexto digital

Las debilidades y la naturaleza del funcionamiento de los diversos **protocolos de comunicación**, son factores que pueden ser aprovechados por posibles atacantes. Por este motivo, en este **máster ciberseguridad** se conocerán cómo funcionan los protocolos. Y, por otra parte, qué tipo de medidas se deben aplicar para mitigar o minimizar estos ataques.

Tengamos siempre en cuenta que una red es un camino hacia otros dispositivos y sistemas que contienen información, y debemos procurar que las medidas a tomar en ese camino sean las más efectivas para **evitar que la información sea vulnerable**.

En este programa se aborda un tema fundamental como es la **recolección de información del objetivo**. El primer paso del **proceso de hacking** es recopilar información de un objetivo.

La recolección de información, también conocida como **footprinting**, es el proceso de reunir toda la información disponible sobre una organización. En la era de Internet, la información está disponible en pedazos y piezas de muchas fuentes diferentes.

Aparentemente, insignificantes trozos de información pueden ser esclarecedores cuando se reúnen y analizan en el **máster ciberseguridad**. **Footprinting** puede ser eficaz en la **identificación de objetivos de alto valor**, que es lo que los **hackers** estarán buscando para concentrar sus esfuerzos.

Existen varias metodologías de **análisis de riesgo** y varios métodos y técnicas que conoceremos en este **máster ciberseguridad**. Se verán también las estrategias preventivas y las diseñadas para contrarrestar una vez que sucede el ataque. Dígase, las **estrategias defensivas** y los métodos de diseño de cada una, en dependencia del tipo del incidencia.

Protección contra fraudes y hackers

Un hacker utiliza **técnicas de recopilación de información** para determinar los objetivos, donde reside la información más valiosa. No sólo la **recolección de información** ayuda a identificar dónde se encuentra la información. Sino que también ayuda a determinar la mejor manera de tener acceso a los objetivos, de acuerdo con este **máster ciberseguridad**.

Esta información se puede utilizar para identificar y eventualmente **hackear sistemas de destino**, como se verá en el **máster ciberseguridad**. Muchas personas saltan directos a la ejecución de **herramientas de hacking**, pero la **recopilación de información** es crítico para minimizar las posibilidades de detección y evaluar dónde gastar más tiempo y esfuerzo.

La **ingeniería social** también se puede utilizar para obtener más información acerca de una organización. Que en última instancia, puede conducir a un ataque. La ingeniería social como **herramienta de recopilación de información** es muy eficaz en la explotación del activo más vulnerable de una organización: la gente.

La interacción humana y la disposición a dar información hacen de la gente una excelente **fuente de información** que usaremos en este **máster ciberseguridad**. Las buenas **técnicas de ingeniería social** pueden acelerar el **proceso de piratería informática**. Y, en la mayoría de los casos producirá información mucho más fácilmente.

Aprovecha la oportunidad de especializarte con este **máster ciberseguridad**, en el cual se ven estos temas y muchos más

relacionados con la seguridad informática.

Objetivos

- Aprender los principios relacionados con la **seguridad informática**, tanto a nivel de sistemas como de protección de la información.
- Conocer y comprender los **distintos tipos de amenazas y vulnerabilidades** a los que se enfrenta un **sistema informático** y de información.
- Adoptar **Mecanismos de Protección** adecuados, auditar y detectar intrusos, administrar la **seguridad**.
- Adoptar, pulir y reutilizar un **modelo de experimentación** para ponerlo en funcionamiento sobre redes que están protegidas y son **inmunes a los ataques**.
- Conocer las **vulnerabilidades** y los **posibles ataques a las redes TCP/IP** y a los sistemas libres.
- Conocer las **diferentes técnicas de exploración de puertos**.
- Conocer los principales tipos de **técnicas para la protección de la información** en las redes y **sistemas telemáticos**.
- Proteger la **seguridad inalámbrica** para mantener confiable la **seguridad informática** de una empresa.
- Conocer los **ataques más utilizados** junto con la **implementación de herramientas de respuesta** ante estos.
- Implementación y robustecimiento de la **Seguridad Informática en la Empresa**.
- Normativa y Aplicación de las **Medidas de Seguridad** relacionadas con la **Protección de Datos**.
- **Peritaje**, Análisis y **Auditoría** de los **Sistemas de Seguridad** y de los **Riesgos**.

Plan de Estudios

Asignatura 1. **Seguridad informática: campos de acción.**

- Introducción y conceptos previos.
- Seguridad de los sistemas de información.
- Seguridad y protección de la información.
- Criptografía.

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 infraestructura para la construcción de confianza.
- Marco normativo y regulatorio de la seguridad y del comercio electrónico.

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

- Seguridad de comunicaciones y criptografía.
- Hacking, Malware y DDOS.
- Hardening y seguridad de la información.
- Auditoría y detección de intrusos.
- Delitos tipificados y fichas de delitos telemáticos.

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.
- Debilidad de los protocolos TCP/IP.

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

- Introducción y conceptos previos.
- Parámetros de estudio. Estructura y topología de redes inalámbricas.
- Equipos inalámbricos Wifi a utilizar y relación de rastreos sobre posibles víctimas.
- Fase de ataque a una red inalámbrica.

Asignatura 6. **Técnicas y herramientas de protección de redes.**

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

Asignatura 7. **Implementación de seguridad informática en la empresa.**

- Firewalls hardware y software.
- Robustecimiento de sistemas.
- Identificación de servicios.
- Protección de datos.

Asignatura 8. **Riesgos legales: protección datos. Medidas seguridad.**

- Introducción a la protección de datos. Conceptos y tipos de datos.
- Origen de la protección de datos. Normativa.
- Sujetos obligados a cumplir la normativa.
- Deber de secreto y medidas de seguridad.

Asignatura 9. **La ciberseguridad desde el ámbito judicial.**

- Derecho y código deontológico del perito informático.
- Evidencias digitales y judiciales.
- Organismos internacionales en ciberseguridad.
- Organismos nacionales relacionados con ciberseguridad.
- Aspectos legales y regulatorios en ciberseguridad.
- La regulación en protección de datos.

Asignatura 10. **Análisis y auditoría forense.**

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

Asignatura 11. **Auditoría del sistema de seguridad.**

- Que es una política de seguridad (PSI), desarrollo de un plan de políticas de seguridad informática.
- Auditoría del sistema de seguridad y análisis de riesgos.
- La norma ISO/IEC 27001 e implantación de un modelo SGSI.
- Cumplimiento y gestión de la seguridad
- Gestión del riesgo e indicadores de riesgo tecnológico (KRI´S).

Asignatura 12. **Trabajo final de máster.**