PLAN DE ESTUDIOS PROGRAMA MÁSTER EN CIBERSEGURIDAD =MCIBER=

ESCUELA: SCIENCE, TECHNOLOGY AND DATA CÓDIGO: 369 v01
AUTOR: SPAIN BUSINESS SCHOOL

Contenido

DESCRIPCIÓN DEL TÍTULO

- Denominación: MÁSTER EN CIBERSEGURIDAD
- Tipo: Máster
- Nivel: MESCES 3 (EQF 5)
- Título: Máster
- Cursos: 1
- Duración: 12 meses
- Periodo de impartición: Octubre
- Nº de créditos (horas): 72 ECTS (1.800 horas)
- Idioma en que se imparte: Español
- Metodología: Presencial, Semipresencial y Online
- Planificación de la enseñanza:
  - Ed. Octubre: De Octubre a Septiembre
- Plazas de nuevo ingreso:
  - Presencial: 15
  - Online: 15
- Distribución de créditos:
  - Obligatorios: 48 ects
  - Prácticas curriculares: 12 ects
  - Trabajo fin de máster: 12 ects
- Centro que imparte la titulación:
  - Spain Business School
    - Campus virtual: https://campus.spainbs.com
    - Campus urbano España:
      - C/ Antonio Toledano 7
      - 28028 Madrid
    - info@spainbs.com
    - +34 917191000
    - +34 610 351 371 (whatsapp)
  - Madrid Executive Business School
    - Campus virtual: https://mebs.es
    - internacional@mebs.es
    - +34 917191000
    - +34 665 179 431 (whatsapp)
- Web del programa. Se puede obtener más información de detalle en la página oficina del programa:
  - https://www.spainbs.com/master-en-ciberseguridad/

JUSTIFICACIÓN

Uno de los objetivos estratégicos de la Universidad es abrirse a todos los sectores de la sociedad con propuestas plurales e interdisciplinares. También lo es captar estudiantes que tienen interés en profundizar en materias específicas, como puede ser la Ciberseguridad, y que ya tengan una base científica y cultural importante en otras áreas del conocimiento.

La Ciberseguridad es uno de los campos de investigación más activos, tanto a nivel nacional como internacional, y uno en los que más innovaciones se producen. En el Máster participarán profesores con una amplia experiencia científica, lo que influye positivamente en capacitar al estudiante para el desempeño de actividades de investigación necesarias en las empresas, siempre relacionadas con el campo de la Ciberseguridad. Asimismo, el Máster procura, dentro de sus posibilidades, que el estudiante pueda configurarse un diseño curricular acorde a sus propios intereses formativos o de investigación.

Desde el punto de vista académico, el objetivo principal del Máster es llevar a cabo la formación

de estudiantes en el ámbito de la Ciberseguridad. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área. Para lograr este fin, se aplicará la metodología de educación propia de la universidad, con la inclusión de una gran variedad recursos multimedia educativos, tanto para los contenidos como las prácticas de evaluación. Se utilizarán los medios de los que dispone la institución para tal fin.

Desde el punto de vista profesional, los Ingenieros en Informática especializados en la Ciberseguridad juegan un papel fundamental en el desarrollo de la sociedad. Este Máster aporta a los profesionales de la Ingeniería Informática (o titulaciones afines) una formación de 60 créditos ECTS, dotándole con capacidades dentro del campo de la Ciberseguridad. En este sentido, el Trabajo Fin de Máster (TFM) potencia las habilidades personales, en diversos aspectos, que van desde la integración de tecnologías, a la adecuada presentación de resultados y conclusiones.

Demanda que cubrirá el máster

El mercado de la ciberseguridad va a ser un sector en auge. Según los datos de mercado mundial el tamaño para 2024 es de USD 203.78 mil millones de dólares estimando un volumen a 2029 de USD 350.23 mil millones de dólares.
[Source: https://www.mordorintelligence.com/es/industry-reports/cyber-security-market]

En nuestro país al creciente preocupación por la ciberseguridad, la aprobación del Esquema Nacional de Seguridad (de obligado cumplimiento para todos los organismos públicos), etc., auguran una demanda creciente de profesionales en ciberseguridad. Por si ello fuera poco, el incremento de los ciberataques se reflejó ya en la Estrategia Española de Seguridad, que considera a los mismos: “una amenaza actual, real y en crecimiento para los intereses nacionales”, haciendo hincapié en la necesidad de garantizar el uso seguro del ciberespacio y una preocupación creciente en la pyme, omo asi lo recoge el plan estratégico 2021-2024 de la Policía nacional.

En América Latina en el informe de 9 de octubre de 2023 presenta por EY (EY Global Cybersecurity Leadership Insights Study) exponía como resumen

- 62 % de las empresas latinoamericanas han sufrido alguna filtración de datos durante el último año
- 52 % de las compañías latinoamericanas han experimentado entre uno y nueve casos de filtraciones.
- 50 % de las empresas de Latinoamérica reportaron una inversión total en ciberseguridad de entre 10 y 49 millones de dólares

Es por ello que la demanda en los próximos años creciente y la oferta económica de los profesionales formatos en el área es igualmente creciente, como lo expone el informe de remuneraciones 2024 realizado por Michael Page.

SECURITY ENGINEER	1-3 años	4-7 años	≥8 años	Bonus
Madrid	35-45K	45-60K	60-70K	N.A
Barcelona	35-45K	45-55K	55-65K	N.A
País Vasco	30-40K	40-50K	50-65K	N.A
Zaragoza	30-40K	40-50K	50-65K	N.A
Galicia	30-38K	38-45K	45-65K	N.A
Valencia	30-35K	35-45K	45-55K	N.A
Málaga	33-38K	38-48K	48-60K	N.A
Sevilla	30-35K	35-45K	45-55K	N.A

DEVSECOPS	1-3 años	4-7 años	≥8 años	Bonus
Madrid	40-60K	60-80K	N.A	10-15%
Barcelona	40-55K	55-75K	N.A	10-15%
País Vasco	40-50K	50-70K	N.A	10-15%
Zaragoza	40-50K	50-70K	N.A	10-15%
Galicia	35-45K	45-60K	N.A	10-15%
Valencia	35-45K	45-65K	N.A	10-15%
Málaga	40-50K	50-70K	N.A	10-15%
Sevilla	35-45K	45-65K	N.A	10-15%

CISO	1-3 años	4-7 años	≥8 años	Bonus
Madrid	50-70K	70-100K	100-150K	15%
Barcelona	50-70K	70-95K	95-140K	15%
País Vasco	45-60K	60-80K	80-100K	15%
Zaragoza	45-60K	60-80K	80-100K	15%
Galicia	45-60K	50-70K	70-90K	15%
Valencia	45-60K	60-80K	80-100K	15%
Málaga	45-60K	60-80K	80-100K	15%
Sevilla	45-60K	60-80K	80-100K	15%

IT AUDIT	1-3 años	4-7 años	≥8 años	Bonus
Madrid	25-35K	35-55K	55-70K	N.A
Barcelona	25-35K	35-50K	50-65K	N.A
País Vasco	30-35K	35-45K	45-55K	N.A
Zaragoza	30-35K	35-45K	45-55K	N.A
Galicia	30-35K	35-45K	45-55K	N.A
Valencia	30-35K	35-45K	45-55K	N.A
Málaga	30-35K	35-45K	45-55K	N.A
Sevilla	30-35K	35-45K	45-55K	N.A

GRC CONSULTANT	1-3 años	4-7 años	≥8 años	Bonus
Madrid	30-35K	35-55K	55-70K	N.A
Barcelona	30-35K	35-55K	55-70K	N.A
País Vasco	30-35K	35-50K	50-65K	N.A
Zaragoza	30-35K	35-50K	50-60K	N.A
Galicia	30-35K	35-50K	50-60K	N.A
Valencia	30-35K	35-50K	50-65K	N.A
Málaga	30-35K	35-50K	50-60K	N.A
Sevilla	30-35K	35-50K	50-60K	N.A

ETHICAL HACKER	1-3 años	4-7 años	≥8 años	Bonus
Madrid	25-35K	35-55K	55-70K	N.A
Barcelona	25-35K	35-50K	50-65K	N.A
País Vasco	30-35K	35-45K	45-55K	N.A
Zaragoza	30-35K	35-45K	45-55K	N.A
Galicia	30-35K	35-45K	45-55K	N.A
Valencia	30-35K	35-45K	45-55K	N.A
Málaga	30-35K	35-45K	45-55K	N.A
Sevilla	30-35K	35-45K	45-55K	N.A

COMPLIANCE AND DATA PROTECTION	1-3 años	4-7 años	≥8 años	Bonus
Madrid	50-60K	60-70K	>75K	10-15%
Barcelona	50-60K	60-70K	>75K	10-15%
País Vasco	50-55K	55-65K	>70K	10-15%
Zaragoza	50-55K	55-60K	>60K	10-15%
Galicia	50-55K	55-60K	>65K	10-15%
Valencia	50-55K	55-65K	>65K	10-15%
Málaga	50-55K	55-65K	>65K	10-15%
Sevilla	50-55K	55-65K	>65K	10-15%

PENTESTER	1-3 años	4-7 años	≥8 años	Bonus
Madrid	30-40K	40-55K	55-70K	N.A
Barcelona	30-40K	40-55K	55-70K	N.A
País Vasco	25-35K	35-48K	48-68K	N.A
Zaragoza	25-35K	35-50K	50-70K	N.A
Galicia	25-35K	35-45K	45-65K	N.A
Valencia	25-35K	35-48K	48-68K	N.A
Málaga	25-35K	35-45K	45-65K	N.A
Sevilla	25-35K	35-45K	45-65K	N.A

Referentes nacionales

En las Universidades españolas podemos encontrar titulaciones cercanas al propuesto aquí, entre los que destacamos los que se han examinado con más detalle, como son el "Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones" ofertado en la Universidad Europea de Madrid, el "Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones por la Universidad" ofertado en Universidad Alfonso X El Sabio, el "Máster Universitario en Seguridad Informática (Ciberseguridad)" ofertado en la Universidad de Cádiz, o el "Máster en Ciberseguridad" ofertado en la Universidad Carlos III de Madrid, o el "Máster Universitario en Investigación en Ciberseguridad" ofertado en la Universidad de León.

Además de los mencionados anteriormente, el resto de Másteres están registrados en el Registro de Universidades, Centros y Títulos (RUCT), y ya publicados en el B.O.E., pudiéndose encontrar en el siguiente buscador:
https://www.educacion.gob.es/ruct/consultaestudios.action?actual=estudios

El listado completo de Másteres relacionados con la Ciberseguridad y Seguridad Informática, con mayor o menor detalle, adaptados al Espacio Europeo de Educación Superior (EEES) y regulados por el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, y por el Real Decreto 861/2010, de 2 de julio por el que se modifica el Real Decreto 1393/2007 de 29 de octubre, son los siguientes:

- Máster Universitario en Ciberseguridad por la Universidad Carlos III de Madrid.
- Máster Universitario en Ciberseguridad por la Universidad Internacional Isabel I de Castilla.
- Máster Universitario en Ciberseguridad por la Universidad Politécnica de Madrid.
- Máster Universitario en Ingeniería de la Seguridad Informática e Inteligencia Artificial por la Universidad Rovira i Virgili.
- Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones por la Universidad Alfonso X El Sabio.
- Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes por la Universidad Rovira i Virgili.
- Máster Universitario en Investigación en Ciberseguridad por la Universidad de León.
- Máster Universitario en Seguridad de la Información por la Universidad de Deusto.
- Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la Universidad Autónoma de Barcelona; la Universidad Rovira i Virgili y la Universitat Oberta de Catalunya.
- Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones por la Universidad Europea de Madrid.
- Máster Universitario en Seguridad Informática (Ciberseguridad) por la Universidad de Cádiz.
- Máster Universitario en Seguridad Informática por la Universidad de Jaén.
- Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja.
- Máster Universitario en Seguridad Informática y Sistemas Inteligentes por la Universidad Rovira i Virgili.
- Máster Universitario en Tecnologías de Protección para Sistemas de Seguridad y Defensa por la Universidad Rey Juan Carlos.

Por otra parte, en España el Instituto Nacional de Ciberseguridad (INCIBE) (https://www.incibe.es/), es el antiguo Instituto Nacional de Tecnologías de las Comunicación, que contribuye a afianzar la confianza digital, dentro de la temática de la Ciberseguridad, tanto a nivel nacional como internacional. Este Instituto organiza eventos, jornadas, cursos, recursos, etc., muy relevantes de Ciberseguridad, entre otras actividades, y acercando a las empresas y al ciudadano de a pie la temática en cuestión. También dispone de un catálogo de Másteres e Instituciones que ofrecen formación en Ciberseguridad.

El Máster que se propone aquí incluye, además de aspectos tecnológicos, temas relacionados con la industria y con formación legislativa. A diferencia de otros títulos de temáticas similares impartidos en Universidades españolas, este Máster se imparte con la metodología enriquecida de la Universidad, por lo que es accesible para una mayor parte de los profesionales de la Informática, que en su mayoría están trabajando y desean compatibilizarlo con su estudio.

Referentes internacionales

Existe un también un interés creciente internacional en la temática de Ciberseguridad. Algunos ejemplos son las ofertas de Másteres de Universidades extranjeras. Por ejemplo, en USA se dispone de un programa estratégico destinado a aumentar el personal cualificado en Ciberseguridad, tanto a nivel institucional como formativo para ejercer de forma profesional. La NSA (National Security Agency) en USA está relacionada y ofrece soporte a varios Centros de excelencia que imparten docencia reglada dentro de la temática de la Ciberseguridad, como son las instituciones de Dakota State University, Naval Postgraduate School, Northeastern University, Tulsa University, etc.

En el ámbito europeo, la agencia europea por la ciberseguridad ENISA [https://www.enisa.europa.eu/] no ha hecho una apuesta tan decidida por la educación

reglada en ciberseguridad como la que encontramos en EEUU, que ha creado un programa estratégico destinado a aumentar el personal cualificado en ciberseguridad en las empresas y en la administración.

Objetivos

El objetivo principal del Máster es llevar a cabo la formación de estudiantes en el ámbito de la Ciberseguridad, tanto para fines de investigación como fines formativos para ejercer de forma profesional. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área.

El objetivo principal del plan de estudios puede desglosarse en diferentes objetivos específicos:

- Utilizar mecanismos criptográficos avanzados para garantizarlos requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.
- Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.
- Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.
- Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.
- Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
- Conocerlas tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.
- Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
- Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.
- Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.
- Conseguirla percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

Perfil egresado

Por una parte, la persona especialista en Ciberseguridad debe ser un/a profesional con capacidad para: utilizar e impulsar técnicas actualizadas que invoquen una cultura general de seguridad informática, distinguir entre las ventajas y desventajas relacionadas con el diseño y la administración de políticas de seguridad sobre los recursos informáticos de una organización, diseñar estrategias para maximizar la ciberseguridad de forma que se convierta en un valor añadido en el negocio, y aplicar estándares nacionales e internacionales y aspectos éticos-legales de la seguridad informática. Los principales perfiles son:

- Ingenieros de seguridad
- Analistas de cibersegrudad
- Hacker ético
- Perito forense
- Consultor en ciberseguridad
- Consultor de security complience

Estos perfiles se orientan a las organizaciones que necesitan protegerse de las ciberamenazas, requieren de personal que sepa identificar ataques y potenciales debilidades en sus sistemas y redes, y sea capaz de proponer el uso y despliegue de medidas y contramedidas para asegurarlos. Se trata de un perfil más ligado a los responsables de ciberseguridad, a través de pruebas y auditorías, le ayudan a mantener los riesgos de seguridad controlados y a actuar frente a ataques. Este segundo perfil encuentra cabida en un número creciente de empresas,

cada vez más dependientes de sus sistemas de información e Internet y de forma específica en sectores críticos, empresariales (como la banca, la energía o el transporte) o públicos (organismos como las Fuerzas Armadas o las Fuerzas y Cuerpos de la Seguridad del Estado)

COMPETENCIAS

Básicas

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Generales

- Analizar métodos y técnicas de ciberataques.
- Diseñar, poner en marcha y mantener un sistema de ciberseguridad.
- Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.
- Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

Específicas

- Utilizar mecanismos criptográficos avanzados para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.
- Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.
- Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.
- Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.
- Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
- Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.
- Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
- Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.
- Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.

- Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

ACCESO Y ADMISIÓN DE ESTUDIANTES

Sistema de información previa

Perfil de ingreso

El título se dirige fundamentalmente a profesionales, que serán titulados universitarios de distinta formación académica previa, fundamentalmente procedentes de Informática, ingenierías de seguridad, telecomunicaciones, así como perfiles cercanos a las titulaciones anteriores. Al estar pensado para un público amplio no se requieren, por tanto, conocimientos avanzados de programación para realizarlo. No obstante, es necesario demostrar capacidad de aprendizaje e inquietud intelectual suficiente para trabajar en entornos informáticos, utilización de algoritmos y análisis básico de datos.

También se dirige a profesionales en activo que desempeñen puestos que requieran de conocimientos y aptitudes de ciberseguridad en cualquiera de sus ámbitos.

Profesionales en búsqueda activa de empleo que quieran adquirir competencias en el ámbito de la ciberseguridad.

Sistemas de información

La Universidad y escuelas asociadas disponen de distintos canales de información (difusión), online, para hacer visible el título de Máster.

- Página web https://sbs.edu.es
- Página web https://mebs.es
- Página propia del máster
- Canales de noticias y comunicaciones sociales de la universidad y Escuelas

Para el servicio de admisión la Universidad y escuelas asociadas centralizan en este servicio la promoción de todos los estudios de grado y posgrado del centro que incluye:

- Campañas de marketing digital (landing pages; Meta y otras redes sociales).
- Asistencia a ferias de posgrado (FIEP; ESPCIALÍZA-T y QS) en ciudades españolas (Bilbao, Zaragoza, Sevilla; Madrid, Valladolid) y capitales de países latinoamericanos (Buenos Aires, Lima, Quito, Panamá, Bogotá, San José y México). Cualquier solicitud de información que se recoge en estas iniciativas de promoción queda registrada en una plataforma de gestión (Salesforce) desde donde cada título informa a sus alumnos potenciales.

Este servicio celebra reuniones de coordinación con todos los responsables de admisión de los distintos títulos y sesiones de formación (p.e.: Atención al cliente + Escritura persuasiva + Llamadas en frío; marketing digital).
Cada septiembre se celebra la Convención anual del servicio a la que asisten los responsables de admisión de centros y los delegados de la UN en España y resto de países. Se ponen en común los resultados del curso vencido; se presentan los objetivos del siguiente; las nuevas ofertas formativas, novedades en el proceso de admisión.

Los alumnos también pueden pedir información del título desde la propia web del Máster o de la web general de másteres de la Universidad)

El servicio de admisión prepara folletos informativos (en versión digital e impresa) de cada uno de sus títulos que se facilitan desde el centro a todas las personas interesadas. Se suele ofrecer

esta documentación cuando en el Instituto Cultura y Sociedad se celebran actividades (congresos, seminarios, etc) que atraen a público potencialmente interesado.

Acceso

El acceso a las titulaciones de máster queda recogidas en el procedimiento de calidad PO-01 y quedan definidas atendiendo al Real Decreto 822/2021, de 28 de septiembre, en su artículo 18 así como la guía de acreditación CUALIFICAM en la subdimensión 1.1 y unidad de análisis 1.1.1, que podemos resumir en:

- Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior del Espacio Europeo de Educación Superior.
- Título de sistemas educativos ajenos al EEES que faculte en el país de expedición para el acceso a enseñanza de máster, homologado o declarado equivalente a titulación y nivel académico de Grado o Licenciado por el Ministerio de Educación y Formación Profesional. En caso de carecer de la mencionada homologación o equivalencia será necesario tener autorización o permiso de acceso otorgado por esta Universidad. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión del interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.
- También se puede cumplir el perfil de ingreso por experiencia profesional acreditada (mínimo 3 años de experiencia en puesto con competencias mínimas de grado o equivalente)

Admisión

En el caso de que el número de candidatos que cumplan los requisitos mencionados en punto anterior supere el número de plazas ofertadas, para la selección de los alumnos se tendrá en cuenta el CV del candidato, en el que se valorará la formación recibida hasta el momento en

1. Informática.
2. Programación, especialmente en Python o entornos similares.
3. Experiencia profesional del candidato en estos temas.

Además de presentar su CV y los documentos que considere oportunos para justificar los requisitos mencionados, la junta directiva del máster podrá solicitar al alumno otros documentos adicionales o bien la realización de una entrevista de admisión, presencial o por vía telemática, que servirá para que el candidato acredite los requisitos exigidos por el máster, tanto sus conocimientos previos como su trayectoria profesional y su motivación para cursar el máster.

El proceso de selección se realizará de forma individual, para cada candidato. La persona encargada de la entrevista del candidato será miembro de la junta directiva del máster o profesor del título. La información que se extraiga de estas conversaciones se pondrá en común y será accesible para el resto de miembros de la junta directiva del máster.
Para realizar esta selección entre los que cumplan los requisitos mencionados en punto anterior, se tendrá en cuenta:

1. Nota media del expediente del grado o titulación que le da acceso a este máster: 40%
2. Adecuación de la formación recibida a este máster: 20%
3. Experiencia profesional relativa al máster: 20%
4. Motivación e interés (10%)
5. Otros (10%)

La matrícula se formalizará online en los plazos establecidos por la universidad.

Apoyo a estudiantes

El alumno contará con el apoyo del orientador académico durante todo el proceso de información, admisión y matrícula. Una vez que el alumno se haya matriculado se le asignará un tutor académico, que puede pertenecer al claustro de profesores del máster o a la junta directiva. Habitualmente, el tutor se encargará también de dirigir el Trabajo de Fin de Máster (TFM) y podrá ser personal de una empresa colaboradora.

La asignación de los tutores es responsabilidad de la junta directiva que tendrá en cuenta los intereses del alumno según lo recogido en las entrevistas de admisión. En cualquier caso, el alumno podrá solicitar un cambio o incluso proponer a un tutor. La junta directiva del máster deberá estar informada y aprobar la asignación, en estos casos. Habitualmente, antes del comienzo de las clases el alumno conocerá ya el nombre de su tutor y la temática de su TFM, si bien en algunos casos, dependiendo de cuándo se haya formalizado la matrícula del alumno, puede confirmarse una vez arrancado el curso.

El asesoramiento académico personalizado pretende que el alumno disponga de apoyo durante el desarrollo del máster con el fin de mejorar su rendimiento académico, facilitar su integración en la vida universitaria, y colaborar en su formación cultural, humana y profesional. Además, pretende:

- facilitar una mejor integración de los estudiantes de nuevo ingreso en el máster;
- conseguir un alto grado de satisfacción con la titulación.

Esta atención personalizada al alumno comprende los siguientes aspectos:

- asesoramiento sobre la metodología de trabajo intelectual;
- asesoramiento y guía para la realización del Trabajo de Fin de Máster;

El alumno contará además con el apoyo de la coordinadora administrativa del máster que se encargará de:

- ayudar y orientar a resolver procesos administrativos;
- informar sobre las posibilidades formativas de la Universidad (cursos, actividades sociales, culturales y deportivas, etc.);

Los potenciales alumnos internacionales contarán con el apoyo, además de la Oficina de Atención Internacional, que ofrece:

- orientación sobre el funcionamiento de los servicios de la Universidad;
- actividades extraacadémicas para estudiantes internacionales;
- información sobre la tramitación de documentos oficiales (visado, homologación de títulos, seguro médico, etc.);
- apoyo a problemas que puedan surgir durante la estancia en Madrid;
- jornadas generales de bienvenida a los estudiantes extranjeros, en las que se les muestran los distintos centros y servicios de la universidad, y en las que se les informa de todo aquello que pueda ser relevante para su estancia (horarios, material, etc.).

Sistema de transferencia y reconocimiento de créditos

El sistema de reconocimiento de créditos queda recogido en el procedimiento de calidad PO-03.

- Reconocimiento de créditos cursados en programas de formación de micro credenciales de al menos 20 ECTS cursadas en SBS.
- Reconocimiento de créditos cursados en otros Programas Máster Profesional.
  El máster deberá ser de la propia escuela o de otra escuela perteneciente a AEEN y este certificado pro el sello CUALIFICAM de Máster Profesional.
- Reconocimiento de créditos cursados en otros Programas Máster Universitarios, oficiales o propios, y de Escuelas de Negocios y Centros de Posgrado acreditados.

En los programas que cumplen el caso anterior, el reconocimiento máximo de créditos no superará el 30% del programa.

- Reconocimiento de créditos de Prácticas Profesionales por experiencia profesional. Será válido tanto por haber cursado los créditos de prácticas con otras universidades o entidades de formación o en su defecto disponer de experiencia profesional según se recoge en la guía docente de prácticas. El máximo de los créditos a reconocer son 12 ECTS según se define en la asignatura.
- En ningún caso se realiza reconocimiento de créditos del Trabajo Fin de Máster.

El sistema de transferencia de créditos queda definido por:

- También se incluirán en su expediente académico la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, que no hayan conducido a la obtención de un título oficial.
- Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursados en cualquier universidad, los transferidos, los reconocidos y los superados para la obtención del correspondiente título, serán incluidos en su expediente académico y reflejados en el Suplemento Europeo al Título.

El procedimiento para el reconocimiento de créditos es el siguiente:
Las solicitudes de reconocimiento y convalidación de créditos superados en otras enseñanzas se dirigirán a Jefatura de Estudios en el que el estudiante haya sido admitido en los plazos y de acuerdo con los procedimientos fijados por la Escuela. La solicitud deberá acompañarse de la siguiente documentación:

- Certificación académica sellada de la Institución de educación en la que consten las asignaturas o materias superadas con indicación de su carácter y las calificaciones obtenidas. En el caso de tratarse de materias de formación básica deberá acreditarse la rama de conocimiento a la que están adscritas.
- Programas oficiales de las materias o asignaturas superadas (Guía docente de detalle sellada por la institución).
- Cuando el estudiante solicite la convalidación de asignaturas o materias cursadas en universidades extranjeras, la certificación académica de la Universidad/Escuela deberá presentarse debidamente legalizada de conformidad con la normativa que resulte de aplicación. Jefatura de Estudios de la titulación podrá admitir los documentos en inglés. Los documentos en otros idiomas deberán presentarse en todo caso con traducción oficial al castellano.
- Los estudiantes de SBS que cambien de titulación no deberán presentar ningún documento por disponer de ellos en la administración universitaria, que procederá a su comprobación de oficio.

Para el caso de prácticas profesionales la documentación será:

- Experiencia laboral
    - Fotocopia de contrato o Vida laboral (o equivalente en el país de origen)
    - Certificado de empresa donde aparezca las funciones desempeñadas
- Prácticas anteriormente realizadas
    - Fotocopia de anexo de prácticas
    - Informe de tutor y/o Memoria académica

Para la resolución de las solicitudes de reconocimiento y convalidación.

- Jefatura de Estudios en el que el estudiante inicie sus estudios, o en quien delegue, resolverá el reconocimiento o convalidación de los créditos superados en otra titulación y/o Universidad de acuerdo con los procedimientos establecidos por la Escuela.
- En las resoluciones de reconocimiento y convalidación deberá valorarse el expediente universitario del alumno en su conjunto, debiéndose tener en cuenta la adecuación entre las competencias y conocimientos asociados a las materias cursadas por el estudiante y los previstos en el plan de estudios, no siendo necesaria la equivalencia total de contenidos ni de carga lectiva por asignatura, materia o módulo.
- El Centro podrá constituir comisiones de apoyo a los responsables académicos de las distintas titulaciones para valorar la adecuación de los conocimientos y competencias

asociados a las materias superadas por el solicitante con las materias del plan de estudios. Formarán parte de estas comisiones profesores de los Departamentos que impartan docencia en los estudios correspondientes. El Centro podrá atribuir esta función a las Comisiones Académicas de Titulación.

Complementos formativos

No se han detallado

PLANIFICACION DE LAS ENSEÑANZAS

El programa de estudios se estructura alrededor de tres grandes bloques:

- Técnicas de Ciberataque: Las asignaturas comprendidas en esta área cubren en detalle las amenazas a las que los sistemas de ciberdefensa deben hacer frente, incluyendo las técnicas actuales de penetración de redes y explotación maliciosa de sistemas el análisis e ingeniería de malware, las técnicas que permiten la fuga de información y las perspectivas actuales en ciberdelitos, ciberterrorismo y ciberguerra.
- Técnicas de Ciberdefensa: Esta área agrupa los conocimientos y tecnologías relacionados con los sistemas de ciberdefensa, la criptografía aplicada y su uso en protocolos y esquemas que garanticen la seguridad de las comunicaciones. Las distintas materias abarcan la protección de datos y comunicaciones, las técnicas de identificación y autenticación de usuarios y sistemas, los sistemas de ciberdefensa, el análisis forense de equipos informáticos, la seguridad en sistemas y comunicaciones móviles, y la ingeniería y desarrollo de sistemas seguros.
- Informática forense: Esta área agrupa los conocimientos centrados en la realización de informes periciales forense de manera profesional tanto para entorno Windows como Linux y dispositivos Android o IOS. Aprenderá a realizar informes estructurados siguiendo las normativas para la no alteración de evidencias.
- Gestión de la Ciberseguridad: Las asignaturas en esta área comprenden los aspectos de gestión y administración de la Ciberseguridad, incluyendo el ciclo de vida y los procedimientos operativos de los centros de ciberdefensa, la creación de planes de seguridad de continuidad y de formación y concienciación del personal, las metodologías de análisis y gestión de riesgos, los procesos de normalización y certificación de productos y sistemas, y el marco legal y regulador de la ciberseguridad.

CARÁCTER ECTS	N.º ECTS
Obligatorios	48
Prácticas	12
TFM	12
TOTAL	**72**

Actividades formativas

- Clases presenciales teóricas
- Prácticas con ordenador
- Seminarios
- Trabajos dirigidos
- Tutorías personalizadas
- Estudio y trabajo personal
- Pruebas presenciales de evaluación
- Elaboración y Defensa del Trabajo Fin de Máster

Sistemas de evaluación

- Intervención en clases, seminarios y clases prácticas
- Resolución de ejercicios con el ordenador
- Evaluaciones parciales
- Examen
- Trabajos individuales y/o en equipo
- Valoración del TFM

Metodologías docentes

A continuación, detallamos las principales características de las metodologías de enseñanza.

La Universidad trabaja con 3 metodologías de enseñanza de clases en directo:

1) Presencial.
2) Semipresencial.
3) Online.

Además, cuenta con una cuarta metodología virtual o a distancia con clases asincronías y recursos de enseñanza (grabados), en la cual el alumno no asiste en directo a clases.

La definición de la presencialidad viene definida según se recoge en la guía de calidad universitaria descrita por ANECA (acreditadora oficial de la calidad universitaria en España) donde:

Presencial:

La metodología presencial se define como aquella que tiene presencia en directo del profesor docente, ya sea en aula o de manera virtual síncrona y siempre que supere un 34% de las horas correspondientes a los ECTS (1 ECTS son 25 horas de trabajo total).
En cada guía docente de la asignatura tendrá una definición concreta de la distribución de actividades presenciales y no presenciales, así como las horas de actividad formativa presencial por actividad concreta.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza presencial, aquella en la que la mayor parte de las actividades formativas se desarrollan preferentemente de forma presencial, es decir, interactuando el profesorado y el alumnado en el mismo espacio físico, sea éste el aula, laboratorios, espacios académicos especializados, etc. (presencia física y síncrona)." Y lo establecido en el RD 822/2021 en su artículo 14.7

Según definición de RD 1125/2003. Y define los siguientes tipos de actividades:

- Actividades presenciales. Son aquellas en las que el profesor o profesora está presente:
  - Actividades presenciales convencionales. Se refieren a las clases de teoría y/o problemas y a las prácticas de laboratorio o aula de informática. Suelen ser actividades sistemáticas y estar recogidas dentro del horario académico del centro.
  - Actividades presenciales no convencionales. El profesorado está presente, pero no están recogidas dentro del horario del centro: tutorías, pruebas de evaluación, seminarios, visitas, exposición de trabajos, etc.
- Actividades no presenciales. El profesor o profesora no está presente en ningún momento: estudio personal, preparación de trabajos e informes individuales o en grupo, etc.

Semipresencial:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza semipresencial, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como semipresencial o híbrida si al menos el 40% -80% de los créditos que lo configuran se imparten en dicha modalidad."

Virtual:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza virtual, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como virtual si al menos el 80% de los créditos que lo configuran se imparten en dicha modalidad."

Cabe destacar que la metodología de la Universidad es enriquecida dado que complementa los directos con recursos adicionales en el campus (cursos de la materia post-producidos, notas técnicas, casos prácticos, referencias adicionales, exámenes, etc.)

Sobre la definición anterior de las metodologías SBS, ¿cómo se trabajan a nivel educativo?

1) Presencial

El alumno asiste presencialmente en aula entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia en aula semanales. El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.
Cada asignatura se configura en un número de ECTS. Cada ECTS son 25 horas totales y siguiendo la norma ANECA de estudios superiores, al menos el 34% de estas horas deben ser en acciones directas con el profesor (8,5). SBS, siguiendo la norma, realiza la siguiente distribución:

- Al menos 5 horas de clase presencial en aula
- 1-1,5 horas de evaluación (examen)
- 1-1,5 horas de tutoría
- 1-1,5 horas de trabajo práctico guiado por el profesor

Cada asignatura cuenta con una guía docente donde queda definido particularmente el funcionamiento en el apartado de Actividades formativas.

2) Semipresencial

El alumno asiste en directo entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia semanales (bien en presencial física en el aula u online directo de la emisión). El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Existe una variación a la metodología en la edición de febrero/marzo. El alumno asiste regularmente en aula los viernes sin limitación a que pudieran establecerse otros días presenciales en aula. Además, tiene entre semana días de clase online directo en una periodicidad entre 1 y 4 que complementa la acción presencial según recoge la guía. En esta variación el número de horas del alumno en directo (presencial aula o virtual) será de 6-14 h semanales.

3) Online

El alumno asiste de manera virtual a las clases, sin limitación a que pueda ser invitado por la escuela a algún periodo presencial en aula o bootcamp intensivo. Atendiendo a la definición del punto anterior, el alumno tendrá clases en directo

de entre 8-20 horas semanales para la edición de septiembre/octubre y 6-14 horas para la edición de febrero/marzo.

Igualmente, el alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Es importante destacar que, con independencia de la metodología, los exámenes se realizan en directo, bien en aula o virtual con identificación y cámara para garantizar la veracidad del alumno. La parte práctica docente utiliza además de metodologías más tradicionales otras metodologías innovadoras basadas en:

- Aprendizaje basado en proyecto
- Estudios, análisis y exposiciones de métodos del caso
- Aprendizaje cooperativo y colaborativo
- Trabajo por ámbitos
- Gamificación educativa

Estructura de las enseñanzas / Programa

MCIBER.- MÁSTER EN CIBERSEGURIDAD		
	72	
	ECTS	
LA CIBERSEGURIDAD	1	Guía docente
Fundamentos de ciberseguridad		
Gobierno de datos e información		
BÁSICOS TECNOLOGÍA	6	
La base web HTML/CSS/JS		Guía docente
La base de Linux		
Programación en Python + Sql		Guía docente Guía docente
HACKING ÉTICO	15	Guía docente
Recolección y escaneo de datos		
Análisis		
Exploración		
Lenguajes de Hacking		
Auditorías Web		
Infraestructuras de hacking		
Auditorias de Passwords y Wifi		
Malware		
Python para la ciberseguridad (pentestting)		
INFORMÁTICA FORENSE	10	Guía docente
Informática forense. Principios y entorno de trabajo		
Recolección de evidencias		
Captura y análisis de evidencias en Windows		
Captura y análisis de evidencias en Linux		
Análisis de correos electrónicos		
El informe pericial		
Captura y análisis de evidencias en Móviles		
Ciberseguridad de defensa		
DIRECCIÓN DE LA CIBERSEGURIDAD	10	Guía docente
Gestión del riesgo operacional		

		Leyes y regulaciones entorno a los datos		
		Ofrecimiento de servicios en la nube		
		Gestión de defensa y respuesta a incidentes		
		Arquitectura de seguridad		
		MLSec: Machine Learning para la Ciberseguridad		
		Seguridad en las operaciones TIC		
		Evaluación de postura de seguridad		
		Laboratorio práctico ISO 27001		
	HABILIDADES Y COMPETENCIAS			
		Gestión emprendedora	2	Guía docente
		Habilidades profesionales y directivas	4	Guía docente
	PRÁCTICAS CURRICULARES		12	Guía docente
	TRABAJO FINAL		12	Guía docente

Calendario ejecución

El plan de ejecución general Europeo se basa en tres periodos según se contempla en la primera columna del pensum anterior:

- Periodo 1: Primer cuatrimestre
- Periodo 2: Segundo cuatrimestre
- Periodo 3: Tercer cuatrimestre

Dependiendo de la metodología variará la carga presencial en aula pero todas las metodologías tendrán una carga mixta, blended, en campus virtual para maximizar el aprendizaje y complementar la propia preparación del presente programa con competencias, negocios digitales y emprendimiento.

Está a disposición del alumno el calendario de ejecución de detalle.

Planificación y gestión de la movilidad de estudiantes propios y de acogida

No se prevé que los estudiantes del máster sean de acogida, ni que los propios lleven a cabo acciones de movilidad.

Descripciones detalladas de los módulos o materias

Ver guías docentes completas para mayor detalle de cada módulo/asignatura.

Procedimientos de coordinación docente horizontal y vertical del plan de estudios

La Junta de Dirección del máster llevará a cabo dos reuniones anuales con el personal académico implicado en el (profesores del claustro).

- Primera reunión (septiembre). Reunión de puesta en marcha del curso académico, en la que se marcarán las pautas generales de funcionamiento del máster (clases presenciales, plazos, sistemas de atención a los alumnos).
- Segunda reunión (julio). Reunión de balance final del curso académico, en la que se examinarán también los resultados de encuestas realizadas a los alumnos. En ella se

proporcionarán datos actualizados sobre la marcha del proceso de admisión de alumnos para el siguiente curso académico.

Las fechas y número de reuniones son orientativas y podrían sufrir cambios adaptados a la marcha del máster. Estas reuniones garantizarán que en todo momento la Junta de Dirección del máster pueda coordinar correctamente y ajustar en lo necesario el funcionamiento docente de la titulación

PERSONAL ACADÉMICO

CATEGORIA		Contratado	JUNIOR MASTER	SENIOR MASTER	DOCTORES
Dirección de programa o cátedra	2	0%		100%	
Otro personal docente	20	30%		85%	15%
Otros recursos de apoyo	3	100%		100%	

Director de programa

- **Francisco Sanz**
  - francisco.sanz@sbs.edu.es
  - https://www.linkedin.com/in/francisco-sanz-044514a4/
  - Nivel docente: Máster
  - Categoría docente: Senior

Subdirector de programa

- **Christian Gutiérrez González**
  - christian.gutierrez@sbs.edu.es
  - https://www.linkedin.com/in/christian-guti%C3%A9rrez-gonz%C3%A1lez-78a1221a9/
  - Nivel docente: Máster
  - Categoría docente: Senior

Otro personal docente

AREA	DOCENTE	CATEGORIA	
Programación	Docentes 3 Tutores 1	Senior Máster	
Base de datos	Docentes 2 Tutores 2	Senior Máster	
Ciberseguridad	Docentes 6 Tutores 2	Senior Máster	
Habilidades	Núria Oriol	Senior Máster	
Emprendimiento	M. Ángel Blanco Cedrún	Senior Máster	

Otros recursos humanos disponibles

La universidad cuenta con los recursos humanos de carácter administrativo

necesarios para llevar a cabo el plan de estudios propuesto.

De forma específica, el programa cuenta con los siguientes perfiles:

- **Tutores académicos**, definido como el personal que realizan funciones docentes directamente relacionadas con la materia. Por lo tanto, hay un tutor académico por cada asignatura. Se expone en la tabla de docentes.
- **Coach educativo**. Realiza funciones académicas no directamente relacionadas con las materias del programa formativo, pero si con la necesidad de orientación del alumno en materia educativa general, motivación, gestión del tiempo, técnicas de estudio, etc.
- **Coach de prácticas**. Realiza funciones académicas no directamente relacionadas con las materias del programa formativo, pero si con el seguimiento del grado de cumplimiento de las actividad y tutela de las prácticas profesionales.
- **Coach académico** (secretaria o coordinadora académica). Realiza funciones académicas no directamente relacionadas con las materias del programa formativo, pero si con el seguimiento del grado de cumplimiento de las actividad y evaluaciones, uso y dudas de la plataforma, etc.

Además, la titulación cuenta con:

- El personal específico de la Escuela
- Los recursos humanos de administración disponibles en las Oficinas Generales de la Universidad. Este personal gestiona la matrícula y la expedición de títulos para los alumnos del Máster y un profesional con categoría de Directivo del Personal de Administración y Servicios (PAS).
- Los recursos humanos disponibles en las sedes de impartición del programa (Madrid, San Salvador, Santo Domingo, etc.). Esta sede cuenta con un equipo directivo y de administración y gestión que da servicio a todos los programas que allí se imparten.
- También cuenta con los servicios de Comunicación, Conserjería, Desarrollo, Protocolo, Admisión, Biblioteca, Prevención, Obras, Limpieza y Capellanía liderados por profesionales.

Mecanismos para asegurar la igualdad entre hombres y mujeres y la no ediscriminación de personas con discapacidad

El profesorado y el personal administrativo asignado al Máster se adecua a los principios establecidos por la Ley 3/2007, de 22 de marzo, para la igualdad efectiva de hombres y mujeres, así como por la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

RECURSOS MATERIALES Y SERVICIOS

Justificación de la adecuación de los medios materiales y servicios disponibles

El máster se coordina desde la sede central en Madrid (España), si bien las clases pueden desarrollarse en otras sedes de la universidad.

Se desarrolla una actividad continua de prospección y búsqueda de empresas colaboradoras, con el interés de establecer acuerdos y convenios de interés en el campo de conocimiento del programa. Todos ellos van encaminados a:

- Posible participación de profesionales de las empresas en:
    - La realización de "Talleres con Empresas" dentro de la Materia "Proyectos" impartiendo Masterclasses para acercar el mundo real y los casos prácticos a las aulas.

    - El "Trabajo Final de Máster" (TFM): propuesta por parte de la empresa de uno o varios retos/proyectos de interés para que los alumnos puedan poner en práctica lo aprendido en la parte teórica.
    - Prácticas extracurriculares
    - Otras mesas redondas, sesiones divulgativas temáticas, etc.
- Inclusión en la Bolsa de Trabajo propia del Máster, para reclutar a los perfiles que consideren más interesantes.
- Incorporación de empleados como alumnos del Máster

Instalaciones y recursos materiales

El máster se impartirá en el campus de la universidad. La sede de Madrid cuenta con las siguientes instalaciones y recursos materiales y técnicos:

- 2 aulas con capacidad entre 25 y 55 plazas. Estos espacios disponen de:
    - Proyección (16:10)
    - Micrófono de solapa
    - Micrófono de ambiente
    - TV de apoyo para alumnos virtuales
    - Sistema completo de emisión en streaming de la clase.
    - Conexiones:
        - 1 VGA + Audio
        - 1 HDMI
        - 2 USB
        - 1 Toma de red
        - Wifi interna
        - Wifi alumno
- 2 seminarios con capacidad para 8 personas que cuentan con:
    - Monitor 48"
    - Webcam
    - PC W11
    - Conexiones:
        - 1 VGA + Audio
        - 1 HDMI
        - 2 USB
        - 1 Toma de red

- Servicio de Biblioteca:
  La Biblioteca del edificio de Madrid contiene los manuales de la bibliografía recomendada.
  Los alumnos de máster podrán acceder a los recursos electrónicos de la biblioteca elibro.com

Los profesores que impartan docencia en el dispondrán de una mesa de trabajo en el espacio abierto destinado a la Administración de Alumni. También existen a disposición de los profesores del claustro un despacho y sala de reuniones.

Servicio de cafetería no atendida y espacio abierto para el alumnado de descanso y estudio.

Todo el edificio tendrá posibilidad de conexión a la red inalámbrica wifi.

Accesibilidad y mantenimiento

En cuanto a la accesibilidad, de acuerdo con lo dispuesto por la Ley 51/2003 de igualdad de oportunidades, no discriminación y accesibilidad de las personas con discapacidad, en el edificio han sido suprimidas las barreras arquitectónicas y de comunicación, de tal manera que estudiantes, profesores o empleados con discapacidad pueden desarrollar su actividad con normalidad. Por otro lado, desde la Universidad se facilita a los estudiantes con

cualquier tipo de discapacidad las condiciones de estudio y las adaptaciones adecuadas para su correcta formación académica.

Para la adecuada realización, mantenimiento y gestión de todas las instalaciones y medios materiales descritos, el campus de Madrid cuenta con personal para atender las tareas de mantenimiento, limpieza, al igual que técnicos para la asistencia a los equipos de las aulas, etc. Toda su actividad se centraliza en los servicios del campus de Madrid.

El Servicio de Prevención de Riesgos Laborales de la Universidad vela por el cumplimiento de la Ley 31/1995 de Riesgos de Prevención Laborales (y la Ley 54/2003.

Servicios vinculados a la docencia

- -Asesoramiento académico. Los estudiantes contarán con un tutor académico durante la realización del máster.
- -Sistema ADI: conjunto de herramientas informáticas de apoyo a la enseñanza accesibles desde Internet, que permite un cauce de comunicación continua entre profesores y estudiantes.
- Servicio de Carreras Profesionales. Su misión es ayudar a los estudiantes a diseñar su trayectoria profesional, y orientarles acerca de las salidas profesionales una vez concluido el máster.

Servicios para la gestión administrativa y académica

Como apoyo para la gestión académica del estudiante y del profesorado, La Universidad cuenta con la Administración de la sede, que gestiona directamente los horarios, datos personales de estudiantes y profesores, plan docente anual, resolución de instancias, listados de estudiantes, gestión presupuestaria, recursos materiales, etc.
Oficinas Generales, donde se realizan las matrículas en las diversas titulaciones que se imparten y en los programas Máster. También se encargan de la expedición de títulos y certificaciones académicas, tramitación de las instancias dirigidas al Rectorado de la Universidad y de todo lo relacionado con la Gestión Académica para el Alumno.

Relaciones internacionales, que informan, sensibilizan, coordinan y facilitan iniciativas sobre internacionalización y cooperación internacional. Este servicio ofrece, además, apoyo y atención a estudiantes internacionales.

Servicio de Asistencia Universitaria, donde se ofrece a los estudiantes información y asesoramiento sobre becas y ayudas al estudio, así como otras vías de financiación de los estudios universitarios.

Servicios de formación permanente. Los estudiantes y profesores cuentan, además, con un conjunto de servicios como apoyo a su formación permanente, intelectual y humana.

Calidad de los servicios

Periódicamente se aplican las encuestas de satisfacción previstas en el Sistema Interno de Calidad, donde estudiantes, profesores y personal de administración y servicios pueden manifestar su satisfacción con los servicios generales de la universidad y los recursos materiales de que disponen (informáticos, aulas, espacios de trabajo, laboratorios y espacios experimentales, bibliotecas y fondos bibliográficos, etc.). Todos los procesos (analítico, estratégico y de soporte) están incluidos en el Sistema de Garantía de Calidad.

Previsión de otros recursos

Se considera que las infraestructuras y equipamientos disponibles actualmente satisfacen con amplitud las necesidades del máster en lo que se refiere a recursos, instalaciones y servicios. No obstante, con los mecanismos existentes a nivel de calidad ya mencionados, en caso de detectarse nuevas necesidades, se adoptarían las medidas necesarias para cubrirlas.

RESULTADOS PREVISTOS

La definición de los resultados académicos queda descrita en el procedimiento PO-14 del sistema interno de gestión de la calidad.

Los valores cuantitativos son:

TASA	DEFINICIÓN	VALOR
Tasa de graduación	Porcentaje de estudiantes que finalizan en el tiempo previsto o un año más	75%
Tasa de abandono	Relación entre los estudiantes que debieron obtener el título en un año determinado y no se han matriculado en el siguiente	25%
Tasa de eficiencia	Calculada como el cociente entre los créditos necesarios para concluir la titulación y el número total de créditos matriculados y reconocidos, expresado en términos porcentuales.	80%

Justificación de los valores propuestos

En primer lugar, estimamos que, al tratarse de un máster orientado a profesionales, se reducen muy sustancialmente las posibilidades de abandono frente a otros títulos.

Asimismo, el plan de estudios diseñado posee un grado importante de variedad y flexibilidad para el alumno, lo cual favorece la adaptación a sus intereses personales y minimiza el abandono o retraso en la obtención del título.

Por último, el plan de asesoramiento permanente previsto velará para que el alumno se gradúe en el tiempo y forma previstos.

SISTEMA DE LA GARANTIA DE CALIDAD DEL TITULO

La Universidad cuenta cos un sistema de gestión interno de la calidad. Para ver más detalle vista el enlace https://www.spainbs.com/sistema-de-calidad

CALENDARIO DE IMPLANTACIÓN

El programa máster se ejecuta en dos ediciones:

- Edición de octubre: Inicio en octubre y finalización en septiembre del año siguiente. Las metodologías de enseñanza de la edición son:
  - Presencial
  - Semipresencial
  - Virtual

- Edición de febrero: Inicio en febrero y finalización en enero del año siguiente. Las metodologías de enseñanza de la edición son:
    - Semipresencial
    - Virtual

En cada implantación docente se generará un documento de calendario de implantación específico a disposición de profesores y alumnos, así como el detalle del cuadro profesional docente.

La primera edición del máster se realizó en octubre de 2024.

Las normas de permanencia son las siguientes:

a) El número máximo de años de permanencia será de cuatro.
1. Se dispone de un número máximo de seis convocatorias por asignatura, dos por curso académico, con independencia de la convocatoria de que se trate (convocatorias de febrero/junio o septiembre).

TITULACIÓN A OBTENER

Una vez el alumno finaliza con éxito el programa máster en la universidad obtendrá el siguiente título:

- Máster otorgado por Spain Business School y acreditado por Cualificam.
    - "Máster Profesional en MDB+ Máster en Digital Business"
    - Acreditación del máster FMID-CMP22-00033
- Máster título propio otorgado por la institución docente que imparte el programa en "Máster en Ciberseguridad"

Nota: Tanto el título de Máster Profesional como el Máster de Formación Permanente (universidad) requiere que el alumno sea título universitario y cumpla los requisitos del perfil de ingreso y acceso a la titulación.

El presente programa ha sido homologado y acreditado por:

- Fundación Madri+D (representación de Aneca de Madrid) a través del programa Cualificam. Certificado FMID-CMP22-00033 (Memoria de aprobación 2022)
- Universidad Católica de Murcia en su plan de estudios del convenio suscrito en 2016.

Reconocimientos y rankings

El programa Máster en Ciberseguridad cuenta con las siguientes recomendaciones y apariciones en rankings:

- Nº. 1 de ranking categoría Transformación digital de El Mundo 2022
- Nº. 2 de ranking categoría Transformación digital de El Mundo 2023
- Nº. 3 de ranking Ciberseguridad Financial Magazine 2024.
- Nº. 3 de ranking Digital Forbes 2022.
- Nº. 5 de ranking Digital Forbes 2021.

La escuela Spain Business School cuenta con los siguientes reconocimientos:

- Mejor escuela de negocios oapra fo4rmarse en Data Science en ranking El Mundo 2021
- Premio a la Excelencia Educativa como Mejor Escuela de Negocios de España 2021
- Premio internacional Prestige Adwards a la Mejor Escuela de Negocios 2021-22
- Premio a la Excelencia Educativa como Mejor Escuela de Negocios de España 2022
- Premio a la Excelencia Educativa como Mejor Escuela de Negocios de España 2024
- Top ranking EdUniversal 2024
- Top ranking educativo Innovatec 2024

La escuela Madrid Executive Business School cuenta con los siguientes reconocimientos:

- Premio a la Excelencia Educativa como Mejor Escuela de Negocios Online de España 2024
- Nº 2 ranking Mejor Escuela de negocios Online 2024 de Financial Magazine