PROGRAMA FORMATIVO EN CIBERSEGURIDAD PARA AMÉRICA LATINA Y EL CARIBE

BID

COSEC UC3M COMPUTER SECURITY LAB

PROGRAMA FORMATIVO EN CIBERSEGURIDAD PARA AMÉRICA LATINA Y EL CARIBE

Banco Interamericano de Desarrollo (BID)
Ariel Nowersztern
Santiago Paz
Darío Kagelmacher
Florencia Cabral Berenfus
Pablo Libedinsky

Computer Security Lab (COSEC)
Arturo Ribagorda
Juan Tapiador
José María de Fuentes
Lorena González

Clasificaciones JEL: F52, I20, I23, I25, I28, J24, J44, J45, O15, O30.

Palabras clave: ciberseguridad; educación superior.

Copyright © 2021 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Nótese que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.

Banco Interamericano de Desarrollo
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

El Sector de Instituciones para el Desarrollo fue responsable de la producción de la publicación.

Colaboradores externos:

Coordinación de la producción editorial: Sarah Schineller, A&S Information Partners, LLC
Revisión editorial: Claudia M. Pasquetti
Diagramación: Gastón Cleiman

PROGRAMA FORMATIVO EN CIBERSEGURIDAD PARA AMÉRICA LATINA Y EL CARIBE

BID

COSEC UC3M COMPUTER SECURITY LAB

Tabla de contenido

Índice de ilustraciones

Índice de cuadros

Prólogo

Vivimos en un mundo cada vez más digitalizado, donde las tecnologías desempeñan un papel crucial en nuestra calidad de vida. Las tecnologías digitales son ya un elemento fundamental en sectores tan variados como el financiero, el gobierno, el transporte, la energía, la salud o la educación. Y esta transformación se ha visto aún más acelerada con el inicio de la pandemia de COVID-19. En 2020 fuimos testigos de cómo la tecnología pasó de ser una comodidad a convertirse en una herramienta esencial.

Como nos recuerdan a diario las noticias, la digitalización ha incrementado nuestro uso de plataformas en línea y, con ello, la probabilidad de vernos afectados por los ataques cibernéticos. Dado el enorme impacto que los incidentes de ciberseguridad pueden tener en la vida de los ciudadanos –en lo económico, en su seguridad, privacidad, o en la continuidad de servicios esenciales–, es una responsabilidad conjunta de todos los actores del mundo digital estar preparados para enfrentar los riesgos del ciberespacio. Para ello, se necesitan recursos humanos capaces de defender nuestro entorno digital. Sin embargo, la evidencia muestra que uno de los grandes desafíos de la ciberseguridad es la escasez de profesionales capacitados. Se estima que para 2021 en el mundo habrá 3,5 millones de vacantes sin llenar en este campo, de las cuales 630.000 estarán en América Latina y el Caribe.

La formación de profesionales especializados en ciberseguridad es clave. Según demostró el Reporte de Ciberseguridad Regional publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) a mediados de 2020, aún existe amplio espacio para el desarrollo de programas de formación terciaria especializada en ciberseguridad en América Latina y el Caribe. Si la formación de profesionales no se refuerza en los próximos años, nuestra región no solo se encontrará expuesta a los cada vez más frecuentes ataques cibernéticos, sino que también verá limitada su capacidad de desarrollo digital. Los riesgos son demasiado grandes como para no hacer nada al respecto.

Desde el BID establecimos una productiva cooperación con la Universidad Carlos III de Madrid, una de las instituciones pioneras en ciberseguridad de

España y con una notable trayectoria académica en la materia. El primer producto de esta colaboración ha sido un curso en línea masivo y abierto (MOOC), que tuvo inicio a comienzos de 2020, enfocado en el aprendizaje de las herramientas y aplicaciones prácticas de ciberseguridad.

Las universidades y centros de formación terciaria cumplen un papel central en el desarrollo de talento humano, especialmente en áreas relacionadas con tecnologías avanzadas. El presente documento, producto de meses de diseño y validación, ofrece un programa de estudios de Maestría en Ciberseguridad de uso libre y gratuito, que apunta a cerrar la brecha de enseñanza en América Latina y el Caribe. Este programa es fruto de un esfuerzo compartido con 68 excelentes instituciones académicas de la región, cuya colaboración estrecha agradecemos. Desde el comienzo del proceso de elaboración, este programa ha sido evaluado y alimentado por las instituciones destinatarias, las cuales reflejaron sus necesidades y recomendaciones a través de encuestas y talleres de discusión. Para esta y otras iniciativas de ciberseguridad, el BID ha contado con el valioso apoyo técnico y financiero del gobierno de España.

Desde nuestra institución estamos muy comprometidos con el fortalecimiento del capital humano de ciberseguridad en la región. El presente documento se une a todos los esfuerzos que hemos venido impulsando en los últimos años para acercar el conocimiento experto y continuar prestando apoyo técnico y financiero a nuestros países miembros con el objeto de fortalecer el ciberespacio de América Latina y el Caribe, y seguir alentando el desarrollo digital en nuestras sociedades.

Miguel Porrúa

Coordinador del Cluster de Datos y Gobierno Digital
División Innovación para Servir al Ciudadano
Banco Interamericano de Desarrollo

Introducción y visión metodológica

/10

El presente documento describe un programa formativo en ciberseguridad, de nivel de máster, desarrollado por el grupo Computer Security Lab (COSEC) de la Universidad Carlos III de Madrid (UC3M) en colaboración con el Banco Interamericano de Desarrollo (BID) para la región de América Latina y el Caribe (ALC).

El desarrollo de este programa de ciberseguridad se ha realizado atendiendo a las necesidades y preferencias detectadas por distintas universidades latinoamericanas. Con él se busca desarrollar un plan enfocado en esta región y cuyo objetivo sea el egreso de profesionales en esta materia que satisfagan las necesidades existentes. Las aportaciones de dichas instituciones han sido recogidas por la UC3M e incorporadas en el programa formativo que aquí se presenta. Así, el diseño del programa se nutre, principalmente, de la visión aportada por las instituciones consultadas, aunque también de la experiencia docente en esta materia de la UC3M.

1. Metodología para la recolección de información

Para recabar la visión de las instituciones, se confeccionó una encuesta (en español y en inglés) con el fin de establecer las bases para el desarrollo del programa formativo. En ella se plantearon las siguientes cuestiones (el anexo 1 presenta la encuesta completa):

- ¿En qué idioma debería impartirse el programa?
- ¿Qué modelo de impartición sería el más aconsejable?
- Con independencia de la respuesta anterior, suponga que se opta por un modelo presencial. Si cada hora de clase presencial requiere 1 hora y 30 minutos de estudio individual, ¿qué carga docente presencial debería tener este máster?
- En su opinión, atendiendo a las necesidades formativas de su país, ¿cuál debería ser la duración de un máster en ciberseguridad?
- ¿Qué titulación deberían tener los estudiantes que accediesen a un máster de esta naturaleza?
- ¿Considera que el plan de estudios debería contemplar la realización de un trabajo de fin de máster (TFM) obligatorio?
- ¿Consideraría una posibilidad que el TFM se realizase como proyecto o trabajo de investigación en alguna empresa?
- ¿Cree que, de acuerdo con las necesidades de su país, el máster debería tener especialidades, de modo que, tras una formación generalista, los alumnos pudiesen elegir una especialidad entre dos o más?
- ¿Considera oportuno que los alumnos realicen parte de su formación en una empresa? [Periodo]
- ¿Cuál debería ser el porcentaje de la carga de este TFM respecto de la carga lectiva total presencial?
- Indique la demanda de las materias en ciberseguridad.

Con el fin de garantizar la eficacia del instrumento, la encuesta trató de concentrar el interés de la región en ciertas materias concretas, aunque sin contemplar los contenidos detallados que deberían abordarse en cada una. Estos pormenores habrían alargado notablemente la encuesta, sin aportar información relevante, debido a las disparidades que sin duda habrían manifestado las universidades encuestadas.

La encuesta fue acompañada del debido documento con información relativa al tratamiento de datos personales, a fin de que los encuestados pudieran

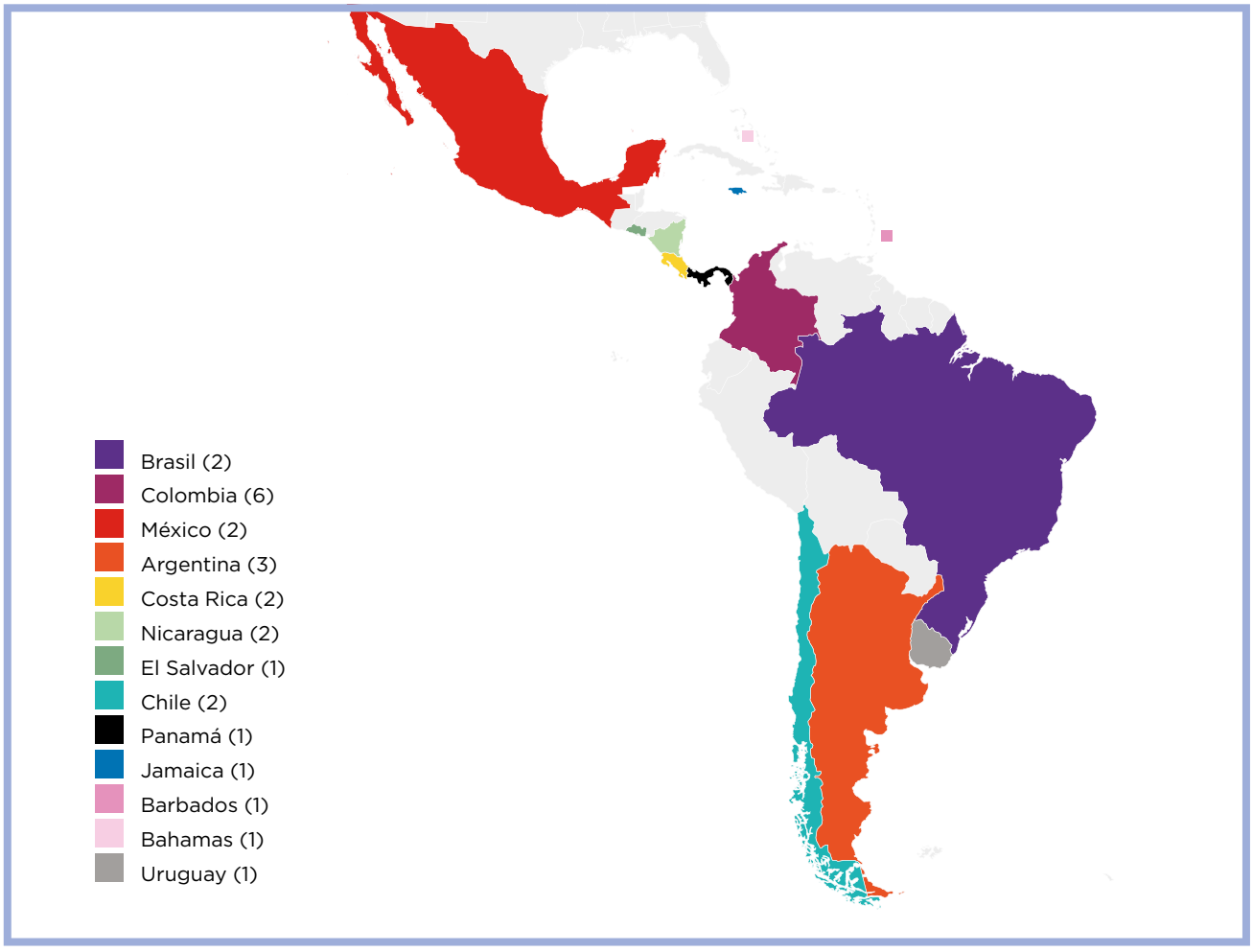
ejercer cualquiera de los derechos previstos en la normativa legal europea,[1] y su adaptación al marco constitucional español,[2] acerca de la protección y del tratamiento de sus datos.

La encuesta se remitió por correo electrónico a un total de 105 universidades latinoamericanas y del Caribe, y posteriormente se envió un recordatorio a las que no habían contestado. Más tarde, se hicieron llegar dos nuevas remesas de correos, la primera a siete profesores de ciberseguridad de universidades señaladas por la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) de México y la segunda a profesores de ciberseguridad de seis universidades de la región objeto del estudio. Se recibieron un total 31 respuestas, de las cuales se

1 Reglamento General (UE) 679/2018 de Protección de Datos Personales.

2 Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.

Ilustración 1. Países participantes y cantidad de universidades que han respondido la encuesta



descartaron una por incompleta y cinco por proceder de la misma institución académica. Así, se adoptaron como válidas un total de 25. La **ilustración 1** muestra los países que han participado de la encuesta y entre paréntesis el número de instituciones académicas en cada uno de ellos que han respondido a la misma.

2. Síntesis de las respuestas y recomendaciones recibidas

El análisis de las respuestas permitió establecer las bases del programa formativo. En la **ilustración 2** se presenta el idioma, el tipo de modelo de enseñanza, la duración del máster y la clase de formación que deberían tener los alumnos según los encuestados.

En lo que respecta al idioma, dada la diversidad de respuestas, no se considera recomendar uno de ellos sino más bien dejarlo al arbitrio de cada universidad. En cualquier caso, por la experiencia de los autores, un máster de carácter eminentemente técnico como el que nos ocupa debería ser impartido en inglés o, al menos, en modalidad bilingüe, siempre que el inglés sea una de las lenguas; por ejemplo, inglés-español, inglés-portugués, etc.

En la **ilustración 3** se muestra si los encuestados se manifestaron de acuerdo o no con establecer un TFM, realizar el mismo en una empresa, dividir el máster en especialidades y realizar parte de su formación en una empresa.

Como se observa, una abrumadora mayoría considera

Ilustración 2. Número de respuestas a la encuesta (I)

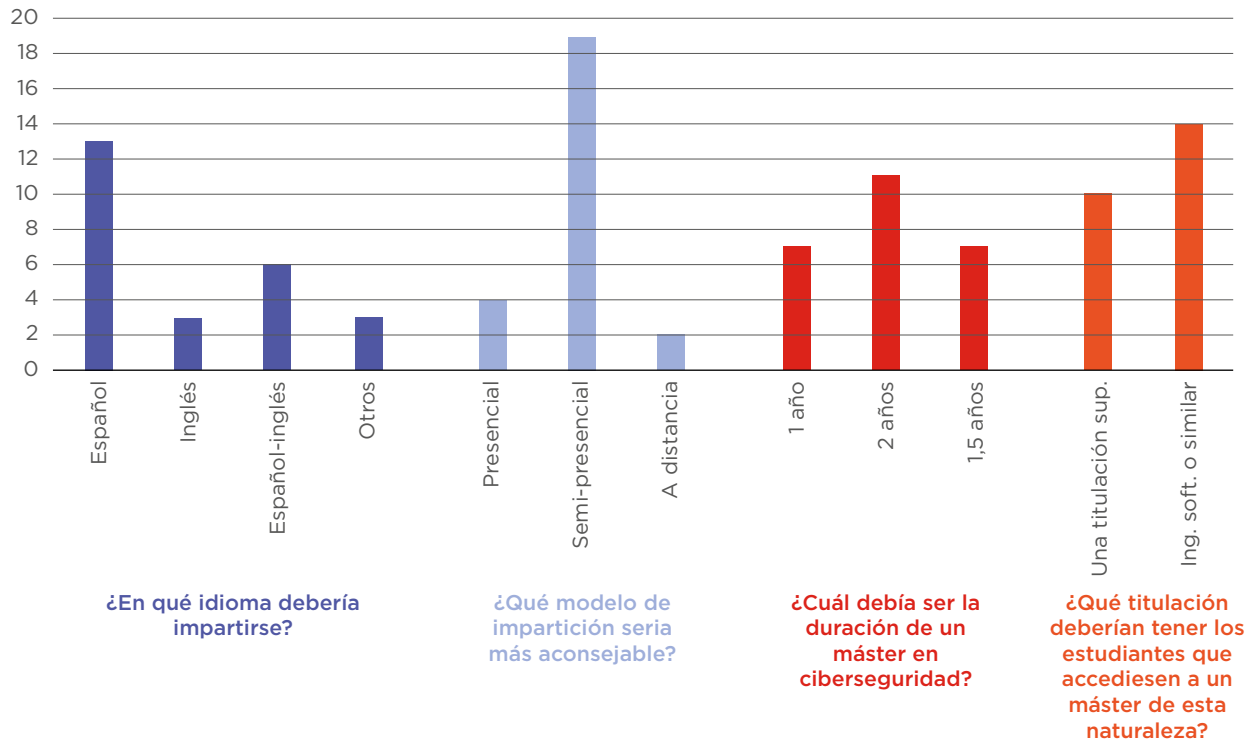
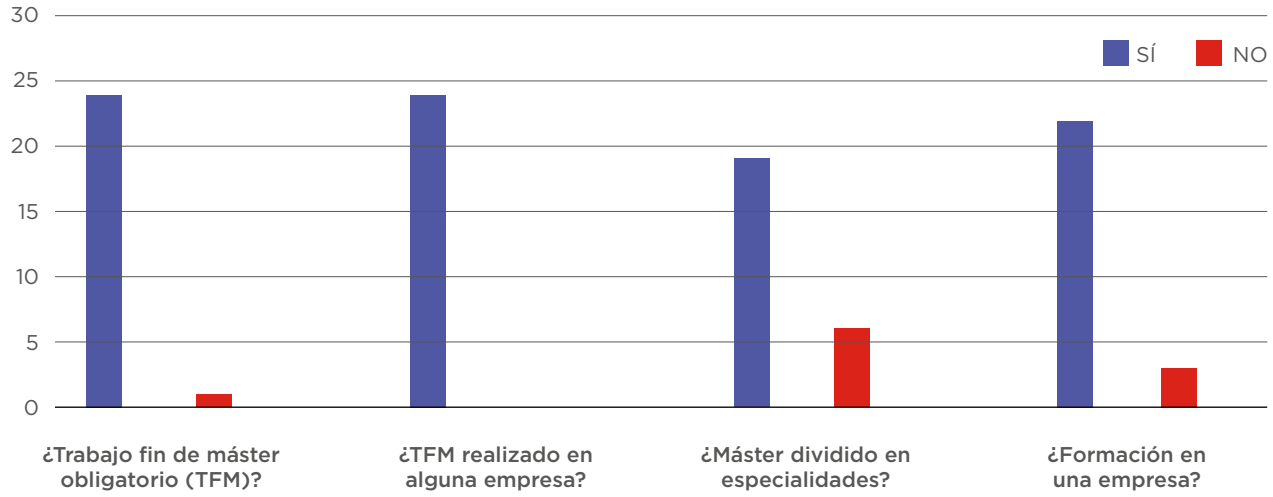


Ilustración 3. Número de respuestas a la encuesta (II)



que el máster debería incluir un TFM; todos, que debería realizarse en el seno de una empresa y casi todos, que los alumnos deberían completar su formación en una empresa (con independencia del TFM). Por último, también son más quienes se inclinan por establecer especialidades.

Con respecto a las materias concretas que podrían conformar el máster, el **cuadro 1** presenta la demanda esperada para las asignaturas planteadas.

En referencia al número de horas semanales de clases presenciales, los encuestados reflejan una

Cuadro 1. Número de respuestas sobre la demanda de asignaturas propuestas

Asignaturas propuestas	Alta demanda	Poca demanda
Desarrollo de sistemas de seguridad / Seg. DevOps	19	6
Analista en ciberseguridad	18	6
Seguridad en sist. industriales (incl. IoT)	10	14
Seguridad en sist. ciberfísicos	10	14
Seguridad en *cloud computing*	22	3
Seguridad en *big data*	19	6
Informática forense	17	7
Dirección y gestión de la seguridad	9	13
Seguridad en redes (IDS, SIEM, etc.)	21	4
Comunicaciones seguras (protocolos)	16	9

Cuadro 2. Síntesis de las recomendaciones facilitadas por las universidades de América Latina y el Caribe encuestadas

Característica	Valor sugerido
Duración	Dos años
Idioma	Debido a la dispersión de las respuestas, no es posible recomendar un idioma de impartición.
Formato de impartición	Semipresencial
Carga de horas de impartición	15 horas semanales
Formación previa	Ingeniero (Licenciado) en sistemas, de *software*, de computación y asimilados.
Trabajo de fin de máster (TFM)	Sí, y se prefiere realizarlo en una empresa
Orientación formativa	Formación generalista y especializada
Formación en empresas	Sí, por un periodo de tres meses
Materias más demandadas	• Desarrollo de sistemas seguros / Seguridad DevOps • Analista en ciberseguridad • Seguridad en *cloud computing* • Seguridad en *big data* • Informática forense • Seguridad en redes (IDS, SIEM, etc.) • Comunicaciones seguras (protocolos)

mayoritaria preferencia por una carga de 15 horas[3] semanales de carácter presencial.

Igualmente, sugieren que se habilite un periodo de formación en el ámbito empresarial de tres meses.

Por tanto, atendiendo a los resultados de la encuesta, el programa formativo tendrá, entre otras, las características que se exponen en el **cuadro 2**.

3. Incorporación de las recomendaciones al diseño del programa y adaptaciones introducidas

Las recomendaciones recibidas se han tomado en consideración para la elaboración del programa formativo. No obstante, durante la confección final del mismo ha sido necesario adaptar algunas de las recomendaciones, tomando diferentes decisiones que se sintetizan en los grupos expuestos a continuación.

Debido a que en su mayoría los encuestados han optado por permitir el acceso a titulados sin formación específica en tecnologías de la información

3 En el documento se hace referencia a horas de clase en vez de considerar créditos cuya duración, en términos de horas de clases presenciales y de trabajos del alumno, puede variar entre países.

y las comunicaciones (TIC), así como por establecer especialidades, realizar una estancia en empresas u organismos públicos y elaborar un TFM, parecía oportuno a efectos organizativos agrupar las asignaturas en módulos según su naturaleza. Así, las asignaturas a cursar por alumnos sin conocimientos específicos de TIC se incorporan a un módulo que se ha llamado de nivelación (módulo 0); las generales de ciberseguridad figuran comprendidas en un módulo denominado generalista o de ciberseguridad general (módulo 1); las asignaturas de especialización, en uno de este mismo nombre (módulo 2); las electivas, en uno llamado de formación complementaria (módulo 3) y por último el TFM y las prácticas en empresas en el designado TFM/prácticum (módulo 4).

a) Incorporación de asignaturas que no figuraban entre las más demandadas

Se ha incorporado una asignatura cuya demanda no había sido identificada como alta, pero cuyo estudio se ha estimado imprescindible para el correcto aprovechamiento de este máster. Se trata de Criptografía aplicada, asignatura que en gran parte de los programas de posgrado en ciberseguridad se dedica, entre otros temas, a tratar las técnicas criptográficas (incluidas las funciones *hash*, firma digital, etc.).

Así mismo, se ha optado por incorporar al programa propuesto otras asignaturas que por experiencia también se consideran convenientes, aunque en este caso como formación elegible al margen de las especialidades. Estas, junto con otras señaladas como más demandadas configuran el módulo 3, Formación complementaria.

Así, en relación con la asignatura "Dirección y gestión de la seguridad" se ha optado por incluirla en el módulo 1 (por tanto, como obligatoria) con el fin de cubrir algunos contenidos demandados por los encuestados como la auditoría y contemplar otros temas; por ejemplo, los sistemas de gestión de la seguridad de la información (familia ISO/IEC 27000, COBIT, marco del NIST) de importancia creciente.

También se han añadido Seguridad en el Internet de las cosas (IoT, por sus siglas en inglés) y Seguridad en sistemas ciberfísicos. Ambas materias están adquiriendo una gran relevancia por la dependencia creciente de los sistemas de control industriales (y fundamentalmente los que soportan infraestructuras críticas) de las tecnologías de la información (TI). Dicho de otro modo, se trata de la integración de las TI en las tecnologías operacionales (TO). Los especialistas en esta materia están siendo cada vez más demandados, según se va desplegando la Industria 4.0 (de la mano en gran parte del IoT).

Finalmente, se ha optado también por incluir una asignatura elegible sobre los aspectos legales de la ciberseguridad, habida cuenta de la cada vez más numerosa incorporación de esta materia a normas legales de todo tipo (códigos penales que contemplan el delito informático, leyes de protección de datos personales, de regulación del uso de Internet y del comercio electrónico, etc.) que no parece que puedan sustraerse de un proyecto formativo en ciberseguridad, aunque sea como materia de libre elección.

Por otra parte, se incorpora la asignatura "Protección de datos", por considerarse imprescindible para comprender muchos de los conceptos asociados con ciberseguridad, cuestión mencionada también por alguno de los encuestados.

b) División de asignaturas

Por cuestiones de metodología docente, y especialmente si se considera alcanzar un calendario equilibrado en el conjunto del periodo de impartición, se han dividido algunas de las asignaturas propuestas en la encuesta en unidades docentes menores. En concreto, la asignatura "Seguridad en redes" se ha considerado oportuno dividirla en "Técnicas de ciberataque" y "Sistemas de ciberdefensa"; y "Analista de ciberseguridad" se desglosaría en "Explotación de sistemas *software*", "Análisis de *malware*", "Amenazas persistentes avanzadas" y "Seguridad en dispositivos móviles". Esta división busca, además, que haya un tratamiento de los conceptos más dirigido, con el consiguiente mayor nivel de profundidad, lo que redundará en un mayor grado de especialización de los egresados.

c) Caracterización de asignaturas y definición de optatividad

Con el fin de conformar una propuesta formativa adaptable al alumno, cualquier programa incluye una fracción de asignaturas que adoptan un carácter optativo. En este sentido, se ha elegido incorporar como tales aquellas en las que se ha indicado una menor demanda (particularmente, "Seguridad en IoT" y "Seguridad en sistemas ciberfísicos"). Además, y en vistas del conjunto global diseñado, se han propuesto otras que pueden resultar de interés atendiendo al panorama actual de la ciberseguridad.

4. Refinamiento de la propuesta inicial y taller de presentación de resultados

Concluida la elaboración de la propuesta inicial, esta fue elevada al BID para que propusiera las recomendaciones que considerara oportunas, y que –tras debatirse– se incorporaron a la misma. Esta propuesta así enriquecida se distribuyó a las universidades que participaron en la encuesta para recibir sus comentarios y reflexiones, los cuales, sumados a la propuesta, dieron lugar al borrador final del programa formativo.

Para concluir, este borrador se discutió durante talleres virtuales, a los que se invitó a diferentes universidades de la región, y de allí resultó el programa formativo definitivo. Se realizaron dos talleres virtuales entre octubre y diciembre de 2020, en los cuales participaron 54 universidades en total.

Programa

/18

1. Descripción del título

El programa de estudios de este máster pretende que los alumnos adquieran conocimientos científicos y tecnológicos avanzados sobre la ciberseguridad, fundamentalmente en sus aspectos más técnicos. Su principal objetivo es proporcionar habilidades, aptitudes y conocimientos teóricos y prácticos en dicho campo, de manera sólida pero flexible para facilitar su adaptación a un entorno tan rápidamente cambiante como este.

Título: Máster en Ciberseguridad

Idioma: A elegir por la universidad

Duración: 2 años, repartidos en 4 cuatrimestres

Número de horas impartidas totales: entre 1.480,5 y 1.699,5 horas

2. Justificación del título

2.1 Justificación del título propuesto, argumentando el interés académico, científico o profesional del mismo

En pocos años la seguridad de la información, y más concretamente la ciberseguridad, ha cobrado una importancia extraordinaria en todos los sectores sociales, públicos y privados, de todos países e incluso a nivel personal de los habitantes de casi todos ellos. Obviamente, ello se debe a la dependencia crítica que nuestras sociedades tienen de los sistemas y redes de comunicación, que en caso de interrupción o simple degradación del servicio recibido, se pondría en serios aprietos a sectores esenciales de estos países. Un ejemplo de ello se muestra en el Global Risks Report[4] que anualmente publica el Foro Económico Mundial (FEM) y que año tras año sitúa a los ciberataques como uno de los riesgos más relevantes en cuanto a probabilidad de ocurrencia e impacto. Así, en la edición decimoquinta del Foro de este año 2020, de un total de 30 riesgos estudiados, los ciberataques aparecen como el séptimo riesgo con mayor probabilidad de ocurrencia y el octavo por impacto. En el informe también figuran los riesgos de robo o fraude de datos y las interrupciones de la infraestructura de información, ambos muy vinculados a los ciberataques.

Por otra parte, el Global Cibersecurity Index,[5] que bienalmente publica la Unión Internacional de Telecomunicaciones (UIT)[6], en su edición de 2018 (última publicada en la fecha del presente informe), clasificó a los países que lo conforman (casi 200) según su nivel de ciberseguridad.[7] Esta clasificación agrupa a los países en tres grandes bloques: países con alto, medio y bajo compromiso con la ciberseguridad.

El primer país de la región de América Latina y el Caribe es Uruguay, que figura en la posición 55.ª (y última) dentro del bloque de países con alto compromiso. Para encontrar el siguiente país de la región se debe descender a la 14.ª posición, pero ya dentro del bloque de compromiso medio (que comprende 53 países), seguido de otros 10 países de la región. Por último,

4 Véase https://www.weforum.org/reports/the-global-risks-report-2020.

5 Véase https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

6 La UIT está constituida por más de 190 países y 800 entidades privadas y públicas.

7 Para su clasificación, se valoran cinco criterios que se denominan pilares. Estos son: legal (marco legal del tratamiento de ciberseguridad y ciberdelincuencia); técnico (instituciones técnicas y marco de tratamiento de ciberseguridad); organizacional (políticas de cooperación institucional, estrategias de ciberseguridad nacionales); fomento de capacidades (investigación, formación, certificación profesional, agencias públicas de impulso) y cooperación (marco de cooperación, redes de compartición de información).

entre los países de bajo compromiso se hallan otros 13 países de la misma región.

De todos modos, si se desea enfocar exclusivamente la región estudiada, el informe más relevante por su nivel de detalle es el titulado "Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe",[8] edición de 2020, del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA). Este reporte toma como base el "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)", desarrollado por el Centro Global de Capacitación de Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford.[9]

El CMM evalúa la robustez de la ciberseguridad desde cincos puntos de vista (o dimensiones, según la terminología del modelo): política y estrategia de ciberseguridad; cultura cibernética y sociedad; educación, capacitación y habilidades en ciberseguridad; marcos legales y regulatorios, y estándares, organizaciones y tecnologías. A su vez, desglosa estas dimensiones en factores (por ejemplo, la primera dimensión la conforman los factores estrategia nacional de ciberseguridad, respuesta a incidentes, y protección de infraestructuras críticas, entre otros) y finalmente subdivide estos factores en distintos componentes (aspectos, en sus propios términos), los cuales analiza para asignar a cada uno de ellos una puntuación, de 1 a 5, según su nivel de evolución (madurez). Estas puntuaciones se corresponden respectivamente con: inicial, formativa, consolidada, estratégica y dinámica. Con estas herramientas del modelo, el informe obtiene el nivel de madurez de cada uno de los países de América Latina y el Caribe.

A la vista de los resultados, el informe señala: *"(...) aunque América Latina y el Caribe ha mejorado sus capacidades de ciberseguridad desde 2016, el nivel de madurez promedio de la región todavía está entre 1 y 2, tomado del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (en el que 1 significa etapa Inicial y 5 significa Dinámica o Avanzada)"*.

En todo caso, el estudio también constata una gran disparidad de resultados entre los diferentes países que conforman la región. Así, mientras que la subregión del Cono Sur presenta el nivel de madurez más elevado en las cinco dimensiones (se mantiene entre 2 y 3), la subregión del Caribe muestra un nivel promedio de entre 1 y 2 en las dimensiones citadas.

En resumen, ya sea que se considere el Global Cibersecurity Index de la UIT o la edición 2020 del informe "Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe" de la OEA y el BID, el resultado es el mismo y expone la fragilidad global de la región (ciertamente con grandes diferencias entre países) en lo que a ciberseguridad respecta.

En cualquier caso, y ya que la seguridad nunca es absoluta, todos los países en mayor o menor grado presentan debilidades en sus sistemas de ciberseguridad, como lo demuestran las estadísticas anuales del Internet Crime Complaint Center del Federal Bureau of Investigation (FBI) de Estados Unidos, que en su *Internet Crime Report*[10] (edición de 2019, última en la fecha del presente estudio) registra un total mundial de 467.361 denuncias, con pérdidas globales de US$3.500 millones. Y eso considerando el dato generalmente aceptado de que el nivel de denuncia de los ciberdelitos es menor

8 Observatorio para la Ciberseguridad de ALC (con la participación del BID, la OEA y el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford), Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe, 2020. Véase https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

9 Véase https://www.oxfordmartin.ox.ac.uk/cyber-security/.

10 Véase https://pdf.ic3.gov/2019_IC3Report.pdf.

que el de cualquier otro tipo de delito, ya sea por la escasa confianza en su esclarecimiento o por la pérdida reputacional que para las empresas supone el reconocimiento de su incapacidad para evitar este tipo de crímenes.

A pesar de esta renuencia a denunciar, en su informe anual de 2018 sobre Estado de la Unión, el presidente de la Unión Europea señalaba que en algunos países europeos los ciberdelitos suponían más del 50% del total de delitos denunciados.[11]

Este ingente volumen de ciberdelitos se ha puesto aún más de manifiesto con la pandemia de la COVID-19. El incremento del teletrabajo, de las reuniones online, del comercio electrónico, de la educación a distancia, etc. ha propiciado un gran aumento de los ciberataques, algunos de ellos contra infraestructura crítica tan importante en estos momentos como la sanitaria.

Sin duda alguna, un facilitador de los ciberdelitos es la carencia mundial de expertos en ciberseguridad, pues la capacidad formativa de las universidades, centros de capacitación profesional y empresas de formación no siempre es suficiente para suministrar los profesionales en ciberseguridad que demandan las empresas y los organismos públicos. Así, según el National Institute of Standard and Technology (NIST), entre septiembre de 2017 y octubre de 2018 se demandaron 313.735 expertos en ciberseguridad.[12] Por su parte, la consultora Frost & Sullivan calculaba que la cantidad de profesionales en ciberseguridad necesarios en 2019 ascendía a casi 5 millones en todo el mundo, mientras que estimaba en casi 4,5 millones los profesionales efectivamente existentes en esa fecha, con un evidente desfase de medio millón de estos trabajadores.[13]

A este respecto, la situación en América Latina y el Caribe es aún peor. Tal y como ha apuntado el CEO de Capabilia, tras su alianza con Deloitte, *"América Latina es hoy, después de Asia, la zona que más vacantes tiene que llenar"*.[14]

Esta carencia de formación en la región se ve refrendada en el citado reporte de ciberseguridad 2020 del BID y OEA, que en el marco de la dimensión "Educación, capacitación y habilidades en ciberseguridad", del modelo CMM arriba mencionado, refleja una madurez no mejor que la presentada en otras dimensiones.

Según este informe, tan solo un tercio de los países de la región ha realizado avances en esta dimensión, obteniendo niveles de madurez medios (grado consolidado), aunque por ejemplo Uruguay llega al nivel estratégico. No obstante, según los profesores Pablo Ruiz Tagle-Vial y Daniel Álvarez Valenzuela: *"El presente reporte da cuenta de un escaso o nulo avance en el nivel de madurez de dos tercios de los países de América Latina y el Caribe en materia de educación, capacitación y desarrollo de habilidades en ciberseguridad. En estos países, la oferta de formación especializada en seguridad digital es inexistente o tiene carácter de incipiente, y usualmente considera solo la dimensión técnica de la ciberseguridad".*

Si se consideran ahora los tres factores (Sensibilización, Marco para la educación y Marco para la formación profesional) que conforman la tercera dimensión "Educación, capacitación y habilidades en

11 Véase https://ec.europa.eu/info/sites/default/files/soteu2018-factsheet-cybersecurity_es.pdf.

12 Véase NIST, New Data Show Demand for Cybersecurity Professionals Accelerating: https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating.

13 Frost & Sullivan, The 2015 (ISC)2 Global Inform. Sec. Workforce Study.

14 Véase Martín Sola y el empleo en ciberseguridad (enero de 2020) en https://tecno.americaeconomia.com/articulos/martin-sola-y-el-empleo-en-ciberseguridad-america-latina-es-hoy-despues-de-asia-la-zona.

ciberseguridad" del CMM, se observa lo siguiente:

- En lo que se refiere a la "Sensibilización" o concienciación, la amplia mayoría se sitúa en niveles "formativos" o "establecidos" (es decir, los niveles segundo y tercero). No obstante, algunos países, como Venezuela, todavía están en el nivel "inicial". En el otro extremo se ubica Uruguay, que muestra un meritorio indicador "estratégico".

- En lo que concierne al "Marco para la educación", ninguno de los países alcanza niveles "estratégicos" o "dinámicos". La amplia mayoría se sitúa en niveles intermedios ("formativos" o "establecidos"), si bien hay cinco países todavía en fase "inicial".

- Finalmente, en lo referente al "Marco para la formación profesional", el panorama es diferente con respecto a los indicadores anteriores, aunque igualmente susceptible de mejora. En este caso, la amplia mayoría de los países se ubica en el nivel "formativo", si bien cinco de ellos están en el nivel "establecido" y nuevamente Uruguay se posiciona en el nivel "estratégico".

A la vista de los indicadores anteriores, la situación educativo-formativa en ciberseguridad en ALC se beneficiaría sustancialmente de un título de máster que, adecuadamente implantado en las universidades participantes, permita la adquisición y consolidación de capacidades avanzadas en todas las facetas de la ciberseguridad. El carácter académico del título permitirá paliar la carencia de una aproximación sistemática y rigurosa a este campo de conocimiento, con la oferta de un plan estructurado que permita una capacitación sólida. Además, es previsible que la implantación de este título sirva como catalizador para la aparición de iniciativas académicas en niveles inferiores (fundamentalmente en las ingenierías o licenciaturas) que faciliten la preparación para el acceso al título propuesto.

2.2 Modelo docente semipresencial: justificación y características

Aunque el modelo de enseñanza universitaria presencial está sólidamente asentado en la sociedad y presenta ventajas innegables, sobre todo en los estudios tecnológicos, no es menos cierto que los cursos semipresenciales de asignaturas técnicas, que solo exigen la personación del alumno durante las clases prácticas, están ganando terreno rápidamente. Esto es cierto sobre todo en los estudios técnicos de posgrado a los que cada vez se apuntan más profesionales titulados que desean cambiar o profundizar su orientación laboral.

El modelo de aprendizaje semipresencial que se plantea para este título cuenta con una sólida base de información, que se combina de manera natural con un conocimiento práctico de habilidades, estrategias y herramientas técnicas que habilitan la resolución de nuevos problemas, y la anticipación de futuras amenazas de ciberseguridad.

La semipresencialidad o *b-learning* (del inglés, *blended learning*, también aprendizaje mixto o bimodal) permite aunar las ventajas del modelo tradicionalmente presencial con las derivadas de la aplicación de la tecnología aplicada al aprendizaje (o *e-learning*). De hecho, habilita un nivel de seguimiento mucho más rico e individualizado, en tanto que las plataformas de enseñanza (como Moodle, Edx, Blackboard Collaborate, Hangouts Meet, etc.) ofrecen multitud de indicadores sobre el desempeño del alumno. Así, es posible determinar si se está siguiendo el plan previsto, si se intenta realizar un cierto ejercicio y si se están superando las pruebas formativas o de evaluación, entre otros muchos indicadores.

La modalidad semipresencial en la que se ofrece este máster está plenamente justificada, considerando una serie de factores. En primer lugar, procede de las recomendaciones de las instituciones académicas consultadas para la preparación de esta propuesta. Por

otra parte, en los últimos tiempos se ha evidenciado un incremento del número de alumnos que optan por una modalidad no puramente presencial, ya que permite una mejor conciliación con el entorno laboral y personal del alumnado.

En este sentido, la actual pandemia global del COVID-19 ha evidenciado la conveniencia de optar por modalidades educativas que no dependan exclusivamente de una presencia física en los centros docentes y, en este caso, puedan tornarse totalmente en no presenciales.

El último de los factores para considerar es que la consecución de las competencias que se desgranan en este documento es alcanzable a través del modelo de enseñanza semipresencial, en cuyo caso el concurso de una plataforma de enseñanza virtual y las clases presenciales son medios complementarios para desarrollar estrategias docentes adecuadas para la ciberseguridad.

Debe destacarse que este ámbito de conocimiento exige de forma singular la aplicación práctica de los conocimientos teóricos adquiridos. Así, es imposible disociar ambas facetas del aprendizaje, pues el especialista en ciberseguridad ha de contar con el bagaje teórico y el conocimiento práctico, de forma similar a otras materias que demandan un alto grado de experimentación.

Además, es importante considerar un marco de formación tanto para estudiantes como para docentes. La semipresencialidad exige el uso de herramientas y recursos de variada índole, de modo que los alumnos deben estar preparados para este nuevo modelo docente y los profesores deben contar con los conocimientos adecuados para impartir sus clases aplicando este modelo.

En todo caso, debe ser el criterio de cada universidad el que determine la modalidad de impartición, pues, por ejemplo, puede ser que potenciales alumnos de ciertas zonas de influencia de una universidad tengan una infraestructura de comunicación inadecuada para la enseñanza semipresencial.

2.2.1 Medios docentes necesarios

Con el fin de dar cabida a esta modalidad docente, las Instituciones educativas deberán contar con una serie de recursos y medios que garanticen la impartición eficaz. En este sentido, además de las propias herramientas telemáticas que permitan la difusión de materiales y la comunicación profesor-alumno, será necesario proporcionar ciertos elementos de información que permitan al estudiante un adecuado seguimiento del plan de estudios. Entre estos elementos se encuentran:

- Un sitio web específico donde se detalle el funcionamiento de esta modalidad formativa y los recursos y medios que estarán a disposición de los alumnos.

- Un cronograma semanal por asignatura, en el cual se especifique no solo la tarea que debe realizar el estudiante sino también las horas de dedicación previstas y las actividades docentes (incluso las evaluativas) que se desarrollarán.

En relación con los medios técnicos que deberán habilitarse para el modelo docente escogido, debe destacarse la necesidad de incorporar sistemas de videoconferencias en las aulas docentes. Esto permitirá que las sesiones presenciales se puedan emitir en directo y que además se graben para que queden a disposición de los alumnos a lo largo del periodo lectivo. Así, se facilitará el seguimiento de las sesiones, especialmente para aquellos estudiantes que por su situación tengan dificultades singulares para acudir a las clases (en aquellas asignaturas que no exijan la presencia a todas las sesiones).

Además de los citados sistemas de videoconferencias, se deberá contar con el equipamiento mínimo para la gestión de la retransmisión y producción del vídeo,

como una cabina de control y personal de supervisión de los medios audiovisuales.

Para un máximo aprovechamiento del modelo docente, sería recomendable que el aula de impartición contase con conectividad y equipamiento informático que le permitiese al profesor interactuar con los alumnos durante la sesión, incluso con aquellos conectados en remoto. Para ello, sería recomendable contar con espacios de conversación interactivos tales como chats, foros de discusión o redes sociales.

Finalmente, dado el alto nivel de experimentación de este máster, es necesario que los alumnos dispongan de la infraestructura adecuada para completar con éxito su formación. Esto se puede conseguir por dos vías:

- **Alumnos con equipos con prestaciones adecuadas.** Los equipos deben tener la suficiente capacidad como para ejecutar múltiples máquinas virtuales simultáneamente para, por ejemplo, lanzar ataques.

- **Organización con un sistema de gestión de usuarios y máquinas virtuales.** Los servicios en la nube son una buena alternativa, en especial los conocidos como sistemas de cyber range para el entrenamiento con entornos ya preparados. Alternativamente, se puede optar por la adquisición de una cantidad de servidores adaptados al número de estudiantes y la compra de licencias de *software* de hipervisor (por ejemplo, VMWare vSphere) para simular distintos entornos de red con múltiples tipos de máquinas virtuales.

2.3 Perfil del egresado y resultados de aprendizaje

El alumno que quiera cursar este máster debe tener una buena base de TIC. El carácter eminentemente práctico del máster requiere contar con un sólido conocimiento de programación, lo cual abarca el uso de los lenguajes C, Java o Python; de sistemas operativos, con discernimiento de los distintos tipos de procesadores, memorias y arquitecturas existentes; y de telecomunicaciones y redes, para conocer los funcionamientos de las redes y los principales protocolos de comunicación. En concreto, la formación previa se establece en el Módulo 0 de este curso, cuya función consiste en proporcionar a los alumnos que no hayan cursado materias asociadas a las tecnologías y las comunicaciones, una buena base y un punto de partida para aprovechar satisfactoriamente las clases teóricas y prácticas.

En otro orden, la curiosidad y la inquietud por la ciberseguridad, así como la creatividad, la capacidad de innovación, el pensamiento crítico y el interés por el aprendizaje continuo son cualidades muy valorables para los potenciales estudiantes del máster.

En lo que respecta a los resultados de aprendizaje, estos se deberían valorar atendiendo a varios instrumentos. Por un lado, se debería contar con encuestas de valoración efectuadas a los estudiantes que, a modo introspectivo, permitirían un análisis del nivel de conocimiento adquirido tras cursar la asignatura. En ellas también valorarían su percepción de la utilidad de dicha asignatura y del método empleado para su impartición. Asimismo, se debería recabar de los alumnos propuestas de mejora para el programa de cada asignatura, para su enseñanza y para el sistema de evaluación de los conocimientos adquiridos.

De la misma manera, se debería recoger la opinión del personal docente (profesores y coordinadores) acerca de su nivel de satisfacción con el desarrollo del curso, el porcentaje de los programas realmente desarrollado, la adecuación del ritmo de enseñanza para alcanzar ese porcentaje y cualesquiera otros indicadores del nivel académico percibido en los alumnos, y su grado de compromiso y seguimiento en relación con las actividades académicas planteadas en la asignatura.

En cualquier caso, los anteriores y cualquier otro instrumento de valoración del proceso de enseñanza-aprendizaje tendrían que estar alineados con lo establecido en el programa de garantía interna de la calidad académica de la Institución que otorgue el título.

3. Competencias

Las competencias establecidas son el mínimo común múltiplo de las competencias que figuran en una muestra significativa de memorias de verificación, de másteres similares al que nos ocupa, aprobadas por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) de España, que es el organismo público responsable de aprobar el otorgamiento de títulos oficiales en el país.

Las **competencias básicas**, presentadas en el **cuadro 3**, constituyen una serie de destrezas, conocimientos y actitudes adaptadas a los diferentes contextos. Así, son aquellas que cualquier estudiante debe adquirir para su desarrollo profesional y su adecuada integración en el entorno laboral en el que desarrollaría su trabajo.

Cuadro 3. Competencias básicas

Código	Denominación
CB1	Disponer de conocimientos que permitan desarrollar o aplicar ideas de forma original, a menudo en un contexto de investigación.
CB2	Aplicar los conocimientos adquiridos y las capacidades desarrolladas de resolución de problemas en entornos novedosos relativos a la ciberseguridad.
CB3	Emitir juicios a partir de información potencialmente incompleta, inexacta o limitada, que incluyan reflexiones sobre las responsabilidades sociales y éticas de su actividad profesional.
CB4	Comunicar sus conclusiones y argumentos subyacentes a públicos diversos, no necesariamente especialistas, con claridad y eficacia.
CB5	Incorporar las habilidades necesarias para un ciclo continuo de aprendizaje que puede ser en gran medida autodirigido o autónomo.
CB6	Disponer de capacidad de coordinación en equipos de trabajo cuya interacción se desarrolle, total o parcialmente, a través de medios de comunicación electrónicos.

Cuadro 4. Competencias generales

Código	Denominación
CG1	Comprender y aplicar métodos y técnicas de investigación de ciberataques a un sistema informático concreto.
CG2	Concebir, diseñar, implementar y mantener un sistema global de ciberdefensa para un entorno técnico definido.
CG3	Elaborar documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad que cuenten con rigor, claridad, concisión y sencillez.
CG4	Conocer la normativa técnica relativa a la ciberseguridad y sus implicaciones para el diseño, la operación y el aseguramiento de sistemas informáticos.
CG5	Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).
CG6	Comprender el estado de las ciberamenazas, a nivel global en general y en el ámbito de América Latina y el Caribe (ALC) en particular, y expresar su alcance mediante un lenguaje técnico claro y preciso.

Cuadro 5. Competencias específicas

Código	Denominación	Áreas de conocimiento de CCG
CE1	Analizar y detectar anomalías y firmas de ataques a los sistemas informáticos y redes de comunicaciones.	*Component Security, Organizational Security*
CE2	Analizar y detectar técnicas de ocultación de ataques a sistemas informáticos y redes de comunicaciones.	*Software Security*
CE3	Conocer las tendencias actuales en técnicas de ciberataque y las consecuencias reales que acarrean.	*Software Security, Societal Security*
CE4	Analizar sistemas para encontrar evidencias de ataques en los mismos, determinar su impacto y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.	*Software Security*
CE5	Aplicar servicios, mecanismos y protocolos de seguridad oportunos para el aseguramiento de una infraestructura informática específica.	*Data Security*
CE6	Diseñar y evaluar arquitecturas de seguridad de sistemas informáticos y redes de comunicación.	*Software Security, System Security*
CE7	Conocer y aplicar los mecanismos criptográficos pertinentes para proteger los datos tanto almacenados en un dispositivo como en tránsito a través de las redes.	*Data Security*
CE8	Analizar y gestionar los riesgos de la introducción de dispositivos personales en un entorno corporativo, y establecer las contramedidas adecuadas para mitigarlos.	*Organizational Security*
CE9	Capacidad para aplicar las metodologías existentes al análisis y gestión de riesgos, transmitir los resultados obtenidos y proponer el tratamiento de riesgos oportuno para un entorno corporativo particular.	*Organizational Security*
CE10	Conocer las amenazas propias de los sistemas ciberfísicos, sus mecanismos específicos de protección y ser capaz de anticiparse a las amenazas que puedan surgir y saber responder a ellas.	*Software Security, System Security*
CE11	Conocer las amenazas derivadas del tratamiento de datos masivos (*big data*) y aplicar medidas de protección eficaces preservando las necesidades propias de dichos entornos operacionales.	*Software Security, System Security*
CE12	Establecer el nivel de seguridad de un sistema basado en la computación en la nube y aplicar medidas de protección proporcionadas y eficaces.	*Software Security, System Security*
CE13	Conocer los procesos y técnicas de desarrollo de programas informáticos que incorporan las necesidades de ciberseguridad desde su diseño hasta su puesta en producción.	*Component Security*

Las **competencias generales**, expuestas en el **cuadro 4**, se refieren a las habilidades, los atributos, los valores y las cualidades que el alumno debería alcanzar. Son generales por cuanto su adquisición se produce al aproximarse a la disciplina de la ciberseguridad de forma global, por lo que son "transversales" a las tecnologías de la información y las telecomunicaciones y a otros campos del saber.

Las **competencias específicas**, presentadas en el **cuadro 5**, se refieren a habilidades concretas relacionadas con un determinado puesto de trabajo y es donde más se denotan las especificidades puntuales de la empresa u organización. Además, para cada competencia, se ha identificado su equivalencia con las áreas de conocimiento establecidas en la ACM Cybersecurity Curricular Guidance (CCG).[15]

Nótese que las competencias básicas en particular se podrían adaptar según las competencias propias de América Latina y, más concretamente, del país en el que se desarrolle el máster.

4. Acceso y admisión de estudiantes

4.1 Requisitos de acceso y perfil de ingreso recomendado

Este máster está orientado a licenciados e ingenieros en áreas de conocimiento afines a las TIC. Sin embargo, de acuerdo con las respuestas de la mayor parte de los encuestados, debe abrirse también a profesionales de otras áreas de ciencias o ingenierías que, ya sea que cuenten con experiencia en el ámbito de las TIC o no, busquen un grado de especialización en ciberseguridad. En este último caso se han previsto asignaturas de nivelación para proporcionar los conocimientos tecnológicos básicos necesarios.

Los solicitantes que hayan obtenido un título en un área de conocimiento diferente deberían ser evaluados por el Comité de Dirección del Máster, con atención a las materias cursadas, la evidencia y los resultados fehacientes de sus capacidades y, en definitiva, al potencial de aprovechamiento de los estudios del máster.

5. Plan de estudios

El presente programa de máster está concebido para proporcionar a los estudiantes una capacitación científico-tecnológica avanzada en materia de ciberseguridad, abordando la disciplina desde una perspectiva integral. Esta concepción se articula mediante la provisión de nociones teóricas, que se acompañan de las herramientas y técnicas adecuadas para su puesta en práctica en un entorno real. El planteo de los contenidos incorpora las facetas de investigación y desarrollo, de modo que los estudiantes puedan no solo desarrollarse profesionalmente en dichas facetas, sino también emplearlas como forma de actualización y reciclaje permanente.

Las asignaturas se han propuesto, principalmente, sobre la base de las opiniones recibidas de los encuestados. Otros aspectos formativos, como el TFM o las prácticas en empresas, han concitado la aceptación por unanimidad de las universidades sondeadas.

5.1 Descripción general del plan de estudios y su planificación

El plan de estudios se organiza atendiendo a una doble dimensión:

- **Estructuración temporal.** El máster adopta

15 Véase Cybersecurity Curricular Guidance for Associate-Degree Programs, ACM (enero de 2020) en: http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf.

la división por periodos académicos cuatrimestrales, que podrán implantarse en la franja anual más conveniente en función de los procesos académicos de admisión de estudiantes de la institución ofertante. En este sentido, el máster consta de cuatro cuatrimestres, que habitualmente se imparten en dos cursos o años lectivos.

La duración más común de un cuatrimestre es de 15 semanas, más una u otras dos para la realización de los exámenes finales. Como la preferencia de los encuestados ha sido de 15 horas semanales (presenciales y a distancia), resultan 225 horas por cuatrimestre. Si se considera que en promedio cada hora de clase supone para el alumno otras 1,5 horas de estudio (o de realización de trabajos) resulta una carga semanal adicional de 22,5 horas, lo que totaliza 37,5 horas de dedicación al máster, cifra que supone una razonable carga de trabajo. En todo caso, como se verá, esta carga semanal varía ligeramente entre cuatrimestres.

- **Estructuración conceptual**. El máster se organiza en módulos, que agrupan una o más asignaturas relacionadas con una faceta de la ciberseguridad. Así, el programa se divide en cuatro módulos principales y uno de nivelación.

  A continuación, se presenta cada uno de los cinco módulos junto con la dedicación requerida en términos de tiempo. Si bien los dos primeros módulos (0 y 1) están conformados por materias obligatorias (el Módulo 0 es solo para alumnos con carencias de formación en TIC), el Módulo 2 se estructura en dos itinerarios de especialización diferentes, de modo que el estudiante puede escoger uno de ambos según sus intereses profesionales. A su vez, el Módulo 3 está constituido íntegramente por asignaturas elegibles que pueden ser escogidas libremente por los alumnos, con independencia del itinerario que hayan seguido en el módulo anterior. Incluso, si la universidad lo considerase oportuno, alumnos de una especialidad podrían escoger como elegibles asignaturas de la otra.

  Finalmente, el Módulo 4 se corresponde con la realización del TFM y las prácticas en una empresa, que servirán como punto de entrada al ámbito laboral.

  Una consideración importante es que la **ciberseguridad no** es una materia **completamente teórica** y, por tanto, **todas las asignaturas deben tener una parte práctica considerable** para complementar la teoría y así conseguir que los alumnos dominen y utilicen las herramientas habituales en el mundo de la ciberseguridad. Además, todas las prácticas realizadas en el máster, y especialmente aquellas en las que se pueda poner en riesgo un sistema, se deberían realizar en entornos virtualizados.

Módulo 0. Nivelación

Dado que numerosos encuestados han señalado sus preferencias por abrir el acceso al máster a cualquier candidato con estudios superiores, independientemente de la naturaleza de su titulación, sea esta técnica, científica u otra, se considera insoslayable brindar a estos estudiantes un módulo de nivelación (Módulo 0) que les dote de los conocimientos mínimos de las TIC, sin los cuales les sería imposible seguir con provecho el resto del máster.

Con este fin, el módulo se estructura en los tres apartados siguientes, que se juzgan como el mínimo imprescindible para el fin propuesto:

A) Arquitectura de sistemas informáticos

B) Fundamentos de redes de comunicaciones

C) Técnicas de programación

Ya que se ha considerado imposible que un alumno sin formación previa en estas materias sea capaz de formarse en ellas en menos de un cuatrimestre, se propone invertir en cada una de estas materias entre 60 y 70 horas de clase.

Módulo 1. Ciberseguridad general

En este módulo se proporcionan al alumno conocimientos sobre las materias de ciberseguridad que se consideran básicas para su formación, sea cual fuere la especialidad que posteriormente escojan y, por tanto, tienen carácter obligatorio.

A) Sistemas de ciberdefensa

B) Técnicas de ciberataque

C) Comunicaciones seguras

D) Criptografía aplicada

E) Explotación de sistemas *software*

F) Dirección y gestión de la seguridad

Para cada una de estas materias se ha considerado razonable dedicar entre 32 y 36 horas de clase.

Módulo 2. Especialización en ciberseguridad

Este módulo tiene dos posibles itinerarios especializados, de modo que el alumno ha de escoger el que se asocie más con sus preferencias.

Al igual que en el módulo anterior, se entiende que es razonable invertir entre 32 y 36 horas de clase para cada asignatura.

2.1 Ingeniería de Sistemas Seguros

Los alumnos que escojan este itinerario se formarán en aspectos relacionados con la especificación, el diseño y el desarrollo, la implantación y el mantenimiento de sistemas seguros. Las asignaturas que deberán cursar son las siguientes:

A) Desarrollo de sistemas seguros y seguridad DevOps

B) Análisis y gestión de riesgos en ciberseguridad

C) Seguridad en el tratamiento de datos masivos (*big data*)

D) Seguridad en la computación en la nube (*cloud computing*)

2.2 Analista de Ciberseguridad

En este itinerario los estudiantes se adiestrarán en el análisis de datos de ciberseguridad, para lo cual cursarán las siguientes asignaturas:

A) Análisis de *malware*

B) Amenazas persistentes avanzadas

C) Informática forense

D) Seguridad en dispositivos móviles

Módulo 3. Formación complementaria

Este módulo se dirige a complementar la formación ya recibida por los estudiantes con otras asignaturas, especializadas o no, que puedan interesar tanto a aquellos que hayan seguido el itinerario de Analista de Ciberseguridad como a los que hayan optado por el de Ingeniería de Sistemas Seguros. Para ello, se proponen las siguientes asignaturas, de las que el estudiante tendrá que escoger tres:

A) Seguridad en IoT

B) Seguridad en sistemas ciberfísicos

C) Marco legal de la ciberseguridad

D) Ciberdelitos, ciberterrorismo y ciberguerra

E) Autenticación y control de acceso

F) Técnicas de exfiltración de información

G) Inteligencia artificial para ciberseguridad

H) Ciberinteligencia

Para cada una de estas asignaturas se estima una dedicación de 23-25 horas de clase.

Parece razonable permitir que un alumno, en vez de optar por una o varias de las anteriores, elija una o varias del itinerario de especialización que no hubiere seleccionado previamente, aunque ello le suponga cursar más horas totales de las previstas para obtener el título de máster.

Además, se establecen un total de **ocho conferencias de carácter obligatorio**, que se impartirán en el último cuatrimestre, que es cuando más provecho puede obtenerse al haber adquirido ya los conocimientos de las asignaturas del máster.

Se pretende que estas conferencias sean impartidas por miembros externos, por ejemplo, trabajadores de empresas de ciberseguridad, funcionarios públicos expertos en ciberseguridad o miembros de las fuerzas y cuerpos de seguridad nacionales, que acerquen el mundo profesional a los alumnos y les ofrezcan distintos puntos de vista sobre algunos de los retos existentes en su país. Así, estas conferencias no han de estar asociadas a materias concretas, sino que permitirán que los ponentes expongan sus experiencias profesionales en distintos entornos empresariales y públicos en los que la ciberseguridad desempeña un papel relevante.

La experiencia demuestra que el tiempo razonable para cada conferencia es de 1,5 horas, lo que totaliza 12 horas.

Módulo 4. Trabajo final y prácticum

Este módulo, de carácter obligatorio, se corresponde con la realización del TFM y de las prácticas (prácticum) en una empresa del sector de la ciberseguridad o de cualquier otro sector que tenga un departamento de ciberseguridad. El TFM se puede llevar a cabo dentro de la firma en la que se realice el prácticum, así como considerando las actividades que allí se efectúen. Además, el prácticum será supervisado de manera conjunta entre docentes y profesionales de la empresa.

De acuerdo con los módulos establecidos, el máster tendrá una duración de dos años. En el **cuadro 6** se puede apreciar la **planificación** del mismo. Nótese que es importante que todos los alumnos dispongan de los conocimientos indicados en el Módulo 0, pero cada universidad puede localizar este módulo en el periodo que considere oportuno; por ejemplo, puede estar abierto durante determinados meses al año para la formación de los futuros alumnos del máster.

Cuadro 6. Planificación temporal del máster

Año 1	
1er cuatrimestre	2º cuatrimestre
Módulo 0	Módulo 1
Año 2	
1er cuatrimestre	2º cuatrimestre
Módulo 2 Módulo 3	Módulo 4 Conferencias

5.2 Actividades formativas, asignaturas que se impartirán, descripción del objetivo y contenidos

5.2.1 Contenido de las asignaturas a impartir

Módulo 0. Nivelación

Como se ha indicado anteriormente, este módulo está compuesto por asignaturas **obligatorias** para los **alumnos** que **no** tengan las **competencias iniciales** necesarias.

A) Arquitectura de sistemas informáticos

Comprender cómo funcionan los ordenadores es esencial para posteriormente ser capaz de detectar posibles problemas. En esta asignatura se introducen los principios del diseño de ordenadores, para que los alumnos conozcan los conceptos básicos sobre los tipos de arquitecturas existentes y el impacto que pueden tener en el rendimiento. Asimismo, se describirán los principales tipos de memoria y procesadores. En concreto, el contenido de esta asignatura es el siguiente:

1) Fundamentos del diseño de computadores
   - 1.1 Estructura básica de un ordenador
   - 1.2 Rendimiento
   - 1.3 Tipos de arquitecturas

2) Sistema de memoria
   - 2.1 Memoria cache
   - 2.2 Memoria principal
   - 2.3 Memoria virtual

3) Funcionamiento de los procesadores
   - 3.1 Procesadores ILP
   - 3.2 Multiprocesadores

4) Lenguaje ensamblador

B) Fundamentos de redes de comunicaciones

Comprender la estructura y el funcionamiento de los ordenadores es un paso previo para estudiar las medidas de protección. En esta asignatura se comienza por presentar los modelos básicos utilizados en las redes de ordenadores, para ir profundizando posteriormente en los distintos niveles que los componen. Así, se llegará a comprender qué ocurre en un ordenador desde que un mensaje se crea hasta que es recibido por el destinatario. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción a las redes de ordenadores
   - 1.1 Modelo de capas OSI (*Open System Interconnection*)
   - 1.2 Modelo de referencia TCP/IP (Internet).

2) Técnicas de transmisión

3) Nivel físico

4) Nivel de enlace
   - 4.1 Direccionamiento
   - 4.2 Tecnologías y dispositivos

5) Nivel de red
   - 5.1 Protocolo IP

6) Nivel de transporte
   - 6.1 Protocolo TCP
   - 6.2 Protocolo UCP

7) Nivel de aplicación
   - 7.1 Protocolos asociados a la transferencia y compartición de ficheros
   - 7.2 Protocolos asociados al correo electrónico
   - 7.3 Protocolos asociados a la navegación web

C) Técnicas de programación

Comprender el desarrollo de programas es necesario para posteriormente identificar los ataques a los mismos o los errores generados. En esta asignatura se estudiarán distintos tipos de técnicas de programación, se analizará cómo se desarrolla un programa, junto con las herramientas necesarias, y se introducirán las bases de la programación en lenguajes de alto y bajo nivel. En particular, el contenido es el siguiente:

1) Tipos de técnicas de programación

- 1.1 Programación estructurada
- 1.2 Programación modular
- 1.3 Programación orientada a objetos
- 1.4 Programación concurrente
- 1.5 Programación funcional
- 1.6 Programación lógica

2) Desarrollo de programas

- 2.1 Compilación
- 2.2 Herramientas de desarrollo

3) Lenguajes de programación

- 3.1 C
- 3.2 Java
- 3.3 Python

Módulo 1. Ciberseguridad general

Este módulo trata de los fundamentos técnicos de la ciberseguridad que constituyen la base de cualquier especialización ulterior de este campo. Para ello, se incluyen las siguientes asignaturas **obligatorias**.

A) Sistemas de ciberdefensa

Comprender los distintos lugares en los que es posible realizar ataques es un requisito necesario para mitigarlos, detectarlos o prevenirlos. En esta asignatura, además de introducir el concepto de ciberdefensa, se presentan los diversos mecanismos que se emplean en esta área, como los cortafuegos, los sistemas de detección de intrusiones (IDS) y los sistemas de gestión de eventos y seguridad de la información. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción a los sistemas de ciberdefensa

2) Sensores locales: auditoría y análisis de eventos

- 2.1 Gestión de usuarios y accesos
- 2.2 Análisis de registros (logs) de seguridad

3) Cortafuegos y segmentación de redes

- 3.1 Fundamentos de filtrado de tráfico
- 3.2 Tipos de cortafuegos
- 3.3 Segmentación de redes

4) Sistemas de detección y prevención de ataques

- 4.1 Detección de firmas de ataque
- 4.2 Detección de anomalías
- 4.3 Respuesta automática a intentos de intrusión

5) Sistemas de gestión de eventos e información de seguridad (SIEM)

- 5.1 Conceptos y arquitecturas de SIEM
- 5.2 Reglas de agregación y correlación
- 5.3 Arquitecturas distribuidas de sensores de detección
- 5.4 Estrategias de sensorización de redes

B) Técnicas de ciberataque

Comprender los procedimientos por los que se pueden llevar a cabo ciberataques es una parte esencial de la ciberseguridad. La asignatura apunta a que los alumnos se familiaricen con los fundamentos y las posibilidades de realización de los ciberataques. Para ello, se enseñan las distintas técnicas que se utilizan para atacar los sistemas, comenzando por una fase de reconocimiento hasta llegar a conseguir controlar un sistema, o provocar fugas de datos y eliminar los rastros que se puedan dejar. En detalle, el contenido de esta asignatura es el siguiente:

1) Introducción a las técnicas de ciberataque

- 1.1 Conceptos y definiciones
- 1.2 Tipos de ciberataques
- 1.3 Fases típicas de una intrusión

2) Adquisición de información del objetivo y análisis de vulnerabilidades

- 2.1 Técnicas de reconocimiento: fuentes abiertas
- 2.2 Enumeración de redes y escaneo de servicios
- 2.3 Identificación y análisis de vulnerabilidades

3) Explotación

- 3.1 Explotación de sistemas de autenticación y explotación de *software*
- 3.2 Consumo de recursos y DoS
- 3.3 Ingeniería social, *malware* y técnicas de evasión

4) Persistencia

- 4.1 Eliminación de evidencias
- 4.2 Escalado de privilegios
- 4.3 Establecimiento de canales de acceso alternativos
- 4.4 Ocultación de presencia

C) Comunicaciones seguras

Comprender los protocolos de comunicación y los aspectos de seguridad de cada uno de ellos es fundamental para otorgar seguridad a las comunicaciones. En esta asignatura se exponen los protocolos seguros utilizados en las redes de comunicación y todo lo que su seguridad conlleva, desde los ataques que se pueden contrarrestar hasta las medidas de defensa que es posible establecer. En detalle, el contenido es el que sigue:

1) Principios de seguridad de redes de comunicaciones

- 1.1 Definiciones y conceptos. Servicios de seguridad vs. mecanismos de seguridad
- 1.2 Ataques más comunes a las redes de comunicaciones
- 1.3 Contramedidas. Costes de la seguridad.

2) Seguridad en el nivel físico y de enlace. Ataques y defensas

- 2.1 Redes Ethernet. Ataques y defensas
- 2.2 Los protocolos PPP y EAP. Autenticación, Autorización y Contabilidad (AAA)
- 2.3 Seguridad en redes inalámbricas

3) Seguridad en el nivel de red

- 3.1 Seguridad en IPv4 e IPv6
- 3.2 Protocolos auxiliares (ICMP, DHCP). Ataques y defensas
- 3.3 Protocolos de encaminamiento. Ataques y defensas
- 3.4 IPsec

4) Seguridad en el nivel de transporte

- 4.1 TLS/SSL

4.2 Redes privadas virtuales (VPN)

5) Seguridad en el nivel de aplicación

5.1 Seguridad en DNS
5.2 Seguridad en aplicaciones ofimáticas: navegación web y correo electrónico
5.3 Seguridad en otras aplicaciones: control y ejecución remota, transferencia y compartición de ficheros.

D) Criptografía aplicada

Comprender las principales medidas para proporcionar seguridad a los datos, en concreto mediante el uso de la criptografía, es un requisito imprescindible en la protección de sistemas y redes. En esta asignatura se definirán los principales tipos y algoritmos criptográficos existentes, así como algoritmos para asegurar la procedencia de los datos, considerando la autenticación y la firma digital. Además, la protección de los datos también requiere conocer si se han modificado y hasta qué punto los datos se ven afectados por ello, para lo cual se deben introducir el concepto y el uso de funciones resumen. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción

1.1 Introducción a la protección de la información: definiciones, dimensiones de la seguridad de la información
1.2 Clasificación de los sistemas de cifrado (simétrico/asimétrico)

2) Cifrado

2.1 Cifradores de bloque y de flujo
2.2 Algoritmos de cifrado: simétricos y asimétricos
2.3 Gestión de claves criptográficas
2.4 Cifrado con curvas elípticas
2.5 Otros mecanismos de cifrado
2.6 Implementaciones. Librerías criptográficas

3) Autenticación de mensajes y entidades

3.1 Funciones hash criptográficas y códigos de autenticación de mensajes (MAC)
3.2 Firma digital. Estándares
3.3 Certificados digitales e infraestructuras de clave pública (PKI)

E) Explotación de sistemas de *software*

Comprender las principales vulnerabilidades de los sistemas, facilita su explotación. En esta asignatura se presentan las principales vulnerabilidades y contramedidas establecidas en tres niveles: de *software*, de red y de web, para cada uno de los cuales se exponen algunas de las vulnerabilidades técnicas más conocidas, junto con los mecanismos para su prevención. Finalmente, en el último apartado se trata la importancia de los repositorios de vulnerabilidades y los lenguajes de intercambio de vulnerabilidades y ataques. A continuación, se indican los temas específicamente alcanzados en esta materia:

1) Introducción

1.1 Vulnerabilidades en componentes *software*
1.2 Mecanismos de explotación
1.3 Herramientas y laboratorio de análisis y síntesis

2) Explotación de vulnerabilidades en el *software*

2.1 Violaciones de memoria
2.2 Condiciones de carrera
2.3 Confusión de privilegios
2.4 Explotación de la interfaz de usuario

3) Explotación de sistemas web

3.1 Vulnerabilidades en el canal
3.2 Vulnerabilidades en el servidor
3.3 Vulnerabilidades en el navegador

4) Información sobre vulnerabilidades y formas de explotación

4.1 Repositorios
4.2 Lenguajes y estándares de representación e intercambio

F) Dirección y gestión de la seguridad

Comprender los procedimientos y normas relacionadas con la gestión de la seguridad de la información es un requisito necesario, pues hoy en día una seguridad basada exclusivamente en consideraciones técnicas es una entelequia. La asignatura permite conocer las normas y marcos de gestión referentes a los sistemas de la información, profundizando en aspectos de formación y concienciación, planes de continuidad, etc. Además, también contempla la auditoría de la seguridad, lo que permite a los alumnos realizar un control y un análisis sistemático de los sistemas. Asimismo, en esta asignatura tendría cabida la Estrategia Nacional de Ciberseguridad, si existe, que suele ser el marco de gestión de la ciberseguridad a nivel estatal en los países que cuenten con ella. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción

1.1 Normalización, evaluación, certificación y acreditación. Instituciones y procesos
1.2 Marco legal

2) Dirección y planeamiento

2.1 Planes de seguridad
2.2 Formación y concienciación
2.3 Clasificación de la información
2.4 Planes de continuidad del negocio
2.5 Centros de respuesta a incidentes (CERT, CSIRT) y de operaciones de seguridad (SOC)

3) Gestión de la seguridad

3.1 COBIT (Control Objectives for Information and Related Technology)
3.2 NIST Cybersecurity Framework & Serie SP 800
3.3 Familia de normas ISO/IEC 27000

4) Auditoría de la seguridad

4.1 Marcos y estándares.
4.2 Auditoría de datos personales
4.3 Evidencias y su análisis
4.4 El informe de auditoría

5) Estrategia Nacional de Ciberseguridad

Módulo 2. Especialización en ciberseguridad

Este módulo (que en realidad abarca dos) se propone especializar al alumno en una de las dos áreas principales que comprende la ciberseguridad. Para ello, como ya se había señalado previamente, se han establecido dos itinerarios: el de la Ingeniería de Sistemas Seguros y el de Analista en Ciberseguridad. El alumno ha de escoger la vía que considere más alineada con sus intereses.

2.1 Ingeniería de Sistemas Seguros

A) Desarrollo de sistemas seguros y seguridad DevOps

Comprender cómo desarrollar un sistema adecuadamente, considerando la seguridad en todo el proceso, puede ser complejo y tedioso, pero fundamental para intentar minimizar el número de posibles ataques que pueda sufrir. Para ello, en

esta asignatura se tratan los principales modelos, arquitecturas y mecanismos para el diseño seguro de *software*. Además, un término que está atrayendo la atención de los expertos es DevOps (*Development Operations*), asociado con metodologías ágiles de desarrollo de código y de gran uso en la actualidad. Sin embargo, en esta asignatura no se hace tanto énfasis en DevOps en tanto metodología o paradigma de desarrollo de *software*, sino en los aspectos de seguridad vinculados. En concreto, el temario propuesto es el siguiente:

1) Conceptos de ingeniería de sistemas seguros

- 1.1 Propiedades de seguridad
- 1.2 Principios de diseño para la seguridad
- 1.3 Arquitecturas *software*

2) Requisitos de *software* seguro

- 2.1 Descomposición de políticas
- 2.2 Tipos de requisitos

3) Diseño de *software* seguro

- 3.1 Procesos de diseño
- 3.2 Consideraciones de diseño
- 3.3 Seguridad de la arquitectura
- 3.4 Tecnologías

4) Seguridad en la implementación

- 4.1 Seguridad de los lenguajes de programación
- 4.2 Bases de datos de vulnerabilidades
- 4.3 Prácticas y controles defensivos
- 4.4 Código fuente. Versiones
- 4.5 Entornos de desarrollo
- 4.6 Revisión y análisis de código
- 4.7 Técnicas anti-manipulación de código

5) Pruebas

- 5.1 Estrategias, planes y casos de prueba
- 5.2 Tipos de pruebas
- 5.3 Evaluación de impacto y acciones correctivas
- 5.4 Gestión del ciclo de vida de los datos de prueba

6) Seguridad en DevOps (DevSecOps)

- 6.1 Concepto
- 6.2 Integración de ciberseguridad en cada fase del proceso

B) Análisis y gestión de riesgos en ciberseguridad

Comprender los riesgos que se ciernen sobre un sistema, los cuales hay que identificar y estimar (analizar) para después decidir si conviene aceptarlos, mitigarlos o rechazarlos, según el caso, y concluir con el tratamiento adecuado de los mitigados, es un proceso que se conoce con el nombre de gestión de riesgos. En esta asignatura se describe el proceso que se debe llevar a cabo para realizar un análisis de riesgos en una organización, identificando todos los activos, valorándolos y determinando el riesgo asociado, para acabar con la elección del tratamiento adecuado para los riesgos no retenidos ni rechazados.

Para ello, se presentarán distintas metodologías de análisis y gestión de riesgos y se mostrarán aplicaciones en varios entornos, como el del IoT o los dispositivos móviles. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción y conceptos generales de análisis de riesgos

- 1.1 Conceptos: activos, amenazas, vulnerabilidades, salvaguardas, etc.
- 1.2 Análisis cualitativo y cuantitativo
- 1.3 Análisis estático y dinámico

2) Metodologías de análisis y gestión de riesgos

2.1 ISACA (COSO), CRAMM, EBIOS, PCI-DSS, NIST SP-800, etc.
2.2 ISO-27005. MAGERIT

3) Análisis de riesgos en entornos actuales y futuros de aplicación

3.1 *Cloud computing*
3.2 *Big data*. Inteligencia artificial
3.3 Internet de las cosas (IoT)

C) Entornos móviles (*wireless, smartphones*, etc.). Seguridad en el tratamiento de datos masivos (*big data*)

Comprender cómo realizar la gestión de grandes cantidades de datos (*big data*) se está convirtiendo en una práctica habitual en multitud de empresas e instituciones. En el mundo de la ciberseguridad, el *big data* ofrece una doble vertiente. Por un lado, el empleo de grandes volúmenes de datos se ha convertido en una herramienta valiosa para identificar y contrarrestar los ataques en tiempo real. Por otro, las empresas usan cada vez más el *big data* para sus procesos de negocios. Por ello, tras realizar una introducción al nexo entre datos masivos y ciberseguridad, en esta asignatura se presentan mecanismos para gestionar y visualizar de forma segura estos datos masivos. Dentro de la gestión de datos se hace énfasis en el análisis de logs y los sistemas de gestión de eventos e información de seguridad que, si bien se presentan en otra asignatura de carácter obligatorio, son esenciales en este ámbito. Además, se introduce la relevancia de la privacidad en esta área, junto con las técnicas que se pueden utilizar para protegerla, y los aspectos legales involucrados en el ámbito del procesado masivo de datos. Específicamente, el programa de esta asignatura abarcaría lo siguiente:

1) Introducción a ciberseguridad en *big data*

1.1 Conceptos básicos
1.2 Retos
1.3 Fuentes de datos
1.4 Aplicaciones de ciberseguridad y *big data*

2) Análisis de datos de ciberseguridad

2.1 Principales técnicas de análisis de datos
2.2 Cómo analizar datos de forma segura
2.3 Técnicas de visualización
2.4 Cuadros de mando

3) Almacenamiento seguro de datos

3.1 Bases de datos enfocadas en seguridad
3.2 Gestión y administración segura de bases de datos

4) Preservación de la privacidad

4.1 Los problemas de la privacidad
4.2 Técnicas de protección de privacidad
4.3 Aspectos legales en *big data*

D) Seguridad en la computación en la nube (*cloud computing*)

Comprender las capacidades que ofrece la nube (*cloud*) para facilitar capacidad de cómputo y almacenamiento es fundamental para el uso y la gestión de muchos sistemas. En este escenario se presentan nuevos retos de seguridad a los que hay que hacer frente. En esta asignatura se exponen los fundamentos del *cloud computing* y sus repercusiones en el ámbito de la ciberseguridad, y se identifican los riesgos y amenazas existentes, así como las técnicas de protección de las infraestructuras de *cloud computing* y las capacidades de gestión de incidentes en este entorno. En concreto, en temario

de la asignatura será como sigue:

1) Fundamentos del *cloud computing*

   1.1 Definición
   1.2 Sistemas y modelos de computación en la nube
   1.3 Retos de seguridad

2) Riesgos y amenazas específicas

   2.1 Externalización. Proveedores de servicios gestionados
   2.2 Compartición de infraestructuras
   2.3 Trazabilidad de la información

3) Técnicas para aseguramiento

   3.1 Contenedores (dockers)
   3.2 Virtualización
   3.3 Balanceadores de carga

2.2 Analista de Ciberseguridad

A) Análisis de *malware*

Comprender la multitud de programas malignos (*malware*) y su tendencia en cantidad y variedad es necesario para saber enfrentarlos. En esta asignatura se contemplan los distintos tipos de *malware* existentes, exponiendo sus comportamientos y las técnicas con que se cuenta para su análisis, tanto básicas como avanzadas, las cuales, aunque requieren conocimientos técnicos superiores, son ineludibles en la identificación de algunos tipos de *malware* y sus características. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción

   1.1 Conceptos básicos y evolución
   1.2 Técnicas de análisis de *malware*

2) Técnicas básicas de análisis

   2.1 Análisis estático básico
   2.2 Análisis dinámico básico

3) Técnicas avanzadas de análisis

   3.1 Desensamblado x86
   3.2 Depuradores. IDA Pro
   3.3 La API de Windows

4) Comportamientos y técnicas de evasión

   4.1 Cargadores
   4.2 Puertas traseras
   4.3 Espías
   4.4 Persistencia
   4.5 Ejecución encubierta
   4.6 Codificación
   4.7 Anti-desensamblado
   4.8 Anti-depurado
   4.9 Anti-virtualización
   4.10 Packers

B) Amenazas persistentes avanzadas

Comprender qué son y cómo funcionan un conjunto concreto de amenazas, que se caracterizan por estar diseñadas para perpetuarse en los equipos que infectan y se denominan amenazas persistentes avanzadas (*Advanced Persistent Threat*, APT), es necesario para tener una visión holística de las amenazas actuales. Las APT aparecieron por primera vez en 2010 y desde entonces se han identificado gran multitud de ellas, las cuales afectan en su mayor parte equipos de gran criticidad como los que soportan las infraestructuras críticas. Se caracterizan por utilizar un conjunto muy amplio de técnicas para realizar ataques y por su sigilosidad y persistencia, rasgos que dificultan mucho su identificación. En esta asignatura los alumnos adquirirán conocimientos sobre las características de las APT, los principales

mecanismos que utilizan y sus familias más conocidas. En concreto, el contenido sería el que a continuación se reseña:

1) Introducción

1.1 Caracterización de las APT
1.2 Comparación con otros programas malignos

2) Estrategias de comando y control

2.1 Arquitecturas
2.2 Sigilo
2.3 Anonimato
2.4 Resiliencia

3) Técnicas de evasión y persistencia

3.1 Ocultación de actividad. Rootkits
3.2 Persistencia sin uso de disco (*data-only*)
3.3 Ataques de mimetización

4) Panorama actual

4.1 Casos de estudio
4.2 Principales actores y capacidades
4.3 Tendencias

C) Informática forense

Comprender en qué momento se ha producido algún tipo de ataque o incidente de seguridad puede ser necesario para identificar su procedencia, lo cual marca el momento de aplicar la denominada informática forense. En esta asignatura el alumno aprenderá las bases del análisis forense tanto en sistemas como en dispositivos móviles, y conocerá distintos tipos de herramientas de análisis forense y los procedimientos y políticas que se han de aplicar. Particularmente, el contenido de esta asignatura es el siguiente:

1) Introducción al análisis forense

1.1 Conceptos básicos
1.2 Casos de ejemplo
1.3 Conceptos técnicos clave

2) Laboratorio de análisis forense

2.1 Políticas y procedimientos
2.2 Garantía de la calidad
2.3 Herramientas
2.4 Evidencias: obtención, análisis y custodia
2.5 Informe forense

3) Herramientas de análisis forense

3.1 Análisis forense de sistemas de ficheros
3.2 Análisis forense de memoria
3.3 Análisis forense en redes de ordenadores
3.4 Internet y correo electrónico
3.5 Análisis forense en dispositivos móviles
3.6 Herramientas y técnicas antiforenses

D) Seguridad en dispositivos móviles

Comprender cómo se protegen los dispositivos móviles es imprescindible, ya que se están utilizando cada vez de forma más masiva. En esta asignatura se presentan las bases de las comunicaciones celulares atendiendo a su seguridad, por ejemplo, introduciendo los problemas de la seguridad en WiFi. Seguidamente, se describirán distintos aspectos sobre la seguridad en los sistemas operativos Android y iOS, por ser los dos más utilizados en dispositivos móviles. Finalmente, se presentarán las novedades sobre las amenazas que sufren este tipo de dispositivos. En concreto, el contenido de esta asignatura es el siguiente:

1) Comunicaciones móviles

1.1 Introducción a las comunicaciones móviles

1.2 Seguridad en comunicaciones inalámbricas

2) Seguridad en Android

2.1 Arquitectura Android
2.2 Modelo de seguridad
2.3 Tipos de aplicaciones Android
2.4 OWASP Mobile Security Testing
2.5 Ingeniería Inversa

3) Seguridad en iOS

3.1 Arquitectura iOS
3.2 Modelo de seguridad
3.3 Auditoría de aplicaciones iOS

4) Aplicaciones móviles maliciosas

4.1 Técnicas de análisis: estáticas y dinámicas
4.2 Ingeniería inversa
4.3 Tendencias

Módulo 3. Formación complementaria

Para que los alumnos continúen su formación en ciberseguridad y a la vez puedan ampliar su conocimiento en otras materias especializadas, pero más horizontales, tendrán que escoger tres asignaturas elegibles de entre las siguientes:

A) Seguridad en Internet de las cosas (IoT)

Comprender los dispositivos que nos rodean y la capacidad de conexión de que disponen para conectarse entre sí y a Internet para compartir información pone de manifiesto múltiples problemas de seguridad. Estos dispositivos, y los medios mediante los que se interconectan, reciben el nombre de IoT y están expuestos a distintos ataques y vulnerabilidades. En esta asignatura se presentan los dispositivos IoT, la seguridad en las distintas arquitecturas y protocolos, y aspectos de seguridad asociados a dispositivos concretos, como los dispositivos médicos, las cámaras de vigilancia o los dispositivos inteligentes de los hogares. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción al Internet de las cosas (IoT)

1.1 Definición de IoT
1.2 Dispositivos IoT. Evolución

2) Arquitecturas y protocolos utilizados en IoT

2.1 Descripción
2.2 Problemas de seguridad
2.3 Medidas de protección

3) Seguridad en dispositivos IoT

3.1 Tendencias
3.2 Dispositivos médicos
3.3 Cámaras de vigilancia
3.4 Dispositivos inteligentes de los hogares
3.5 Otros

B) Seguridad en sistemas ciberfísicos

Comprender los riesgos y amenazas de los sistemas ciberfísicos, aquellos cuyo diseño y funcionamiento se basa en la interacción de sistemas mecánicos y tecnologías de la comunicación, posibilita su adecuada monitorización y control, ya sea de manera física o remota. Ejemplos de este tipo de sistemas son las plataformas embarcadas en robots, sensores y actuadores, e incluso combinaciones de las mismas como los vehículos o los sistemas industriales. En esta asignatura se realiza una introducción a estos sistemas ciberfísicos, para posteriormente tratar las arquitecturas de referencia de estos sistemas y finalmente definir las amenazas concretas a las que se exponen. En concreto, el contenido de la asignatura es el siguiente:

1) Introducción a los sistemas ciberfísicos

   1.1 Definición
   1.2 Principales sistemas ciberfísicos. Aplicaciones

2) Arquitecturas de referencia en los sistemas ciberfísicos

   2.1 Sistemas industriales
   2.2 Sistemas embebidos

3) Amenazas específicas

   3.1 Riesgos y ataques
   3.2 Contramedidas
   3.3 Tendencias

C) Marco legal de la ciberseguridad

Comprender los aspectos legales de la ciberseguridad ayuda a disponer de una visión global, no exclusivamente técnica, de esta disciplina. Además, estos aspectos técnicos están íntimamente vinculados con las previsiones legales de los distintos países. Así, el conocimiento de los aspectos legales de la protección de datos personales es de gran utilidad en el desarrollo de programas, el conocimiento de la validez legal de la firma digital (o electrónica y sus distintas modalidades) y se torna necesario a la hora de planificar defensas frente a ciberataques o ilícitos penales, como los delitos informáticos, para algunos sistemas de respuesta a incidentes. También cabría aquí tratar la regulación legal (en los países que la contemplan) de la seguridad de los sistemas y redes.

En concreto, el contenido de esta asignatura es el siguiente:

1) Normativa legal sobre protección de datos personales

2) El delito informático. Convenio de Budapest sobre ciberdelincuencia

3) Aspectos legales de la firma digital

4) La regulación legal de la seguridad en redes y sistemas de información

5) Ley de protección de infraestructuras críticas

D) Ciberdelitos, ciberterrorismo y ciberguerra

Comprender los distintos tipos de amenazas existentes, en sus múltiples formas y en base a los objetivos que se desea alcanzar, ayuda a comprender sus orígenes. En esta asignatura se realiza una introducción a las ciberamenazas, identificándose distintos tipos de ciberataques como los citados, y a continuación se enfocan sus características y el modus operandi de cada uno, ejemplificando todo ello con múltiples casos reales. Así, el temario de esta asignatura queda como a continuación se indica:

1) Introducción, definiciones y conceptos básicos

   1.1 Orígenes
   1.2 Ciberataques
   1.3 Economía sumergida
   1.4 Tendencias
   1.5 Impacto económico, financiero y social de los ciberataques
   1.6 Identificación y perfilado de ciberdelincuentes

2) Ciberataques y ciberactivismo

   2.1 Tipos de ciberataques
   2.2 Ciberdelitos
   2.3 Ciberespionaje
   2.4 Análisis de casos prácticos
   2.5 Aspectos legales

3) Ciberterrorismo y ciberoperaciones contra infraestructuras críticas

- 3.1 Infraestructuras críticas: interconexión y vulnerabilidades
- 3.2 Sistemas de control industrial
- 3.3 Otras infraestructuras críticas
- 3.4 Análisis de casos prácticos

4) Ciberguerra

- 4.1 Ciberarmamento: instrumentos lógicos, físicos y psicológicos
- 4.2 Ciberdoctrina (Manual de Tallín)
- 4.3 Estrategias de desinformación
- 4.4 Análisis de casos prácticos

E) Autenticación y control de acceso

Comprender cómo los usuarios y los sistemas gestionan quién tiene acceso a qué se conoce como control de acceso y es de vital importancia en todos los sistemas. Asimismo, para poder gestionar el acceso, los usuarios o las entidades tienen que autenticarse en primer lugar. En esta asignatura se presentan los modelos y mecanismos de autenticación y control de acceso, tanto a nivel de red como de usuario, junto con sus tecnologías y aplicaciones. En concreto, el contenido de esta asignatura es el siguiente:

1) Autenticación

- 1.1 Fundamentos de las técnicas de autenticación
- 1.2 Contraseñas
- 1.3 Reto-respuesta
- 1.4 Biometría
- 1.5 Autenticación multifactor
- 1.6 Usabilidad
- 1.7 Sistemas de identidad federada
- 1.7 Confianza digital

2) Control de acceso discrecional

- 2.1 La matriz de control de acceso
- 2.2 Transiciones y estados seguros
- 2.3 Políticas de seguridad

3) Control de acceso obligatorio

- 3.1 Fundamentos
- 3.2 Confidencialidad: Bell-La Padula
- 3.3 Integridad: Biba
- 3.4 Modelos híbridos: la muralla china y Clark-Wilson
- 3.5 Control de acceso basado en roles (RBAC)

4) Mecanismos de control de acceso

- 4.1 Listas de control de acceso
- 4.2 Capacidades
- 4.3 Implementación en sistemas operativos

F) Técnicas de exfiltración de datos

Comprender las técnicas utilizadas para exfiltrar datos sensibles, como los personales, ayuda a conocer uno de los objetivos, cada vez más habituales, de los atacantes. Así, las fugas de información (*data leaks*), ya sea que se produzcan por error u omisión o de manera intencionada, constituyen uno de los eventos de seguridad más críticos en los entornos corporativos modernos. Con el fin de familiarizarse con esta temática, en la asignatura se abordan tanto las técnicas para lograr el robo de datos como los mecanismos para su detección. En concreto, el contenido es el siguiente:

1) Introducción

- 1.1 Almacenamiento y replicación
- 1.2 Tendencias
- 1.3 Aspectos legales

2) Sistemas de protección

2.1 Técnicas de marcado
2.2 Herramientas de monitorización
2.3 Sistemas de prevención. Soluciones DLP (*data leakage prevention*)

3) Técnicas de exfiltración

3.1 Esteganografía clásica
3.2 Esteganografía moderna
3.3 Uso de medios no convencionales
3.4 Canales laterales
3.5 Detección. Esteganálisis y caracterización matemática

G) Inteligencia artificial para ciberseguridad

Comprender las técnicas y los algoritmos de inteligencia artificial (IA) más usados en ciberseguridad, así como su aplicación en este contexto resulta fundamental. La IA se está utilizando en un sinfín de áreas y también puede disponerse de ella en ciberseguridad. En esta asignatura se presentarán las áreas de la ciberseguridad en las que se puede aplicar la IA, así como los algoritmos y las herramientas más apropiadas para cada caso. Se trabajará especialmente en la detección de ciberataques y en la autenticación de usuarios, por su creciente interés. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción

1.1 Definición de inteligencia artificial
1.2 Algoritmos de inteligencia artificial
1.3 Usos de la inteligencia artificial en ciberseguridad
1.4 Ingeniería de características (*feature engineering*)
1.5 Explicabilidad (*explainability*)

2) Uso de la inteligencia artificial para la detección de ataques

2.1 Patrones
2.2 Algoritmos
2.3 Herramientas

3) Uso de la inteligencia artificial para autenticación

3.1 Patrones
3.2 Algoritmos
3.3 Herramientas

H) Ciberinteligencia

El objetivo en este caso es comprender las técnicas y herramientas más utilizadas en ciberinteligencia. Existe gran cantidad de recursos de los que es posible obtener información, pero se debe aprender a adquirirla y a analizarla. Para ello, luego de una introducción, en esta asignatura se definen e identifican los tipos más comunes de ciberinteligencia, a saber: inteligencia de fuentes humanas, de fuentes abiertas, de fuentes privadas y de señales, y también se presentan las herramientas más utilizadas en cada caso, así como los posibles casos de uso. En concreto, el contenido de esta asignatura es el siguiente:

1) Introducción

1.1 Historia de la ciberinteligencia
1.2 Usos de la ciberinteligencia
1.3 Usos de la inteligencia artificial en ciberseguridad

2) Inteligencia de fuentes humanas (HUMINT)

2.1 Definición
2.2 Herramientas
2.3 Casos de uso

3) Inteligencia de fuentes abiertas (OSINT)

3.1 Definición
3.2 Herramientas
3.3 Casos de uso

4) Inteligencia de fuentes privadas (PRIVINT)

4.1 Definición
4.2 Herramientas
4.3 Casos de uso

5) Inteligencia de señales (SIGINT)

5.1 Definición
5.2 Herramientas
5.3 Casos de uso

i) Conferencias

En este módulo se plantea contar con un total de ocho conferencias a impartir en el último cuatrimestre del segundo año, de una duración de entre 1 hora y 1,5 horas. Los ponentes deben ser expertos en distintas áreas de la ciberseguridad y presentar a los alumnos su conocimiento concreto de un tema partiendo de su experiencia profesional. Con esto se pretende establecer vínculos entre la academia y la industria, para que los alumnos conozcan las problemáticas y situaciones reales a las que se enfrentarán durante su vida laboral. Aquí se propone un listado meramente orientativo de posibles temáticas:

- Cómo crear un APT desde cero
- Control y mitigación de riesgos en las infraestructuras críticas
- Auditoría de seguridad de un sistema
- La persecución del delito informático
- Experiencias de un CISO
- El funcionamiento de un CERT o CSIRT
- La gestión y organización de la ciberseguridad en el Estado (organismos competentes, misiones, estructura, etc.)
- La mente de un *hacker*
- El derecho en la ciberseguridad
- Sistemas de formación en ciberseguridad
- Seguridad física en entornos informáticos
- Analizando *malware* avanzado
- Sistemas de protección de datos en una organización
- Criptomonedas: un arma de doble filo
- El peligro de los *data brokers*
- La evaluación de un producto para certificarlo frente a la norma ISO/IEC 15 408
- Cuestiones éticas subyacentes de la ciberseguridad

Módulo 4. Trabajo de fin de máster y prácticum

El TFM constituye un proyecto académico con una carga de trabajo de 240 horas de dedicación. El objetivo del trabajo es demostrar la adquisición de una o, preferiblemente, varias de las competencias adquiridas a lo largo del máster. Para ello, se puede realizar un proyecto académico asociado a la ciberseguridad y, en concreto, alineado con algunas de las asignaturas impartidas; también hay prácticas de tres meses de duración en una empresa propiamente de ciberseguridad o en un departamento de ciberseguridad. El alumno deberá confeccionar un documento que describa el proyecto realizado.

El TFM deberá ser defendido oralmente ante un tribunal evaluador, cuya composición y organización quedará definida por la institución ofertante. En cualquier caso, los miembros del tribunal deberán ser expertos académicos en el área de ciberseguridad, y se incorporará algún miembro de instituciones académicas ajenas. También podrá formar parte del tribunal algún representante del sector industrial de reconocido prestigio, siempre que se asegure que la mayoría de los miembros están vinculados a una institución académica. Con el fin de calificar los trabajos de forma homogénea, se propone el uso de una matriz de evaluación, en

Cuadro 7. Matriz de evaluación del trabajo de fin de máster

		Muy bien (4)	Bien (3)	Regular (2)	Mal (1)
Memoria	Organización y estructura				
	Planteamiento del problema				
	Estado de la cuestión				
Contribución	Dificultad y contribución técnica				
Presentación	Exposición oral				
	Defensa				
NOTA FINAL					

la que se asignen valores a distintos criterios, tanto en términos de contenido como de presentación. El **cuadro 7** muestra un ejemplo de una posible matriz de evaluación, donde los criterios concretos sobre los valores de la matriz los debe establecer cada institución. Finalmente, para ayudar en la difusión del máster y dar valor a los trabajos realizados, se recomienda la publicación de los TFM en formato abierto, preferiblemente a través del repositorio institucional que cada universidad disponga.

Además del propio TFM, el módulo se completa con un periodo de prácticas de tres meses en empresas (prácticum). Dicho periodo deberá ser independiente del empleado para realizar el TFM y constituirá el punto de entrada del estudiante en el ámbito laboral de la ciberseguridad. A lo largo del periodo el alumno contará con un docente encargado de su supervisión y con un profesional de la institución receptora que actuará como mentor. El prácticum estará avalado por un plan previo, acordado entre las instituciones participantes, en el que se describirán las tareas a realizar y los indicadores de rendimiento a emplear. La acreditación de la realización se obtendrá tras la presentación de un informe positivo de superación del periodo, que necesariamente deberán refrendar ambas instituciones. En caso de que el alumno esté trabajando y ya haya iniciado su carrera profesional, se plantean las siguientes alternativas:

- El prácticum se sustituye por la realización de un TFM de mayor complejidad y extensión, lo cual se tendrá que valorar con el director del mismo.
- Si el alumno realiza actividades relacionadas con la ciberseguridad en la empresa en la que trabaja, estas podrían convalidarse por el prácticum. No obstante, el docente encargado de la supervisión del trabajo ha de valorarlo y aprobarlo.

5.2.2 Asignaturas y competencias

En el **cuadro 8** se presenta un resumen de las asignaturas y actividades que se deben realizar en cada uno de los módulos establecidos, junto con las competencias que se asignan en cada caso. Nótese que en el módulo de nivelación (Módulo 0), debido a que pretende servir como punto de inicio para los estudiantes de disciplinas ajenas a las TIC, se adquieren solamente competencias básicas.

Cuadro 8. Competencias por asignaturas y actividades

	Básicas						Generales						Específicas												
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	12	13
M0																									
a	x		x	x	x	x																			
b	x		x	x	x	x																			
c	x		x	x	x	x																			
M1																									
a	x	x	x	x	x	x	x	x	x	x				x			x	x	x						
b		x	x	x	x	x		x	x	x		x		x			x								
c	x	x	x	x	x	x	x	x	x	x			x	x			x								
d	x	x	x	x	x	x	x		x	x			x		x										
e	x	x	x	x	x	x	x		x	x		x	x		x					x					
f		x	x	x	x	x			x	x	x	x					x								
M2																									
2.1																									
a		x	x	x	x	x		x	x	x							x	x							x
b		x	x	x	x	x		x	x	x	x						x			x	x				
c	x	x	x	x	x	x	x	x	x	x							x						x		
d	x	x	x	x	x	x	x	x	x	x		x					x	x						x	
2.2																									
a	x	x	x	x	x	x	x		x	x			x		x				x						
b	x	x	x	x	x	x	x		x	x			x	x	x										
c	x	x	x	x	x	x	x	x	x	x						x									
d	x	x	x	x	x	x	x	x	x	x				x				x							
M3																									
a	x	x	x	x	x	x	x	x	x	x							x			x					
b	x	x	x	x	x	x	x	x	x	x							x	x				x			
c			x	x	x					x							x	x			x				
d	x	x	x	x	x	x	x		x	x					x										
e	x	x	x	x	x	x	x	x	x	x							x								
f	x	x	x	x	x	x		x	x			x		x	x				x	x					
g	x	x	x	x	x		x	x					x										x		
h	x	x	x	x	x							x			x										
Sm	x	x	x		x	x	x	x	x	x	x	x			x	x	x	x	x						
M4	x	x	x	x	x	x	x	x	x	x	x					x	x	x	x	x					

Cuadro 9. Asignación horaria

Tipo de asignatura	Horas impartidas (mín./máx.)	Horas trabajo del alumno / online (mín./máx.)
Obligatoria	32-36	48-54
Elegible	23-25	34,5-37,5
TFM	---	250-300
Prácticum	---	250-300
Conferencias	8-12	---

5.2.3 Resumen del contenido del curso y asignación horaria

En el **cuadro 9** se indican los tipos de asignaturas, obligatorio o elegible, considerando que el alumno ha de escoger un bloque de asignaturas del Módulo 2 (M2); y el número de horas presenciales y de trabajo del estudiante que se asignan. En el Módulo 4 (M4) hay que considerar que el prácticum se ha establecido como trabajo a media jornada (4 horas) durante tres meses.

Si se considera que este máster es de carácter semipresencial, el número de horas de trabajo del alumno es significativamente superior al de las clases presenciales. En el **cuadro 9** se muestra un intervalo de horas a impartir y las horas de trabajo del alumno. Posteriormente, cada institución deberá ajustar la distribución atendiendo a criterios organizativos propios. Así, si se cursan las seis asignaturas obligatorias correspondientes al Módulo 1, las cuatro obligatorias de la especialidad escogida en el Módulo 2, las tres elegibles del Módulo 3, el TFM, el prácticum y las conferencias, el número de horas totales del máster ascendería a 1.480,5 como mínimo y llevaría 1.699,5 como máximo.

5.5 Metodologías docentes

Dado el carácter semipresencial del máster, una parte del mismo requerirá asistencia, mientras que otra parte se podrá realizar a distancia. Así, a continuación, se exponen las distintas actividades que componen la metodología, algunas de ellas con carácter presencial (P) y otras que puedan ser realizadas tanto presencialmente como a distancia (O).

Dentro de la metodología docente se considera:

- (P) Exposiciones en clase del profesor con el apoyo de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.

- (P/O) Discusión presencial o a distancia de textos recomendados por el profesor de la asignatura: artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión (presencial o a distancia), bien para ampliar y consolidar los conocimientos de la asignatura.

- (P/O) Resolución individual o grupal de casos prácticos, problemas, etc. planteados por el profesor.

- (P) Exposición y discusión, bajo la moderación del profesor, de temas relacionados con el contenido de la materia, así como de casos prácticos.

- (P/O) Elaboración de trabajos teórico-prácticos e informes de manera individual o en grupo.

Cada profesor podrá escoger las actividades metodológicas que más se adecuen a su asignatura. No obstante, se recomienda que al final de cada curso se realice una reunión en la que docentes y estudiantes reflexionen sobre las fortalezas y debilidades de las metodologías utilizadas, con el fin de mejorar en futuras ediciones.

5.6 Sistemas de evaluación

Dentro del sistema de evaluación se contemplan las siguientes posibilidades:

- Participación en clase, en las sesiones impartidas a distancia y en los foros telemáticos habilitados.

- Trabajos individuales o en grupo realizados durante el curso.

- Cuestionarios, colecciones de problemas o restos prácticos realizados durante el curso.

- Examen final.

Cada profesor tendrá que escoger la o las formas de evaluación que más se adecuen a su asignatura. No obstante, dado que el máster es de carácter semipresencial y las prácticas constituyen un aspecto relevante, se recomienda que, en caso de existir examen final, la nota que se asigne al mismo corresponda a un porcentaje complementario del resto de las calificaciones. Por ejemplo, una posible distribución de la evaluación se puede realizar en base al siguiente criterio:

- Actividades presenciales y prácticas: 30%.

- Exámenes parciales, trabajos y otro tipo de actividades: 30%.

- Examen final: 40%.

5.7 Plan de lanzamiento del máster

La difusión de los objetivos, de los contenidos, del profesorado, etc. del máster debería realizarse con suficiente antelación al comienzo del curso académico correspondiente.

La acción más eficiente suele ser la que se realiza en forma de charlas (más distendidas que las conferencias), impartidas por el director o subdirector del máster a alumnos del último curso de cada una de las titulaciones cercanas a la temática de la ciberseguridad. En estas charlas se expondría la importancia de la ciberseguridad en el presente y el futuro, los ataques y los atacantes, la inversión empresarial y la demanda de profesionales en esta materia, para concluir con los objetivos y la presentación del programa de máster y los recursos informáticos (servidores y redes) a disposición de los estudiantes. Todo ello con ayuda de tablas y gráficos (y quizás vídeos, por ejemplo, de YouTube).

Si la universidad tiene una asociación de exalumnos o un servicio de orientación para el empleo, suele ser útil remitir correos a los inscritos en una o el otro.

Del mismo modo, dirigirse por correo a empresas que demandan profesionales de ciberseguridad, así como productoras de *software*, informándolas del máster es una buena opción, pues a menudo estas prefieren formar a sus empleados de confianza, becándoles total o parcialmente estos estudios, antes que acudir al mercado laboral.

Por último, resulta imprescindible anunciar el máster en la página web de la universidad, presentando sus objetivos, programa académico, profesorado, porcentaje de egresados que trabajan en el sector (obviamente a partir de la segunda edición) y recursos docentes. Y mejor aún si el director del máster graba un vídeo corto (tres o cuatro minutos como máximo), en el que trate los mismos aspectos mencionados.

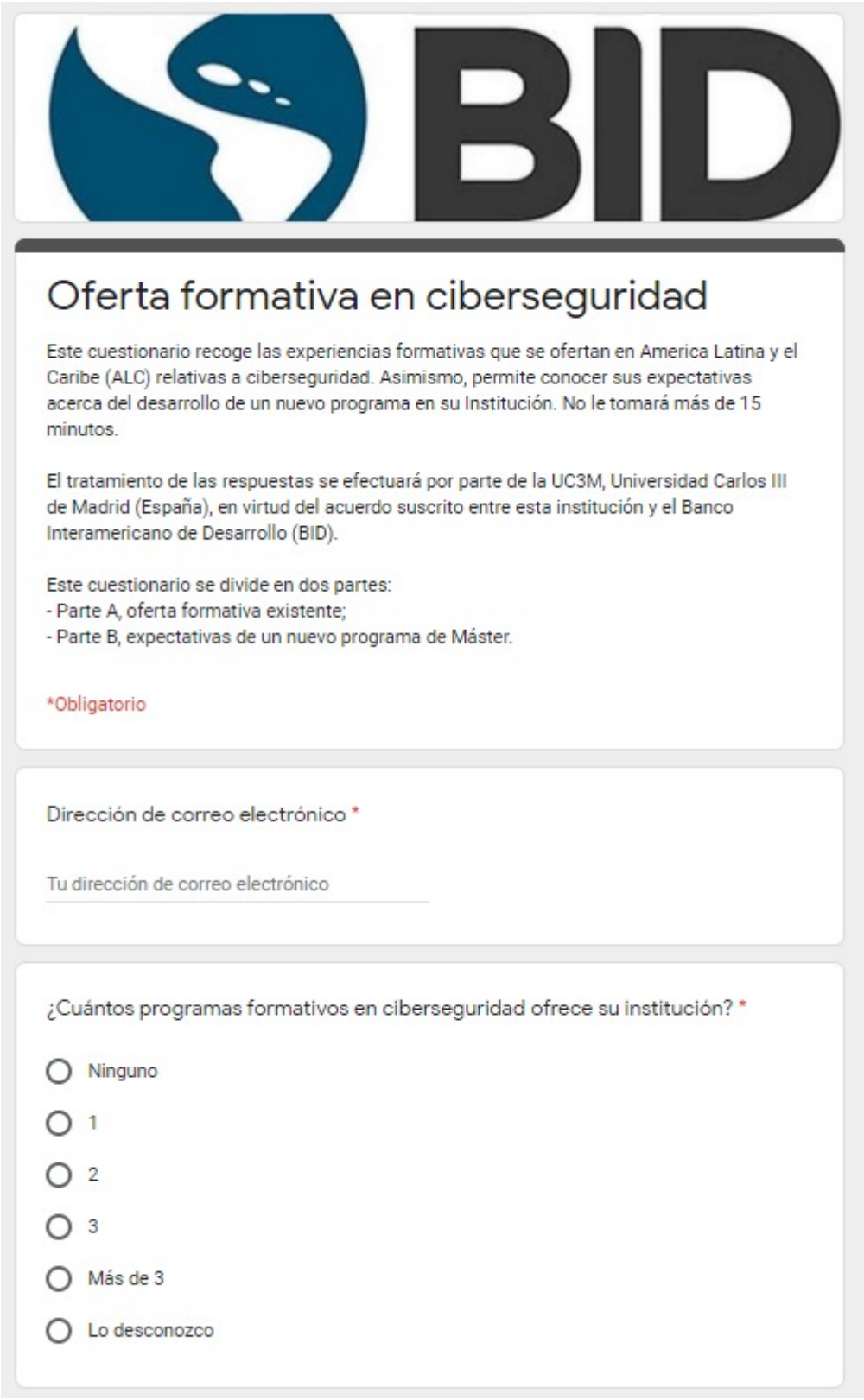
Anexos

/50

Anexo 1

Encuesta enviada a las universidades

En este anexo se detalla la encuesta que se ha realizado.



Oferta formativa en ciberseguridad

Este cuestionario recoge las experiencias formativas que se ofertan en America Latina y el Caribe (ALC) relativas a ciberseguridad. Asimismo, permite conocer sus expectativas acerca del desarrollo de un nuevo programa en su Institución. No le tomará más de 15 minutos.

El tratamiento de las respuestas se efectuará por parte de la UC3M, Universidad Carlos III de Madrid (España), en virtud del acuerdo suscrito entre esta institución y el Banco Interamericano de Desarrollo (BID).

Este cuestionario se divide en dos partes:
- Parte A, oferta formativa existente;
- Parte B, expectativas de un nuevo programa de Máster.

*Obligatorio

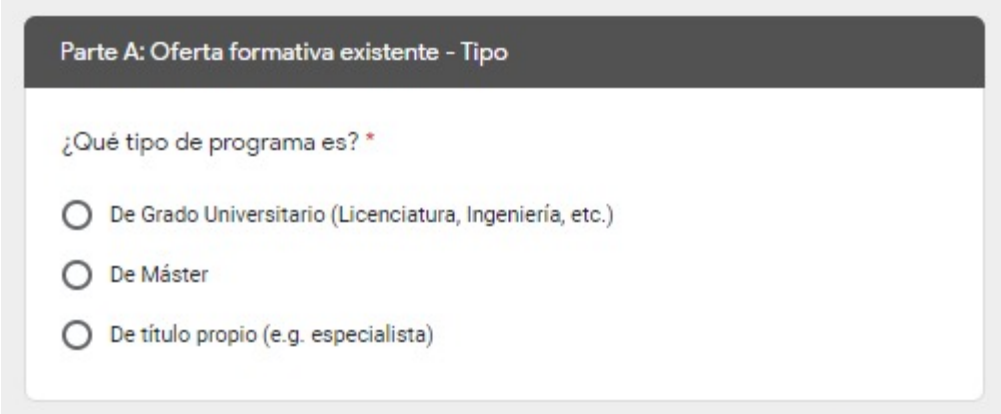
Dirección de correo electrónico *

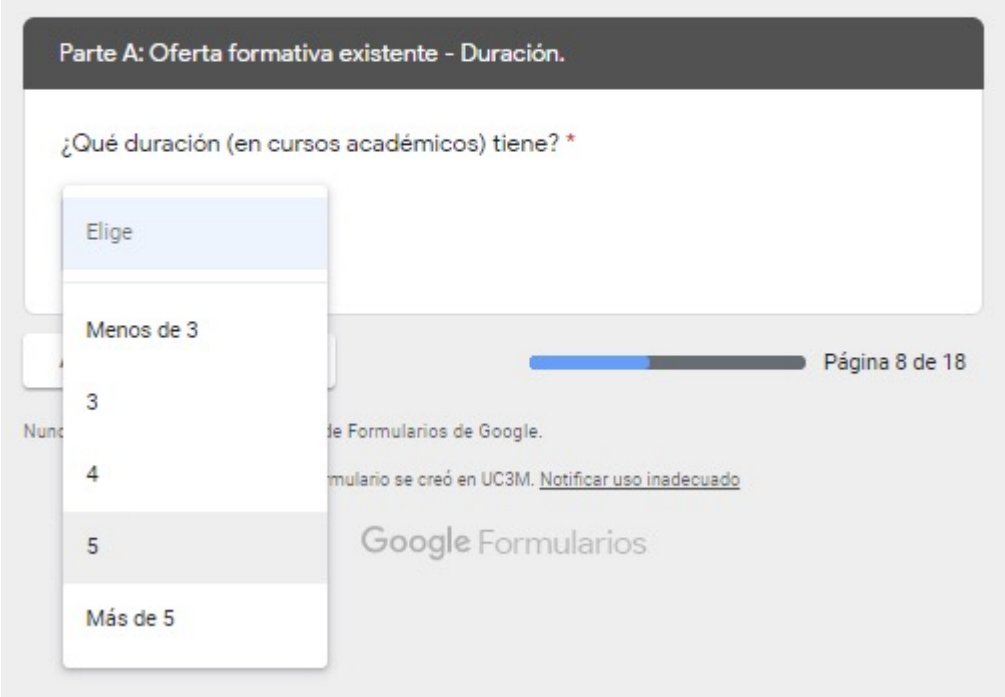
Tu dirección de correo electrónico

¿Cuántos programas formativos en ciberseguridad ofrece su institución? *

- Ninguno
- 1
- 2
- 3
- Más de 3
- Lo desconozco

Si existen programas formativos en ciberseguridad, se plantean las siguientes preguntas para cada uno de ellos.





Parte A: Oferta formativa existente - Contenidos, organización, datos generales

Entre las materias existentes ¿cuáles son las más demandadas dentro de los siguientes grupos? *

	Poca demanda	Alta demanda	No se oferta
Seg. en redes (IDS, SIEM, etc.)	○	○	○
Comunic. seguras (protocolos)	○	○	○
Sist. de ataque y defensa	○	○	○
Informática forense	○	○	○
Desarrollo seguro de software	○	○	○
Gestión de la seguridad	○	○	○
Protección de datos (cifrado, firma, etc.)	○	○	○
Análisis y auditorías de seguridad	○	○	○
Certif. de sist. y prod.	○	○	○
Identif. Autentic. y Ctrl. Acceso	○	○	○
Seg. en disp. móviles	○	○	○
Otra	○	○	○

Si consignó "Otra", indique aquí el nombre de dicha asignatura

Tu respuesta

¿En qué idioma(s) se imparte? *

- [ ] Español
- [ ] Inglés
- [ ] Otro:

Indique la dirección web del programa

Tu respuesta

¿Cuántos alumnos tiene por curso? *

Tu respuesta

¿Qué modelo docente sigue? *

- ○ Presencial
- ○ Semi-presencial
- ○ A distancia

Parte A: Oferta formativa existente - Tipo

¿Qué tipo de programa es? *

- ○ De Grado Universitario (Licenciatura, Ingeniería, etc.)
- ○ De Máster
- ○ De título propio (e.g. especialista)

Posteriormente, a todos los encuestados se les pregunta por sus expectativas ante un nuevo programa formativo en ciberseguridad.

Parte B: Expectativas de un programa formativo de Máster en Ciberseguridad

En esta Sección se recogerá la información sobre qué tipo de programa formativo podría ser interesante desarrollar en materia de ciberseguridad, diferente al que ya ofrezca su institución (en su caso)

NOTA 1: Le rogamos que todas las respuestas sean acordes con las necesidades formativas de su país

NOTA 2: Téngase presente, que en las asignaturas que tengan una fuerte carga practica (dado el carácter de este máster, casi todas ellas), las clases prácticas (con manejo individual del ordenador) no deberían impartirse a más de 15 (máximo 20) alumnos, pudiendo elevarse este número a un máximo de 40 en las clases de teoría.

En su opinión, atendiendo a las necesidades formativas de su país, ¿cuál debía ser la duración de un máster en ciberseguridad? *

- ○ Un año lectivo.
- ○ Un año y medio lectivo
- ○ Dos años lectivos.

¿En qué idioma debería impartirse? *

- ☐ Español
- ☐ Inglés
- ☐ Otro: _____

¿Qué titulación deberían tener los estudiantes que accediesen a un máster de esta naturaleza? *

- ○ Ingeniero (Licenciado) de sistemas, de software, de computación, etc.
- ○ Cualquier ingeniería (licenciatura).
- ○ Cualquier titulación superior.

¿Qué modelo de impartición sería más aconsejable? *

- ○ Presencial
- ○ Semi-presencial
- ○ A distancia

Con independencia de la respuesta anterior, suponga que se opta por un modelo presencial. Si cada hora de clase presencial requiere 1 hora y 30 minutos de estudio individual, ¿qué carga docente presencial debería tener este máster? *

- ○ 15 horas semanales (37,5 horas totales de dedicación del alumno a la semana)
- ○ 20 horas semanales (50 horas totales de dedicación del alumno a la semana)
- ○ Otro: _____

¿Considera oportuno que los alumnos realicen parte de su formación en una empresa? *

	Sí, 3 meses	Sí, 6 meses	No
Periodo	○	○	○

¿Considera que el plan de estudios debería contemplar la realización de un trabajo fin de máster obligatorio (TFM)? *

- ○ Sí
- ○ No

Parte B: Expectativas - TFM

¿Cuál debería ser el tanto por ciento de la carga de este TFM, respecto de la carga lectiva total presencial? *

- ○ 15%
- ○ 20%
- ○ 25%
- ○ Otro: _____

¿Consideraría una posibilidad que el TFM se realizase como proyecto o trabajo de investigación en alguna empresa?

- ○ Sí
- ○ No

Parte B: Expectativas - especialidades

¿Cree que las necesidades de su país aconsejarían que el máster tuviese especialidades de modo que, tras una formación generalista, los alumnos pudiesen elegir una especialidad entre dos o más? *

- ○ Sí
- ○ No

Parte B: Expectativas - materias

Consigne aquí las materias de interés, algunas de las cuales podrían ser especialidades

Señale cuál/cuáles de las siguientes materias podría/n ser de interés

	Poca demanda	Alta demanda	Ninguna
Desarrollo de sist. seg./ Seg. DevOps	○	○	○
Analista en ciberseguridad	○	○	○
Seg. en sist. industriales (incl. IoT)	○	○	○
Seg. en sist. ciberfísicos	○	○	○
Seguridad en cloud computing	○	○	○
Seguridad en big data	○	○	○
Informática forense	○	○	○
Dir. y gest. de la seg. (si el Máster es de 2 años)	○	○	○
Seg. en redes (IDS, SIEM, etc.)	○	○	○
Comunicaciones seguras (protocolos)	○	○	○
Otra*	○	○	○

Datos de contacto

Por favor, consigne aquí sus datos de contacto. Serán utilizados sólo en caso de necesitar aclaraciones sobre su oferta académica en ciberseguridad

Universidad / Centro de Investigación *

Tu respuesta

País *

Tu respuesta

Anexo 2

Lista de universidades que contribuyeron al desarrollo del programa

En el siguiente cuadro se presentan las instituciones que contribuyeron al desarrollo del programa, ya sea contestando la encuesta o participando en los talleres de retroalimentación.

Universidades que respondieron la encuesta o participaron de los talleres
Centro Universitário de Mineiros (UNIFIMES)
Escuela Superior Politécnica del Litoral (ESPOL)
Instituto de Computação, Universidade Estadual de Campinas (UNICAMP)
Instituto Federal Baiano (IFBAIANO)
Instituto Federal de Alagoas (IFAL)
Instituto Federal de Brasília (IFB)
Instituto Federal de Ceará (IFCE)
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense (IFSUL)
Instituto Federal de Mato Grosso (IFMT)
Instituto Federal de Minas Gerais (IFMG)
Instituto Federal de Rondônia (IFRO)
Instituto Federal de Santa Catarina (IFSC)
Instituto Federal de São Paulo (IFSP)
Instituto Federal de Sergipe (IFS)
Instituto Federal do Acre (IFAC)
Instituto Federal do Amazonas (IFAM)
Instituto Federal do Maranhão (IFMA)
Instituto Federal do Pará (IFPA)
Instituto Federal do Piauí (IFPI)
Instituto Federal do Sul de Minas Gerais (IFSULDEMINAS)
Instituto Federal do Tocantins (IFTO)
Instituto Federal do Triângulo Mineiro (IFTM)
Instituto Tecnológico de Buenos Aires

Instituto Tecnológico de Costa Rica
Pontificia Universidad Javeriana
Tecnológico de Monterrey
The University of the West Indies
Universidad Nacional Autónoma de Nicaragua (UNAN), Managua
Universidad Austral
Universidad Cenfotec
Universidad de Buenos Aires
Universidad de Chile
Universidad de Costa Rica
Universidad de la República Oriental del Uruguay
Universidad de la Sabana
Universidad de los Andes
Universidad de San Francisco de Quito
Universidad de Talca
Universidad del Rosario
Universidad del Valle
Universidad EAFIT
Universidad Federal do Ceará
Universidad Francisco Gavidia
Universidad Iberoamericana
Universidad Industrial de Santander
Universidad Latina de Costa Rica
Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)
Universidad Mayor de San Simón, Bolivia
Universidad Nacional Autónoma de México
Universidad Nacional Autónoma de Nicaragua
Universidad Nacional de Caaguazú
Universidad Nacional de La Plata
Universidad Nacional de Rosario

Universidad Pontificia Bolivariana, Seccional Bucaramanga
Universidad Técnica Federico Santa María
Universidad Tecnológica de Panamá
Universidad Tecnológica del Uruguay
Universidade de São Paulo
Universidade do Vale do Itajaí (UNIVALI)
Universidade Estadual da Região Tocantina do Maranhão
Universidade Federal de Mato Grosso (UFMT)
Universidade Federal do Pará (UFPA)
Universidade Federal do Paraná (UFPR)
Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA)
Universidade Federal Fluminense (UFF)
Universidade Nilton Lins
University of The Bahamas
University of the West Indies, Cave Hill Campus


BID