CENTRO DE ESTUDIOS
GARRIGUES

Programa Executive *online*

Ciberseguridad, riesgos y seguridad digital

CENTRO DE ESTUDIOS
GARRIGUES

Programa Executive *online* Ciberseguridad, riesgos y seguridad digital

Introducción

La seguridad es uno de los pilares de la sociedad desde el punto de vista personal y profesional. En plena era de transformación digital, especialmente tras la pandemia, en la que el negocio ha ido fundamentándose y valiéndose de las tecnologías, es necesario, tanto a nivel empresarial como de administración pública, contar con una Ciberse-guridad adecuada a esta transformación. No solo se trata de reaccionar ante el cambio, sino de antici-parse al mismo.

Hoy en día, hay un amplio número de sectores en los que la Ciberseguridad es parte del negocio. En ese sentido, la normativa en seguridad y en protección de datos ha ido creciendo y adaptándose al cambio, lo que supone un reto constante para las organizaciones que, sin embargo, no solo deben dar cuenta del cumplimiento normativo, sino también de una capacidad de responder a los requerimientos del negocio.

Además, el cada vez más creciente uso masivo de las tecnologías de la información, así como el aumento de la interconectividad de los sistemas y plataformas, y la necesidad absoluta de las conexiones remotas, conllevan nuevos riesgos para las empresas, dado que están afectadas directa o indirectamente, por el aumento exponencial de las amenazas. Estas amenazas, a su vez, responden a diferentes fines: cada día son más frecuentes los ataques de Estado, los intereses geopolíticos contra Estados, contra grandes multinacionales con enorme capacidad de influencia, los robos de cantidades ingentes de datos, de información (privada y profesional), el crimen organizado con fines económicos, la desinformación, o los fraudes financieros a pequeña y gran escala. Otro aspecto de gran importancia serán las nuevas tecnologías y la capacidad de influencia de las mismas en el negocio, de forma que nos permita prepararnos desde el punto de vista de Ciberseguri-dad para dar respuesta a dichos desafíos y de los riesgos que debemos conocer y gestionar, así como saber cómo podemos aprovecharnos también de esas nuevas tecnologías, para mejorar nuestras capacidades de prevención, defensa y reacción, comprendiendo cómo la ciberresiliencia juega un papel fundamental.

Este programa propone la adquisición de conocimientos especializados, con una perspectiva de visión global de la seguridad de la información, la Ciberseguridad y los riesgos tecnológicos. Se dotará al alumno de una visión holística en estrategia y gobernanza, así como de una visión tecnológica y técnica que permita comprender las diferentes áreas de la Ciberseguridad así como analizar las relaciones entre todas ellas. Asimismo, este programa abrirá, por un lado, las puertas a un sector en una profunda expansión, donde hay una escasa oferta de profesionales para atender la enorme demanda ya existente de este tipo de perfiles y conocimientos, y por otro lado, permitirá continuar con el desarrollo profesional de quienes ya se encuentran en este sector, formándose en áreas diferentes.

Modalidad	**Duración**	**Precio**
Online	9 semanas	€ 2.500

CENTRO DE ESTUDIOS
GARRIGUES

El Centro de Estudios Garrigues es una institución de enseñanza de posgrado y formación ejecutiva que, mediante diferentes iniciativas de formación e investigación, promueve la difusión de conocimiento con la garantía, calidad y experiencia acumulada del despacho Garrigues.

Perfil del participante

El programa está dirigido a todas aquellas personas que estén interesadas en profundizar en un área tan demandada como la Ciberseguridad, buscando la visión estratégica y los conocimientos necesarios para afrontar los retos de esta materia desde un enfoque práctico.

En particular, está dirigido a:

- Profesionales que desarrollen la actividad de asesoramiento en materia de seguridad de la información.
- Profesionales que tengan que tomar decisiones de negocio en los que el conocimiento en materia de seguridad de la información y sus implicaciones sea relevante.
- Expertos en alguna de las áreas de la seguridad de la información que quieran completar su formación y sus conocimientos con una perspectiva holística, desde el punto de vista de un CISO.
- Otros profesionales de despachos o empresas que quieran completar y actualizar sus conocimientos en materia de Ciberseguridad.
- Directivos cuya responsabilidad no se centra en el ámbito de la Ciberseguridad pero requieran de un conocimiento específico para conocer los riesgos y el impacto o impulsar la implementación de las medidas necesarias en su empresa.
- Estudiantes de últimos años de carrera y jóvenes profesionales del sector IT que deseen abrir su futuro profesional en el área de la Ciberseguridad.

Objetivos

En España se produjeron, en el último año, más de 40.000 ciberataques al día. La creciente digitalización, así como la continua escalada en la dependencia tecnológica por parte de la mayoría de sectores de negocio, ya antes de la pandemia y, con más razón, tras la misma, proporcionan un campo de acción muy elevado para los delincuentes, donde se calcula que la pérdida generada por ciberataques está por encima del 1% del PIB mundial, sin contar con los numerosos robos de información que cada día nos preocupan más. Sin embargo, este escenario también proporciona una oportunidad para desarrollar una carrera profesional: se calcula que en 2022 haya alrededor de 1,8 millones de puestos de trabajo relacionados con la Ciberseguridad vacantes en el mundo.

Ser un profesional de la Ciberseguridad y aprovechar las oportunidades que ello representa exige la adquisición de unos conocimientos como los que este programa proporciona, que aporten una visión global, comprendiendo las amenazas y los riesgos a los que las empresas están expuestos, así como los mecanismos de estas para ser seguras y ciberresilientes. Todo ello, combinando el punto de vista teórico con casos prácticos que permitan una ejemplificación y aproximación práctica fundamental y diferencial.

Estructura del programa

Programa Executive *online*

Ciberseguridad, riesgos y seguridad digital

Programa Executive *online*
Ciberseguridad, riesgos y seguridad digital

Este es un programa 100% online que cuenta con ejercicios dinámicos e interactivos y un fundamento eminentemente práctico, de modo que cada módulo se completa con casos prácticos.

Además el alumno tendrá acceso a vídeos y clases en directo del claustro de profesores.

1. De la seguridad informática a la Ciberseguridad y seguridad digital
1.1.- Origen y evolución. Información, gente, tecnología y procesos. Riesgos. Infosec. Ciberseguridad y ciberresiliencia

2. Ciberamenazas y ciberinteligencia
2.1.- Qué y cuáles son las amenazas. Inteligencia de amenazas. Ataque vs defensa
2.2.- Geopolítica. Desinformación e influencia. Ciberespacio como vector a la capa humana
2.3.- Defensa y respuesta global. Iniciativas globales y nacionales (caso de España). Relación público-privada y el negocio de la Ciberseguridad

3. Gestión de riesgos de seguridad de la información y tecnológicos
3.1.- Comprendiendo el riesgo. Gestión del riesgo (mitigar/transferir/aceptar/evitar). Marcos y metodología
3.2.- Riesgos de seguridad de la información, terceros, ciberriesgo y riesgo operacional

4. Cumplimiento normativo
4.1.- ¿Por qué la regulación? Marcos regulatorios y cumplimiento
4.2.- El asunto de la privacidad y la Ciberseguridad

5. Estrategia y gobernanza de la Ciberseguridad
5.1.- Marcos de referencia principales y desarrollo de un marco de Ciberseguridad
5.2.- Estrategia y gobierno vs seguridad operativa. Roles y responsabilidades, modelo de tres líneas de defensa. Inversión, eficiencia y reducción del riesgo

6. Marco de Ciberseguridad aplicado
6.1.- Tecnología y procesos de Identificación y protección
6.2.- Tecnología y procesos de detección
6.3.- Tecnología y procesos de respuesta y recuperación

7. Hacking ético y pruebas de seguridad
7.1.- Pruebas de intrusión, hacking ético y red team. De la inteligencia de amenazas y escenarios a la ejecución
7.2.- Métodos de explotación de vulnerabilidades. Análisis de vulnerabilidades

8. Ciberseguridad y transformación
8.1.- Cloud. Tipos y su seguridad
8.2.- Big data. Inteligencia artificial. Machine learning. Deep learning
8.3.- Aplicaciones de inteligencia artificial y ética
8.4.- Computación cuántica. Robotics process automation (RPA)

9. De camino hacia la ciberresiliencia
9.1.- Gestión de ciberincidentes. Ciberresiliencia
9.2.- Gestión de crisis y continuidad de negocio

10. Escenario práctico simulado inter modular
10.1.- Caso práctico fin de curso

CENTRO DE ESTUDIOS
GARRIGUES

Profesores

El Programa online "Ciberseguridad, riesgos y seguridad digital" del Centro de Estudios Garrigues cuenta con un panel de profesores compuesto por expertos de primer nivel que disponen de un conocimiento profundo y de primera mano en este ámbito, al tener un rol protagonista en el ámbito de la dirección y operación de la Ciberseguridad.

Sergio Padilla Foubelo (Director del programa)

Responsable de la Unidad de Riesgos y Seguridad de la Información en Banco de España.

Experto en Ciberseguridad, riesgos de seguridad de la información, ciber resiliencia, continuidad de negocio y nuevas tecnologías.

Desde 2017 es responsable de la seguridad de la información, la gobernanza y estrategia en Ciberseguridad, la gestión de riesgos tecnológicos en el Banco de España y el representante en los foros internacionales de dichas materias. Cuenta también con una dilatada experiencia nacional e internacional, comenzando en Accenture y habiendo ostentado, ya en el Banco, desde 2009, diferentes cargos de responsabilidad para las Infraestructuras de los Mercados Financieros del Eurosistema, siendo actualmente Security Officer del Banco de España para las mismas.

Ángel Gómez de Ágreda

Coronel de aviación. Analista geopolítico. Doctor en Ingeniería de Organización por la Universidad Politécnica de Madrid (UPM).

Ha sido jefe de cooperación del Mando Conjunto de Ciberdefensa y profesor en el Centro Superior de Estudios de la Defensa. Piloto y paracaidista militar.

Escritor y divulgador. Miembro de las juntas del Observatorio del Impacto Social y Ético de la Inteligencia Artificia (OdiseIA) y de la Asociación Española de la Singularidad (AES). Académico correspondiente de las Artes y las Ciencias Militares (ACAMI).

Profesores

Rubén Fernández Nieto

CISO Global de Grupo DIA.

Desde 2019 es Responsable Global Corporativo de Seguridad de la Información. Entre sus funciones, destacan la definición de la Estrategia en Ciberseguridad así como la Gestión de Riesgos Tecnológicos en el Grupo DIA y el Compliance relativo a Ciberseguridad.

Más de 20 años de experiencia en Ciberseguridad, análisis y Gestión de Riesgos de Seguridad de la Información, Compliance, Continuidad de Negocio y Contingencia. Cuenta con una amplia trayectoria internacional, habiendo trabajado con asiduidad en proyectos internacionales para Sudamérica, Centroamérica, Europa y Estados Unidos, para grandes empresas.

Ramsés Gallego

Security, Risk & Governance International Director para Micro Focus.

Ha sido Strategist & Evangelist para la oficina del CTO en Symantec y con anterioridad tuvo un rol similar en Dell Security y en CA Technologies.

Asimismo ha participado en el Comité de Certificación CISM y CGEIT de ISACA durante varios años y ha sido Presidente de la Conferencia ISRM (Information Security & Risk Management).

Reconocido ponente internacional con galardones en 4 continentes, incluyendo el John Kuyers Award como Best Speaker.

Posee una combinación de certificaciones de alto valor para diversas industrias , CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT y Six Sigma Black Belt.

Elena Matilla Rodríguez

Chief Information Security Officer en el Grupo Red Eléctrica.

Vinculada al mundo del gobierno, gestión, riesgos, cumplimiento y concienciación en Ciberseguridad desde hace más de 20 años.

Con anterioridad, trabajó como consultora senior en la empresa Ingeniería de Sistemas para la Defensa de España (ISDEFE), liderando proyectos de Ciberseguridad para el Ministerio de Defensa Español y las Fuerzas y Cuerpos de Seguridad del Estado y anteriormente, como Jefa de Proyectos de seguridad de la información en el grupo de telecomunicaciones europeo France Telecom.

Profesores

Antonio Fernandes

Chief Information Security Officer.

Evaluador de proyectos de innovación y Ciberseguridad para el European Innovation Council o la European Defense Agency, y miembro del subgrupo de expertos "Artificial Intelligence (AI) connected products and other new challen ges in product safety" de la Comisión Europea.

Recientemente votado como Most Valued Hacker en la HackerOne Meetup de Madrid y reconocido como Chief Security Envoy por la unidad de Ciberseguridad de Telefonica, Elevenpaths.

Alejandro López Parra

Chief Information Security Officer en LaLiga.

En su posición actual, es el máximo responsable de su sistema de gestión de la seguridad con el objetivo de gobernar la seguridad, así como prevenir y gestionar los incidentes de seguridad de La Liga Nacional de Fútbol Profesional.

Cuenta con más de 15 años en el ámbito de la seguridad de la información, tanto en el sector privado como en el público, habiendo sido también responsable en el equipo de respuesta a incidentes (CERT) del Instituto Nacional de Ciberseguridad de España (INCIBE).

Cristiano Paris

Experto superior en Ciberseguridad en el Banco Central Europeo.

En 2016 se incorporó al Banco Central Europeo, trabajando inicialmente en el campo de la Supervisión Bancaria, y más tarde pasó a la Dirección de Infraestructura Financiera y Pagos, donde es responsable de supervisar la seguridad y la ciberresiliencia de las Infraestructuras del Mercado Financiero del Eurosistema. Anteriormente, trabajó en la Banca d'Italia (Banco Central Italiano) como Auditor de TI en la Dirección de auditoría interna.

Es miembro de la Junta del Capítulo de Milán de ISACA, así como instructor certificado para la certificación de Auditor de Sistemas de Información Certificados (CISA) de ISACA.

CENTRO DE ESTUDIOS
GARRIGUES

Síguenos

centrogarrigues.com

T (+34) 91 514 53 30
informacion.centro@garrigues.com