GRC ZIBERSEGURTASUN KORPORATIBOKO EXEKUTIBOA IKASTAROA (ONLINE)

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	60 ORDU
EGUTEGIA	2024/09/17 - 2024/11/22 As-At-Az-Og-Or
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

HELBURUAK

Conocimiento de todos los conceptos, actividades y buenas prácticas relativas a la Seguridad de la Información GRC, para su aplicación en una organización.

Adquisición de una visión de conjunto para la toma de decisiones a nivel ejecutivo con una base teórico-práctica adecuada, y el liderazgo y la conducción de un programa de Seguridad de la Información en cualquier compañía.

NORI ZUZENDUA

Este itinerario formativo se concibe desde un ejercicio de síntesis de conocimientos en materia de ciberseguridad GRC: tratando de conjugar el ser lo suficientemente exhaustivos (en este sentido es de los más completos del mercado en la actualidad), y que pueda ser abordado en un tiempo razonable.

Se orienta principalmente a ejecutivos, líderes o profesionales de capas intermedias en el mundo corporativo o análogo, que buscan adquirir conocimientos en el ámbito de la seguridad de la información GRC con una formación a su ritmo, y que les permita incorporar la visión de ciberseguridad, buenas prácticas y normativa asociada en su organización.

La finalidad es proporcionar:

- Conocimiento en materia de ciberseguridad
- Herramientas para la toma de decisiones
- Soporte a la implantación de políticas, buenas prácticas y observancia de regulaciones

De esta manera, les permitirá:

- A nivel personal o individual, robustecer su perfil con conocimientos de ciberseguridad GRC, en un mercado con una gran carencia de profesionales*.
- A nivel corporativo, incrementar la protección de sus organizaciones y por tanto reducir el nivel de riesgo en el cumplimiento de sus objetivos.

• Según el Observatorio de INCIBE (Instituto de Ciberseguridad de España), la brecha de talento en el mercado de ciberseguridad era de 22K profesionales en 2022, y crecerá hasta los 83K en 2024.

PROGRAMA

• Introducción

• Gobierno de la Seguridad. Introducción de conceptos y necesidad de seguridad de la información, aspectos presupuestarios, gobierno, sistemas de gestión de seguridad de la información, planes directores de seguridad, programas y políticas, modelos de madurez y gestión de tecnologías de la información.

• Análisis de Riesgos. Introducción, estándares internacionales de gestión del riesgo ISO 31000 e ISO 27005 (Tecnologías de Ia Información), enfoques de gestión del riesgo y metodologías asociadas (MAGERIT, COBIT, OCTAVE, NIST SP 800-30 y SP 800-37), ejemplos de herramientas, y actividad práctica asociada.

• Cumplimiento normativo. Revisión de aspectos principales de normas y estándares nacionales e internacionales:

- Transversales como ISO27001, Esquema Nacional de Seguridad, ISO 22301 de continuidad de negocio, o NIST Cybersecurity Framework, entre otras.
- Normas del sector industrial como NIST SP 800-82 o ISA/IEC 62443.
- De entornos cloud, como ISO 27017, ISO 27018 o los recursos de la Cloud Security Alliance.
- De otros sectores de actividad, como el sanitario (HIPAA, ISO 27799…), marítimo, financiero, telecomunicaciones, transporte, energía, …
- De pagos electrónicos, como PCI-DSS.
- De firma electrónica.
- De privacidad.

• Regulación Legal. Aspectos de cumplimiento normativo que serán de aplicación general, o específicos (según el ámbito de actividad): ley general de telecomunicaciones, ley de servicios de la sociedad de la información, normativas de pagos electrónicos como PSD y PSD2, todo lo relativo a firma electrónica y el reglamento europeo IDAS, Esquema Nacional de Seguridad y directiva NIS/2, y por último analizaremos con más profundidad los diferentes ámbitos de la protección de datos, los derechos de propiedad intelectual e industrial, y los contratos informáticos y electrónicos y sus variantes.

IRAKASLEAK

Lizarraga Durandegui, Jesus Maria