FICHA DE ASIGNATURA

Título: Gobierno de la seguridad

Descripción: El gobierno de la ciberseguridad es la disciplina encargada de dirigir, monitorizar y evaluar el rendimiento de las distintas iniciativas puestas en marcha desde el área de la ciberseguridad para:

- Velar por el cumplimiento del marco normativo y regulatorio.
- Minimizar la probabilidad de ocurrencia y potencial impacto de incidentes de ciberseguridad
- Maximizar las capacidades de detección de ataques e incidentes
- Liderar y coordinar la gestión y resolución de incidentes de ciberseguridad

Pero el gobierno de la ciberseguridad también es hablar de modelos y metodologías, de objetivos de negocio, de estrategia, de alineación de objetivos de negocio con objetivos de ciberseguridad, de iniciativas o actividades alineadas con objetivos de negocio y de priorizar dichas iniciativas en términos beneficio, costos y riesgos asociados.

Carácter: *Obligatoria*

Créditos ECTS: 3

Contextualización: Comprender que para llevar la ciberseguridad al lugar organizativo que le corresponde hay que saber hablar en términos de negocio y alinear laciberseguridad con los objetivos de negocio. Conocer y poner en práctica herramientas que permitan mejores y más eficientes tomas de decisión en materia de gobierno de la ciberseguridad..

Modalidad: Online

Temario:

Semana 1:

- Tema 1: Marcos y modelos de gobierno de la ciberseguridad

    1.1- Estándares y buenas prácticas de la industria

    1.2- Impulsores del buen gobierno de la ciberseguridad

    1.3- Principios rectores del modelo de gobierno

    1.4- Estructuras organizativas

    1.6- Métodos y modelos de responsabilidad

    1.7- Monitorización del gobierno

    1.9- Técnicas de comunicación y reporting

    1.10- Técnicas y metodologías de revisión/auditoría

    1.11- Mejora continua

 Tema 2: Gestión estratégica de la ciberseguridad

2.1- Relación entre estrategia de empresa y ciberseguridad

2.2- Técnicas y procesos de planificación estratégica

2.3- Documentación y comunicación de la estrategia de ciberseguridad

2.4- Metodologías de priorización de iniciativas de ciberseguridad

2.6- Métricas e indicadores

2.5- Asignación de objetivos personalizados

 Evaluación Continua:

o Ejercicios: Actividad 1 – Alinear Modelo e iniciativas de ciberseguridad con estrategia de empresa

Semana 2:

 Tema 3: Optimización de recursos y gestión del riesgo

3.1.- Variables principales en la relación de costos

3.1.1- Recursos humanos internos

3.1.2- Adquisición de sistemas de ciberseguridad

3.1.3- Servicios externalizados

3.2- Interoperabilidad, estandarización y economías de escala

3.3- Costos y precio de un producto o servicio

3.4- Gestión del riesgo

3.5- Conceptos de gestión de Nivel de servicio

 Evaluación Continua:

o Ejercicios: Actividad 2 – Transformación de iniciativas en proyectos y servicios, y priorización de éstos

Semana 3:

 Tema 4: Obtención de beneficios

4.1- Inversiones: VAL IT

4.2- Éxito de un proyecto

4.3- Proyectos y estrategia

4.4- Gestión de la cartera (portfolio) de proyectos

4.5- Técnicas de evaluación de proyectos

- Evaluación Continua:
- Ejercicios: Completar actividad 1 y 2

Competencias:

Generales

- CG8 – Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Básicas

- CB6 – Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB7 – Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de estos.
- CB8 – Que los estudiantes sepan comunicar sus conclusiones y conocimientos, así como las razones que las sustentan, a públicos especializados y no especializados de una forma clara y sin ambigüedades.
- CB9 – Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de una manera auto-dirigida o autónoma en gran medida.

Transversales

- CT4 – Gestionar la adquisición, estructuración, análisis y visualización de datos e información (en el ámbito informático y de seguridad), y valorar de forma crítica los resultados de esta gestión.
- CT12 – Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (en el ámbito informático y de seguridad) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

Específicas

- CE9 – Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios, sistemas inteligentes y sistemas basados en el conocimiento.

Actividades Formativas:

Actividad Formativa	Horas	Presencialidad
Clases Magistrales (Video-Sesiones)	6	100
Clases de Tutoría	6	100
Ejercicios prácticos Individuales	20	0
Estudio autónomo	30	0

Metodologías docentes:

- Clase magistral / método expositivo
- Plataforma virtual de aprendizaje
- Aprendizaje Cooperativo (realización de trabajos)
- Aprendizaje Basado en Problemas (ABP)
- Entornos de simulación (recreación de problemas reales)

Sistema de Evaluación:

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Presentación de trabajos y/o proyectos	60.0	60.0
Examen escrito/oral (prueba objetiva, prueba de respuesta corta y/o prueba de desarrollo).	40.0	40.0

Bibliografía:

1.- CGEIT® Review Manual 7th Edition, ISACA

18

2.- El Cuadro de Mando Integral (BSC, Balanced Scorecard), Robert Kaplan & David

Norton

3.- Nunca comas solo, Keith Ferrazzi

4.- Otras indicadas en los contenidos entregados