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 de beneficio, costos y riesgos asociados.

Carácter*: Obligatoria*

Créditos ECTS: 3

Contextualización *(Máximo 60 palabras)*: Comprender que para llevar la ciberseguridad al lugar organizativo que le corresponde hay que saber hablar en términos de negocio y alinear la ciberseguridad 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:

- Certificación de seguridad: Normativa y marcos de referencia (COBIT, Control Objectives for Information Systems and related Technology), estándares (ISO) y optimización de recursos.
- Gestión estratégica de la seguridad en una organización.
- Beneficios derivados del gobierno de la seguridad y certificaciones
- Alineación de la normativa con las necesidades de negocio

Competencias Específicas:

CE5 - Comprender la interacción entre negocio, activos y ciberseguridad en una organización.

CE6 - Elaborar estrategias de alineamiento entre soluciones de ciberseguridad y objetivos de negocio

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	15	100%
Desarrollo de actividades del portafolio	12	0
Trabajo autónomo del alumno	48	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

Normativa específica*:*

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