Gestión y Administración de la Ciberseguridad

Curso Académico: (2019 / 2020) **Fecha de revisión: 25-04-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: RIBAGORDA GARNACHO, ARTURO

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No aplicable

OBJETIVOS

COMPETENCIAS BÁSICA:
Capacidad de integrar conocimientos y formular juicios a partir informaciones incompletas o poco precisas.
Capacidad de comunicar sus opiniones y juicios y las razones que los sustentas públicos, especializados y no, de un modo claro y sin ambigüedades.
Habilidad de estudiar y aprender de modo autodirigido y autónomo

RESULTADOS DEL APRENDIZAJE
1. Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS).
2. Partiendo del plan director de tecnologías de la información de una organización, de su plan general de seguridad (contra riesgos naturales, tecnológicos, etc.) y conociendo sus recursos humanos, tecnológicos, etc., elaborar un plan de seguridad de la información.
3. Construir un plan de continuidad conocido el tiempo máximo de recuperación admisible
4. Elaborar un plan de concienciación y formación en seguridad adaptado a la estructura organizativa de una empresa
5. Elaborar y mantener un sistema de clasificación de la información.
6. Conocer el funcionamiento de los Centros de Operaciones de Seguridad, sus relaciones mutuas y las normas de intercambio de informaciones acerca de incidentes de seguridad
7. Conocer las disposiciones legales de aplicación en materia de ciberseguridad y sus implicaciones en el diseño de sistemas seguros

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción y Conceptos Básicos. Normalización, evaluación, certificación y acreditación. Instituciones de normalización. Marco legal
2. Sistemas de gestión de la seguridad de la información. Normas ISO/IEC. Serie 27XXX. UNE-ISO/IEC 27000:2014, UNE-EN ISO/IEC 27001:2017, UNE-EN ISO/IEC 27002:2017. Normas certificables de la serie
3. Planes de seguridad
4. Formación y Concienciación
5. Clasificación de la información
6. Planes de Continuidad del negocio. UNE-EN-ISO 22301:2015 y UNE-ISO 22313:2013.
7. Centros de operaciones de ciberseguridad
8. Estrategias y Marco Legal de la ciberseguridad
9. Auditoría de la seguridad. Marcos y estándares para la auditoría. Auditoría de datos personales. Evidencias. Análisis. El informe de auditoría

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Clases teórico prácticas
Tutorías
Trabajo en grupo
Trabajo individual del estudiante

METODOLOGÍAS DOCENTES

Exposiciones en clase del profesor con soporte 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.

Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.

Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos

Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

La evaluación tiene como misión conocer el grado de cumplimiento de los objetivos de aprendizaje, por ello se valorará todo el trabajo del alumno, individual o colectivamente, mediante la evaluación continua de sus actividades a través de los ejercicios y exámenes, trabajos prácticos y otras actividades académicas formativas descritas anteriormente.
Se realizará una evaluación formativa a través de la realimentación continua, que permita al alumno evaluar qué conoce y qué se espera de él.
La nota final tendrá en cuenta las actividades individuales del alumno y las actividades de equipo. Las actividades llevadas a cabo durante el curso, individuales o en grupo, supondrán un 45% de la nota, un examen parcial (no liberatorio) otro 15%, mientras que el examen final individual constituirá el restante 40%. En todo caso, la realización de examen final es obligatoria, siendo necesario obtener, al menos, el 40% de la nota máxima posible en este examen para poder superar la asignatura.
Para la convocatoria extraordinaria, se pueden dar tres situaciones según que el estudiante:
a) Haya seguido el proceso de evaluación continua y desee mantener la nota de esta. En este caso, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.
b) No haya seguido el proceso de evaluación continua. En este caso, tendrá derecho a realizar un examen con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso.
c) Haya seguido el proceso de evaluación continua, pero desee ser calificado en la convocatoria extraordinaria en las mismas condiciones indicadas en el apartado b).

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- C.M. Fernández Sánchez y M. Piattini Velthuis Modelo para el gobierno de las TIC basado en las normas ISO, AENOR, 2012
- L. Gómez Fernández; P.P. Fernández Rivero Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS, AENOR.
- NORMA UNE-ISO/IEC 27000:2014, AENOR, 2014
- NORMA UNE-ISO/IEC 27001:2014, AENOR, 2014
- NORMA UNE-ISO/IEC 27002:2015, AENOR, 2015

RECURSOS ELECTRÓNICOS BÁSICOS

- ENISA . Publications: www.enisa.europa.eu/publications
- INCIBE . Guías: www.incibe.es/CERT/guias_estudios
- NIST . Special Publications (800 Series): csrc.nist.gov/publications/PubsSPs.html