

FICHA DE ASIGNATURA

Título: Cumplimiento normativo y RGPD

Descripción: Esta asignatura dotará al alumno de los conocimientos y las habilidades necesarias para el cumplimiento legal en la implantación y el gobierno de la ciberseguridad. En esta asignatura de cumplimiento se explican las normas nacionales e internacionales de referencia en la evaluación de la seguridad, pero sobre todo los aspectos legales que hay que cumplir, pues constituyen el punto de partida a partir del cual se debe construir la arquitectura de protección de nuestros sistemas informáticos. El incumplimiento legislativo, además del riesgo de sufrir un ataque, conlleva el riesgo de tener que pagar importantes multas, incrementando de esta forma las pérdidas producidas por un ciberataque. Se abordarán los ámbitos de: políticas de seguridad, privacidad y protección de datos, Esquema Nacional de Seguridad, Marcos de referencias y Estándares Nacionales e Internacionales, Certificación, Modelo de referencia familia ISO 27000.

Carácter: Obligatoria

Créditos ECTS: 6

Contextualización: El programa de esta asignatura proporciona una serie de conocimientos en el campo del cumplimiento legal que les serán de utilidad en su formación como expertos en seguridad informática, al proporcionarles los conceptos básicos para la comprensión de la legislación nacional e internacional que aplica en el ámbito de la ciberseguridad y además conocer las herramientas de autoevaluación y/o certificación.

Modalidad: Online

Temario:

- Legislación aplicable en España a la Ciberseguridad. Estrategia Nacional de Ciberseguridad. Código de Derecho de la Ciberseguridad.
- Privacidad y protección de datos (RGPD). Valoración y notificación de brechas. Derechos digitales.
- Seguridad en la administración, estrategia nacional y esquema nacional de seguridad. Legislación general y específica para infraestructuras críticas y su protección (PIC)
- Marcos de referencia y mejores prácticas: ISO, SANS (SysAdmin, Audit, Network, and Security), COBIT, ISACA (Information Systems Audit and Control Association)
- Ciberdelincuencia Nacional e Internacional (Convenio de Budapest).

Competencias Específicas:

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.

CE9 - Conocer la normativa que regula la certificación de seguridad en sistemas de la información y su implementación dentro de una organización.

CE11 - Aplicar las directrices generales en materia de Ciberseguridad en España derivadas de la Estrategia Nacional de Ciberseguridad y normativas implicadas.

Actividades Formativas:

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	30	100%
Desarrollo de actividades del portafolio	24	0
Trabajo autónomo del alumno	96	0

Metodologías docentes:

- Clase magistral
- Aprendizaje Cooperativo
- Tareas comunicativas
- Aprendizaje Basado en Problemas (ABP)
- Entornos de simulación
- Método del caso

Sistema de Evaluación:

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Trabajos individuales dirigidos	30.0	40.0
Pruebas de conocimiento	70.0	60.0

Normativa específica:

Bibliografía:

- BS7799:1 "Information Security Management- Part 1: Code of practice for information security management"
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION Estándares de Seguridad, ISACA, IEC/ISO. <http://www.isaca.org>
- ISO27001:2005 " Information Security Management- Specifications for an ISM"
- ISO/IEC 17799:2005 "Information Technology- Code of Practice for Information Security Management"
- Normas, estándares, Leyes y demás de las políticas de seguridad. 1150204-159-250-214
<https://seguridadinformaticaufps.wikispaces.com/Normas,+estandares+Leyes+y+demas+de+las+politicasyde+seguridad.+1150204-159-250-214>
https://www.incibe.es/empresas/que_te_interesa/Cumplimiento_legal/
- Information Security Policy Templates <https://www.sans.org/securityresources/policies/>
- INCIBE Cumplimiento legal
https://www.incibe.es/empresas/que_te_interesa/Cumplimiento_legal/
- Dictamen 4/2007 sobre el concepto de datos personales:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf
- Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

- Dictamen 15/2011 sobre la definición del consentimiento:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp187_es.pdf
- GUÍA para una Evaluación de Impacto en la Protección de Datos Personales
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Informe de Actividades del Centro Criptológico Nacional
<https://www.ccn.cni.es/documentos/CCN-Informe-de-actividades-2011-2012.pdf>
- Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones
<https://www.ccn-cert.cni.es/>
- El ENS en ISOTools: Una comparación con ISO 27001:
<http://www.isotools.org/esquema-nacional-de-seguridad.cfm>
- «El análisis de riesgos en la ISO 27001 y en el Esquema Nacional de Seguridad»:
<http://www.seinhe.com/posts/11-el-analisis-de-riesgosen-la-iso-27001-y-en-el-esquema-nacional-de-seguridad>