GESTIÓN Y ADMINISTRACIÓN DE LA SEGURIDAD

PROGRAMA DETALLADO

1. Introducción y Conceptos Básicos. Normalización, evaluación, certificación y acreditación. Instituciones de normalización. Marco legal
   1.1 Introducción y Conceptos Básicos
   1.2 Normalización, certificación, acreditación, etc. Marco legal
   1.3 Normalización internacional
   1.4 Normalización europea
   1.5 Normalización nacional. UNE. Comités técnicos de normalización
   1.6 Normas de iure y de facto. Ejemplos
2. Sistemas de gestión de la seguridad de la información. Normas ISO/IEC. Serie 27XXX
   2.1 UNE-ISO/IEC 27000:2014
   2.2 UNE-EN ISO/IEC 27001:2017
   2.3 UNE-EN ISO/IEC 27002:2017
   2.4 Normas certificables de la serie
3. Formación y Concienciación
4. Clasificación de la información
5. Planes de Continuidad del negocio.
   5.1 UNE-EN-ISO 22301:2015. Sistema de Gestión de la Continuidad del Negocio (SGCN). Especificaciones
   5.2 UNE-ISO 22313:2013. Sistema de Gestión de la Continuidad del Negocio (SGCN). Directrices
6. Centros de operaciones de ciberseguridad
   5.1 Estructura y organización
   5.2 Personal, procesos y procedimientos
   5.3 Metodologías de Respuesta a Incidentes. CSIRTs
7. Estrategias y Marco Legal de la ciberseguridad
   7.1 Estrategia Nacional de ciberseguridad
   7.2 Ley 11/2007 y RD 3/2010 Esquema Nacional de Seguridad
   7.3 Ley 53/2002 de firma electrónica
   7.4 El “delito informático” y el Código Penal
   7.5 Directivas de la UE
8. Auditoría de la seguridad. Marcos y estándares para la auditoría. Auditoría de datos personales. Evidencias. Análisis. El informe de auditoría
   8.1 Objetivos de control. Sistema de control interno
   8.2 Marcos y estándares para la auditoría.
   8.3 Auditoría de seguridad de los datos personales
   8.4 Objetivos, ámbito, fases, técnicas y herramientas de la auditoría:
   8.5 Aspectos a revisar. Fuentes a considerar
   8.6 Análisis. Evidencias. El informe de auditoría

Mayo 2018