Máster Universitario en Protección de Datos, Innovación y Seguridad

DOMINIO VI:

GESTIÓN CORPORATIVA DE LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD NEBRIJA

11. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

11.1 ISO 27001: Sistema de gestión de seguridad de la información.

Prof. Jesús Yáñez Colomo
Socio Risk, Compliance y Ciberseguridad en ECIJA Abogados.

- Conceptos de Seguridad de la información según ISO 27001.
- Ventajas de un SGSI. Factores para garantizar su éxito.
- Sistemas de gestión de seguridad de la información y el Reglamento General de Protección de Datos Europeo.
- Planificar, hacer, verificar y actuar.
- Alcance, objetivos y partes interesadas.
- Estructura documental, análisis y gestión del riesgo.
- Declaración de aplicabilidad, selección de controles y métricas.
- Exigibilidad de ISO 27001 a proveedores o terceros.
- Certificación y auditorías.

11.2 ISO 27002: Fundamentos de seguridad de la información.

Prof. Ricardo Cañizares Sales
Director de Consultoría en EULEN Seguridad.

- Diferenciación ISO 27001 e ISO 27002.
- El concepto y valor de la información.
- Medidas de seguridad, riesgos y daños.
- Implementación de un sistema de gestión de seguridad de la información fundamentado sobre el análisis y gestión de riesgos.
- Medidas físicas y técnicas.
- Medidas organizativas.
- Exigibilidad a terceros.

11.3 La gestión de la seguridad de los tratamientos.

Prof. José Luis Colom Planas
Director de auditoría y cumplimiento normativo en Audertis.

- El Reglamento General de Protección de Datos y la seguridad. La Disposición adicional primera de la LO 3/2018.
- El Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001:2013.
- La norma ISO/IEC DIS 27552 sobre extensiones de la norma ISO/IEC 27001 para sistemas de gestión de la privacidad.
- Requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Seguridad de los activos y organizacional. Medidas de seguridad basadas en el riesgo.
- Unificar la Declaración de Aplicabilidad (SOA), orientada a la seguridad de la información, con las medidas jurídico-organizativas que dispone el Reglamento General de Protección de Datos.
- Planes de continuidad del negocio. La norma ISO 22301:2012. Recuperación ante desastres.

11.4 Aplicación del Esquema Nacional de Seguridad.

Prof. José Manuel Laperal González
Responsable Seguridad Sistemas de Información Sanitaria y Secretario del Comité Delgado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid. Delegado de Seguridad y Enlace del Servicio Madrileño de Salud.

- Auditoría del Esquema Nacional de Seguridad.
- Política de seguridad, declaración de aplicabilidad, normativa, principales metodologías de análisis de riesgos.
- Plan Director de Seguridad.
- Real Decreto 12/2018 sobre seguridad de las redes y sistemas de información.
- Otros sistemas de control de riesgos: Cobit, PCI-DSS.

11.5 Nociones sobre el Esquema Nacional de Interoperabilidad.

Prof. Miguel Ángel Miguel Ruíz
Business Development Manager en Govertis Advisory Services.

- Ámbito de aplicación
- Adecuación al Esquema Nacional de Interoperabilidad
- Principios y directrices de interoperabilidad en el intercambio y conservación de la información electrónica por parte de Administraciones Públicas.
- Normas técnicas de interoperabilidad.
- Elementos comunes sobre la actuación de las Administraciones Públicas en materia de interoperabilidad.

11.6 Introducción a los Sistemas de Gestión de Seguridad de la Información.

Prof. Raúl Prieto Pozo
Delegado de Protección de Datos y Responsable Gobierno de Seguridad de la Información del Grupo Sothis.

- Los sistemas de gestión de seguridad de la información como catalizador de cumplimiento normativo
- Continuidad de negocio (ISO 22301).
- Real Decreto 12/2018 sobre seguridad de las redes y sistemas de información.
- Notificación de brechas de seguridad a diferentes organismos.
- Gestión de riesgos acumulados.

11.7 Aplicación práctica e integrada de los Sistemas de Gestión de Seguridad de la Información.

Prof. Raúl Prieto Pozo
Delegado de Protección de Datos y Responsable Gobierno de Seguridad de la Información del Grupo Sothis.

- Gestión integral de diferentes sistemas y normativas conexas.
- Soluciones de modelos de gestión.

11.8 La Ley de Protección de Infraestructuras Críticas (PIC).

Prof. José Manuel Laperal González
Responsable Seguridad Sistemas de Información Sanitaria y Secretario del Comité Delgado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid. Delegado de Seguridad y Enlace del Servicio Madrileño de Salud.

- Objetivos y fundamentos de la Ley y su reglamento de desarrollo.
- Planes sectoriales.
- Operadores críticos: responsabilidades y obligaciones.
- Aspectos principales de un Plan de Seguridad de un Operador (PSO).
- Infraestructura crítica: el Plan de Protección Específico (PPE).
- Alineamiento con la directiva NIST.

12. AUDITORÍA Y EVALUACIÓN DEL NIVEL DE PROTECCIÓN.

12.1 La auditoría de protección de datos.

Prof. Ricardo Barrasa García
Socio en NTASYS y Presidente de ISACA Madrid.

- El proceso de auditoría. Cuestiones generales y aproximación a la auditoría.
- Características básicas de la auditoría.
- Elaboración del informe de auditoría.
- Aspectos básicos e importancia del informe de auditoría.
- Ejecución y seguimiento de acciones correctoras.

12.2 La auditoría de seguridad de la información.

Prof. Iker Osorio Alfonso
Chief Information Security Officer en Cetelem.

- La función de auditoría en los sistemas de información.
- Conceptos básicos, estándares y directrices de auditoría de seguridad de la información.
- Control interno y mejora continua. Buenas prácticas.
- Integración de la auditoría de protección de datos en la auditoría de seguridad de la información.
- Planificación, ejecución y seguimiento.

12.3 Seguridad de los encargados del tratamiento.

Prof. Antonio Ramos García
Socio Director de n+1 Intelligence & Research y CEO de LEET Security. Vicepresidente ISACA Madrid, Miembro Lista de Expertos de ENISA.

- Nuevo escenario respecto a los encargados de tratamiento.
- Opciones de supervisión de terceros.
- Proceso de gestión de riesgo proveedor / terceras partes.
- Relación con las medidas de seguridad del responsable.

12.4 Workshop: Auditoría de privacidad y protección de datos.

Prof. Alonso Hurtado Bueno
Socio del Área de IT, Risk & Compliance en ECIJA Abogados.

- Requisitos de privacidad de obligaciones legales, contractuales y textos legales.
- Principios y objetivos de la auditoría.
- Recopilación de información para identificar los tratamientos de los datos personales
- Nivel de medidas de seguridad en función de la sensibilidad de los datos y riesgos asociados.
- Monitorización de amenazas en la red.
- Copias de seguridad y pruebas de recuperación de datos.
- Cifrado, pseudoanonimización y anonimización.
- Mecanismos de control de acceso a los datos.
- Trazabilidad de los datos.
- Diagnóstico y recomendaciones.
- Adecuación de las medidas y controles a la normativa.
- Identificación de deficiencias y vulnerabilidades.
- Propuesta de medidas para corregir los errores.
- Conclusiones del informe.

12.5 Workshop: Implantación de un sistema de gestión de seguridad de la información.

Prof. Francisco Ruíz Navarro
Responsable de servicios de seguridad en Mnemo.

- Implantación de un sistema general de seguridad de la información: Roles y responsabilidades, gestión del riesgo, controles
- Implantación de un Esquema Nacional de Seguridad: Política de Seguridad, gestión del riesgo, declaración de aplicabilidad.
- Elaboración de un Plan Director de Seguridad.

12.6 Workshop: Análisis, identificación y flujo de procesos.

Prof. Diego Alonso Asensio
Fundador y Project Manager de Nize Partners.

- Modelización en base a BPMN 2.0