ÍNDICE

2.2.3. Posibles escenarios de riesgo del Reglamento (UE) 2016/679

2.3. EL PROGRAMA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD EN UNA ORGANIZACIÓN. INTRODUCCIÓN AL CUMPLIMIENTO NORMATIVO: EL CÓDIGO PENAL ESPAÑOL Y LA LEY ORGÁNICA 1/2015

2.3.1. El Diseño y la implantación del programa de protección de datos en el contexto de la organización

2.3.2. Objetivos del programa de cumplimiento

2.3.3. La “Accountability” o la trazabilidad del modelo de cumplimiento

2.4. LA SEGURIDAD DE LA INFORMACIÓN

2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos

2.4.1.1. Esquema Nacional de Seguridad

2.4.1.1.1. Relación con el Esquema Nacional de Interoperabilidad.

2.4.1.1.2. Sujetos a los que se aplica

2.4.1.1.3. CCN-STIC: normas, instrucciones, guías y recomendaciones del CCN-CERT

2.4.1.1.4. Principios básicos y requisitos mínimos.

2.4.1.1.5. Categorización

2.4.1.1.6. Las medidas de seguridad

2.4.1.1.7. Plan de Adecuación

2.4.1.2. Directiva NIS (UE) 2016/1148

2.4.1.3. Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

2.4.2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades. Misión, y gobierno efectivo de la Seguridad de la Información (SI) Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.

2.4.2.1. Gobierno efectivo de la Seguridad de la Información.

2.4.2.2. Las métricas IT

2.4.3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.

2.4.3.1. Seguridad desde el diseño y por defecto

2.4.3.2. Integración de la seguridad y la privacidad en el ciclo de vida

2.4.3.3. El control de calidad de los Sistemas de Información

2.5. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS “EIPD”

2.5.1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares

2.5.2. Breve referencia a la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de derechos digitales

2.5.3. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos. Análisis de la necesidad de llevar a cabo la evaluación y consultas previas

2.6. LA GESTIÓN DE RIESGOS

2.7. BIBLIOGRAFÍA Y REFERENCIAS

ANEXO

01. Guía de Seguridad ENS (CCN-STIC-800) Glosario de términos y abreviaturas

02. Guía de Seguridad ENS (CCN-STIC-801) Responsabilidades y funciones

03. Guía de Seguridad de las TIC's ENS (CCN-STIC-802) Guía de Auditoría

04. Guía de Seguridad de las TIC's ENS (CCN-STIC-803) Valoración de los sistemas

05. Guía de Seguridad de las TIC's ENS (CCN-STIC-804) Guía de Implantación

06. Guía de Seguridad ENS (CCN-STIC-805) Política de Seguridad de la Información

07. Guía de Seguridad ENS (CCN-STIC-806) Plan de adecuación

08. Guía de Seguridad de las TIC's ENS (CCN-STIC-807) Criptología de empleo en el Esquema Nacional de Seguridad

09. Guía de Seguridad ENS (CCN-STIC-808) Verificación del cumplimiento de las medidas en el ENS

10. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

11. Methodology For Privacy Risk Management. How to implement the Data Protection Act.

12. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

13. Guía práctica de Análisis de riesgos en los tratamientos de datos Personales sujetos al RGPD. Agencia Española de Protección de Datos (AEPD)

14. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Agencia Española de Protección de Datos (AEPD)

15. Annual Cyber Security Assessment 2017 Estonian Information System Authority