Índice

Agradecimientos 9

Introducción 11

1. Los Sistemas de Gestión de la Seguridad de la Información (SGSI) 13
   - 1.1. Definición de un SGSI 13
   - 1.2. El ciclo de mejora continua 14
   - 1.3. La Norma ISO/IEC 27001:2017 15
     - 1.3.1. Novedades en la última versión de la norma 15
     - 1.3.2. Objeto y campo de aplicación de la norma 17
   - 1.4. La Norma ISO/IEC 27002:2017 17
     - 1.4.1. Objeto y campo de aplicación 17

2. Requisitos de la Norma ISO/IEC 27001 19
   - 2.1. Contexto de la organización 19
     - 2.1.1. Sistema de gestión de la seguridad de la información 19
     - 2.1.2. Conocer la organización 20
     - 2.1.3. Definición del alcance del SGSI 21
   - 2.2. Establecimiento y gestión del SGSI 21
     - 2.2.1. Liderazgo 21
     - 2.2.2. Planificación 23
     - 2.2.3. Soporte 27
     - 2.2.4. Operación 29
     - 2.2.5. Evaluación y desempeño 30
     - 2.2.6. Mejora 32
     - 2.2.7. El anexo A de la norma 33

3. Recomendaciones de la Norma ISO/IEC 27002 35
   - 3.1. Políticas de seguridad de la información 36
   - 3.2. Organización de la seguridad de la información 37

3.3. Seguridad relativa a los recursos humanos 38
3.4. Gestión de activos 39
3.5. Control de acceso 40
3.6. Criptografía 43
3.7. Seguridad física y del entorno 43
3.8. Seguridad de las operaciones 45
3.9. Seguridad de las comunicaciones 48
3.10. Adquisición, desarrollo y mantenimiento de los sistemas de información . 49
3.11. Relación con proveedores 52
3.12. Gestión de incidentes de seguridad de la información 53
3.13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio 54
3.14. Cumplimiento 55
4. Definir e implementar un SGSI 57
4.1. Fases del proyecto 57
4.2. Documentación del SGSI 60
4.3. Política de seguridad 60
4.4. Evaluación de riesgos 61
4.4.1. Elaboración del inventario de activos 61
4.4.2. Identificar y valorar amenazas 63
4.4.3. Calcular el impacto 64
4.4.4. Calcular el riesgo 65
4.5. Identificar a los propietarios de los riesgos y tratamiento de los riesgos . . 67
4.6. Determinar las medidas de seguridad 67
4.7. Evaluar los riesgos residuales 69
4.8. Plan de tratamiento del riesgo 71
4.9. Información documentada sobre procesos 71
4.10. Formación y concienciación 73
4.11. Auditoría interna 73
4.12. Revisión por la dirección 74
4.13. Evidencias 74
5. El proceso de certificación 77
6. Relación entre los apartados de la norma y la información documentada del sistema 81
7. Caso práctico: modelo de SGSI 83
7.1. Contexto de la organización 83
7.1.1. Presentación 83
7.1.2. Estructura de la empresa 84

7.1.3. Aspectos técnicos 84
7.2. Documentación de la política de seguridad 85
7.2.1. Política de seguridad de la información 85
7.2.2. Definición del SGSI 86
7.2.3. Marco organizativo de la seguridad de la información 88
7.2.4. Evaluación de riesgos de seguridad 89
7.3. El inventario de activos 90
7.3.1. Procesos de negocio 90
7.3.2. Inventario de activos 90
7.3.3. Relación proceso de negocio/activos 91
7.3.4. Valoración de activos 92
7.4. Resultados de la evaluación de riesgos 93
7.4.1. Identificación y valoración de amenazas 93
7.4.2. Cálculo del riesgo 98
7.4.3. Tratamiento del riesgo 102
7.5. Determinar los controles y declaración de aplicabilidad 103
7.5.1. Declaración de aplicabilidad 104
7.6. Documentación de la gestión de riesgos 113
7.6.1. Valoración de amenazas tras la aplicación de medidas 113
7.6.2. Cálculo de riesgos residuales 118
7.7. Documentación del plan de tratamiento del riesgo 123
7.7.1. Objetivo 123
7.7.2. Alcance 123
7.7.3. Responsabilidades 123
7.7.4. Tareas 123
7.7.5. Seguimiento 125
7.7.6. Objetivos e indicadores 125
7.8. Documentación del procedimiento de gestión de métricas de seguridad 127
7.8.1. Objetivo 127
7.8.2. Alcance 127
7.8.3. Responsabilidades 127
7.8.4. Desarrollo 128
7.8.5. Requisitos de documentación 129
7.8.6. Referencias 130
7.8.7. Anexos 130
7.9. Documentación del procedimiento de gestión de incidencias 131
7.9.1. Objetivo 131
7.9.2. Alcance 131

7.9.3. Responsabilidades 131
7.9.4. Desarrollo 131
7.9.5. Requisitos de documentación 132
7.9.6. Referencias 132
7.9.7. Anexos 132
8. El Esquema Nacional de Seguridad (ENS) 135
8.1. Introducción al ENS 135
8.2. Ámbito de aplicación del ENS 137
8.2.1. Ámbito subjetivo de aplicación 137
8.2.2. Ámbito objetivo de aplicación 138
8.3. Conformidad con el ENS 138
8.3.1. Sector privado y Esquema Nacional de Seguridad 139
8.4. Beneficios del ENS 139
8.5. Plan de adecuación al ENS 140
8.5.1. Política de seguridad en el ENS 141
8.5.2. Categorización de los sistemas 143
8.5.3. Análisis de riesgos 144
8.5.4. Declaración de aplicabilidad 145
8.5.5. Insuficiencias del sistema 145
8.5.6. Plan de mejora de seguridad 146
8.6. Implantación del ENS 146
8.7. Auditoría del ENS 147
8.8. Actualización del ENS 148
9. Cumplir con el ENS a través de un SGSI según ISO/IEC 27001 149
9.1. Motivación 150
9.2. Alcance 150
9.3. Política de seguridad 151
9.4. Marco organizativo 151
9.5. Dimensiones de la seguridad 152
9.6. Categorización y riesgos 152
9.7. Catálogo de controles 153
9.8. Auditorías y certificación 153
Bibliografía 155
Sobre los autores 163