GUÍA DE SEGURIDAD
(CCN-STIC 825)

ESQUEMA NACIONAL DE SEGURIDAD
CERTIFICACIONES 27001

NOVIEMBRE 2013

Edita:

NIPO: 002-13-052-X

Fecha de Edición: noviembre de 2013

José A. Mañas ha participado en la elaboración y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre de 2013

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El Esquema Nacional de Seguridad (ENS, en adelante) establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración (Anexo I) del nivel de seguridad en cada dimensión, y a la categoría (Artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.
2. Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados, la información manejada, y los riesgos a que están expuestos.

2. OBJETO

3. En esta guía se considera la relación del ENS con normas y estándares de gestión de la seguridad de la información, de amplia difusión. Concretamente, con las normas ISO/IEC 27001 e ISO/IEC 27002 publicadas en 2005 y revisadas en 2013.
4. Nótese que la correspondencia no es una relación matemática de equivalencia. Lo que se busca en esta guía es, en primer lugar, explicar la utilización de una certificación 27001 como soporte de cumplimiento del ENS y, en segundo lugar, determinar qué controles de la norma 27002 son necesarios para el cumplimiento de cada medida del Anexo II y, en su caso, qué elementos adicionales son requeridos. Es decir, si el organismo tiene una certificación 27001 y se han cubierto los controles referenciados de la 27002, con incorporar lo adicional se puede considerar cumplido el Anexo II.

3. ALCANCE

5. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.

4. NORMAS ISO

4.1. ISO/IEC 27001

6. La norma 27001 es una norma internacional, de gestión, de cumplimiento voluntario y certificable. Quiere esto decir que un auditor autorizado, previa inspección del sistema de gestión de la seguridad del sistema de información, certifica que es conforme a la norma.
7. Se certifica un sistema de gestión, que se define como sigue.
8. Según ISO/IEC - Annex SL - Proposals for management system standards (2012)

Sistema de gestión - management system

> set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives .
>
> Note 1: A management system can address a single discipline or several disciplines.

Note 2: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

9. Según UNE-ISO/IEC 27000:2012 - Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

Sistema de gestión:

Sistema para establecer la política, los procedimientos, las directrices y los recursos asociados para lograr los objetivos de la organización.

Sistema de gestión de la seguridad de la información (SGSI)

Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

10. La norma 27001 se ha revisado en 2013.

4.2. ISO/IEC 27002

11. La norma 27002 recoge un conjunto de puntos de control que pueden o deben tenerse en consideración dentro del sistema de gestión.

12. La norma 27002 no es certificable. Los controles descritos en la norma 27002 se recogen en un anexo normativo de la norma 27001, y deben ser tenidos en cuenta durante el proceso de certificación.

13. La norma 27002 se ha revisado en 2013.

4.3. EVIDENCIA DE CUMPLIMIENTO DE LA ISO 27001 Y EL ENS

14. La norma 27001 es una norma internacional certificable y de carácter voluntario para cualquier sistema de gestión de seguridad de la información. Su cumplimiento se evidencia *erga omnes* mediante una certificación, expedida por un auditor autorizado y previa auditoría con resultado satisfactorio.

15. Por su parte, el ENS es una disposición de carácter legal, de obligado cumplimiento para los sistemas de información del ámbito de aplicación de la Ley 11/2007. Su cumplimiento se evidencia *erga omnes* mediante una declaración de conformidad legal, previa auditoría con resultado satisfactorio.

16. Ambos mecanismos son distintos aunque, como se verá en los siguientes apartados, pueden desarrollarse acompasadamente.

17. Cuadro resumen

	ISO 27001	**Esquema Nacional de Seguridad (RD 3/2010)**

	ISO 27001	Esquema Nacional de Seguridad (RD 3/2010)
Ontología	Norma internacional de seguridad, sin rango legal.	Regulación legal de carácter estatal, perteneciente al ordenamiento jurídico español derivado de la Ley 11/2007.
Carácter	certificación voluntaria	cumplimiento obligatorio
Ámbito de aplicación	Para cualquier sistema de gestión de seguridad de la información.	Para los sistemas de información de las Administraciones públicas comprendidos en el ámbito de aplicación de la Ley 11/2007.
Modulación de las medidas	Según criterio del auditor	Regulado en función de los tipos de activos y los niveles de seguridad requeridos
Evidencia de cumplimiento o conformidad	Mediante certificación, expedida por un auditor autorizado, previa auditoría con resultado satisfactorio.	Mediante declaración de conformidad legal, previa auditoría con resultado satisfactorio.

5. CUMPLIMIENTO DEL ENS A TRAVÉS DE UNA CERTIFICACIÓN 27001

18. El ENS es una regulación nacional de obligado cumplimiento para las administraciones públicas y se enmarca dentro del ordenamiento jurídico derivado de la Ley 11/2007.

19. El ENS requiere un proceso de categorización (Anexo I) y una serie mínima de medidas de seguridad (Anexo II) que son obligatorias u opcionales en función de la categoría del sistema. La máxima libertad que se concede es que el organismo demuestre que ha implantado medidas alternativas que alcanzan el mismo nivel de protección.

20. El primer requisito para poder utilizar una certificación 27001 como soporte de cumplimiento del ENS es que el alcance de la certificación 27001 cubra lo exigido por la Ley 11/2007, tanto desde el punto de vista de los activos esenciales (Anexo I) como del equipamiento empleado[1].

21. Además, hay que destacar que el Anexo II modula los requisitos en función de la categoría del sistema de información, mientras que en una certificación 27001 el nivel de exigencia queda a la discreción del auditor y su criterio de qué es "control suficiente". En las tablas de esta guía se entenderá que el criterio del auditor 27001 se ajusta a la proporcionalidad establecida en el ENS para poder decir que un control 27002 está cubierto satisfactoriamente.

22. El ENS requiere un sistema de gestión en:

    - Anexo II (Medidas de seguridad), Marco operacional [op], Planificación [op.pl], Arquitectura de seguridad [op.pl.2]
    - Anexo III (Auditoría de la Seguridad), Objeto de la auditoría; si bien la auditoría se requiere sólo para los sistemas de categoría MEDIA o ALTA.

23. Las secciones siguientes relacionan las medidas de seguridad recogidas en el Anexo II con los controles de las normas 27001 y 27002 que pueden utilizarse como justificación

[1] Nótese que una certificación 27001 tiene el alcance que el cliente determine. Basta que quede claramente delimitado qué parte del sistema de gestión está siendo certificado.

de su cumplimiento, indicándose cuando sea el caso que el ENS requiere medidas adicionales a las indicadas en la norma 27002.

24. Hay que tener en cuenta que la estructuración de las medidas no es la misma en el ENS que en las normas 27001 y 27002. Algunos aspectos están contemplados en varias secciones. Cuando se cita una o más secciones de la 27002, nos referimos a la parte principal, conscientes de que otras secciones pudieran ser pertinentes para los detalles.

5.1. CUADRO RESUMEN

25. La siguiente tabla resume las diferencias que cabe esperar entre una certificación 27001 y el cumplimiento del ENS. Hay que hacer notar que la norma 27002 es más descriptiva que imperativa y que el detalle de lo que se haya implementado depende del buen criterio del certificador, por lo que un aspecto requerido por el ENS puede citarse en la sección correspondiente de la 27002 y sin embargo haberse obviado por las razones que sea. Por eso, siempre hay que verificar que se cumple lo que exige el ENS para las dimensiones y la categoría que corresponda.

26. La última columna estima el esfuerzo adicional que puede ser necesario para completar lo requerido por el ENS. Se emplean los siguientes niveles:

nivel	comentario
0	cubierto siempre conviene validar que se contemplan los detalles específicos del ENS
1	probablemente cubierto hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea marginal
2	probablemente se necesite completar hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea significativo
3	no cubierto son aspectos que no se cubren en los controles de la norma 27002 ni en los requisitos de la norma 27001, por lo que deberán ser objeto de una auditoría específica

MEDIDAS DE SEGURIDAD

org	Marco organizativo	
org.1	Política de seguridad	1
org.2	Normativa de seguridad	1
org.3	Procedimientos de seguridad	1
org.4	Proceso de autorización	1

op	Marco operacional

MEDIDAS DE SEGURIDAD

op.pl	Planificación	
op.pl.1	Análisis de riesgos	1
op.pl.2	Arquitectura de seguridad	1
op.pl.3	Adquisición de nuevos componentes	2
op.pl.4	Dimensionamiento / Gestión de capacidades	1
op.pl.5	Componentes certificados	3
op.acc	Control de acceso	
op.acc.1	Identificación	1
op.acc.2	Requisitos de acceso	1
op.acc.3	Segregación de funciones y tareas	0
op.acc.4	Proceso de gestión de derechos de acceso	1
op.acc.5	Mecanismo de autenticación	3
op.acc.6	Acceso local (local logon)	1
op.acc.7	Acceso remoto (remote login)	1
op.exp	Explotación	
op.exp.1	Inventario de activos	0
op.exp.2	Configuración de seguridad	3
op.exp.3	Gestión de la configuración	3
op.exp.4	Mantenimiento	1
op.exp.5	Gestión de cambios	1
op.exp.6	Protección frente a código dañino	0
op.exp.7	Gestión de incidencias	0
op.exp.8	Registro de la actividad de los usuarios	0
op.exp.9	Registro de la gestión de incidencias	0
op.exp.10	Protección de los registros de actividad	0
op.exp.11	Protección de claves criptográficas	1
op.ext	Servicios externos	
op.ext.1	Contratación y acuerdos de nivel de servicio	1
op.ext.2	Gestión diaria	1
op.ext.9	Medios alternativos	2
op.cont	Continuidad del servicio	
op.cont.1	Análisis de impacto	0
op.cont.2	Plan de continuidad	0
op.cont.3	Pruebas periódicas	0
op.mon	Monitorización del sistema	
op.mon.1	Detección de intrusión	2
op.mon.2	Sistema de métricas	1

mp	**Medidas de protección**	
mp.if	Protección de las instalaciones e infraestructuras	
mp.if.1	Áreas separadas y con control de acceso	0
mp.if.2	Identificación de las personas	0
mp.if.3	Acondicionamiento de los locales	0
mp.if.4	Energía eléctrica	0
mp.if.5	Protección frente a incendios	0
mp.if.6	Protección frente a inundaciones	0
mp.if.7	Registro de entrada y salida de equipamiento	0
mp.if.9	Instalaciones alternativas	1
mp.per	Gestión del personal	
mp.per.1	Caracterización del puesto de trabajo	0
mp.per.2	Deberes y obligaciones	0
mp.per.3	Concienciación	0

MEDIDAS DE SEGURIDAD		
mp.per.4	Formación	0
mp.per.9	Personal alternativo	1
mp.eq	Protección de los equipos	
mp.eq.1	Puesto de trabajo despejado	0
mp.eq.2	Bloqueo del puesto de trabajo	0
mp.eq.3	Protección de portátiles	1
mp.eq.9	Medios alternativos	1
mp.com	Protección de las comunicaciones	
mp.com.1	Perímetro seguro	2
mp.com.2	Protección de la confidencialidad	1
mp.com.3	Protección de la autenticicidad y de la integridad	1
mp.com.4	Segregación de redes	0
mp.com.9	Medios alternativos	1
mp.si	Protección de los soportes de información	
mp.si.1	Etiquetado	0
mp.si.2	Criptografía	1
mp.si.3	Custodia	0
mp.si.4	Transporte	0
mp.si.5	Borrado y destrucción	0
mp.sw	Protección de las aplicaciones informáticas	
mp.sw.1	Desarrollo	0
mp.sw.2	Aceptación y puesta en servicio	1
mp.info	Protección de la información	
mp.info.1	Datos de carácter personal	0
mp.info.2	Calificación de la información	0
mp.info.3	Cifrado de la información	2
mp.info.4	Firma electrónica	3
mp.info.5	Sellos de tiempo	3
mp.info.6	Limpieza de documentos	3
mp.info.9	Copias de seguridad (backup)	0
mp.s	Protección de los servicios	
mp.s.1	Protección del correo electrónico	0
mp.s.2	Protección de servicios y aplicaciones web	3
mp.s.8	Protección frente a la denegación de servicio	3
mp.s.9	Medios alternativos	2

5.2. ASPECTOS DE CONTINUIDAD

27. En el ENS la continuidad del servicio se cubre agregando varias medidas.

28. Unas medidas son de tipo operativo

[op.cont] Continuidad del servicio

[op.cont.1] Análisis de impacto

[op.cont.2] Plan de continuidad

[op.cont.3] Pruebas periódicas

29. Otras son medidas concretas sobre tipos concretos de activos

[mp.if.9] Instalaciones alternativas

[mp.per.9] Personal alternativo

[mp.eq.9] Medios alternativos (equipos)

[mp.com.9] Medios alternativos (comunicaciones)

[mp.info.9] Copias de seguridad (backup)

[mp.s.9] Medios alternativos (servicios)

30. La idea subyacente es que las normas 27001 y 27002 no son normas de continuidad, especialidad que se delega en las normas ISO/IEC 27031, ISO 22313 e ISO 22301.

31. Aunque los requisitos del ENS se pueden cumplir con los procesos de 27001 y los controles de 27002, conviene revisar los puntos citados con una visión holística.

6. [ORG] MARCO ORGANIZATIVO

6.1. [ORG.1] POLÍTICA DE SEGURIDAD

- 27001:2005
  - 4.2.1 – Establecimiento del SGSI
  - 5.1 – Compromiso de la dirección
- 27001:2013
  - 4 – Contexto de la organización
  - 5.2 – Política
  - 5.3 – Roles, responsabilidades y autoridad
- 27002:2005
  - 5.1.1 - Documento de política de seguridad de la información
  - 5.1.2 - Revisión de la política de seguridad de la información
  - 6.1.1 - Compromiso de la Dirección con la seguridad de la información
  - 6.1.2 - Coordinación de la seguridad de la información
  - 6.1.3 - Asignación de responsabilidades relativas a la seguridad de la información
  - 15.1.1 - Identificación de legislación aplicable
- 27002:2013
  - 6.1.1 - Roles y responsabilidades relativas a la seguridad de la información
  - 18.1.1 - Identificación de legislación aplicable y requisitos contractuales

32. El ENS distingue entre una Política de Seguridad [de la Información] y múltiple normativa de seguridad. La Política es un documento único, de alto nivel y de larga duración que establece los puntos fundamentales sobre los que pivota la seguridad de la organización. La normativa desarrolla aspectos puntuales, de forma dinámica, adaptándose a las circunstancias del momento.

33. La norma 27002 hablaba de política en su versión de 2005, pero sólo habla de políticas en su versión de 2013. ¿Qué ha pasado? Ha ocurrido que la Política se ha sacado de los controles de detalle de la 27002 y se ha llevado al marco de gestión de la 27001.

34. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

6.2. [ORG.2] NORMATIVA DE SEGURIDAD

- 27002:2005
  - 6.1.7 - Contacto con grupos de especial interés
  - 7.1.3 - Uso aceptable de los activos
  - 13.2.1 - Responsabilidades y procedimientos

    - 15.2.1 - Cumplimiento de las políticas y normas de seguridad
- 27002:2013
    - 5.1.1 - Políticas de seguridad de la información
    - 5.1.2 - Revisión de las políticas de seguridad de la información
    - 6.1.4 - Contacto con grupos de especial interés
    - 8.1.3 - Uso aceptable de los activos
    - 10.8.1 - Políticas y procedimientos de intercambio de información
    - 11.4.1 - Política de uso de los servicios en red
    - 13.2.1 - Políticas y procedimientos de transferencia de información
    - 15.1.1 - Política de seguridad de la información en las relaciones con proveedores
    - 16.1.1 - Responsabilidades y procedimientos
    - 18.2.2 - Cumplimiento de las políticas y normas de seguridad

35. En líneas generales, el término "normativa" en el ENS se corresponde con el término *"policies"* en la norma 27002. Las diferentes normas se encuentran distribuidas en los diferentes apartados de la norma 27002, cerca de sus elementos técnicos correspondientes.

36. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

6.3. [ORG.3] PROCEDIMIENTOS DE SEGURIDAD

- 27002:2005
    - 6.1.6 - Contacto con las autoridades
    - 10.1.1 - Documentación de los procedimientos de operación
    - 13.2.1 - Responsabilidades y procedimientos
    - 15.1.2 - Derechos de propiedad intelectual (IPR)
    - 15.2.2 - Comprobación del cumplimiento técnico
- 27002:2013
    - 6.1.3 - Contacto con las autoridades
    - 12.1.1 - Documentación de los procedimientos de operación
    - 13.2.1 - Políticas y procedimientos de transferencia de información
    - 16.1.1 - Responsabilidades y procedimientos
    - 18.1.2 - Derechos de propiedad intelectual (IPR)
    - 18.2.3 - Comprobación del cumplimiento técnico

37. Los diferentes procedimientos se encuentran distribuidos en los diferentes apartados de la norma 27002, cerca de sus elementos técnicos correspondientes.

38. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

6.4. [ORG.4] PROCESO DE AUTORIZACIÓN

- 27002:2005
    - 6.1.4 - Proceso de autorización de recursos para el tratamiento de la información

    - 6.2.3 - Tratamiento de la seguridad en contratos con terceros
    - 10.6.1 - Controles de red
    - 10.6.2 - Seguridad de los servicios de red
    - 10.7.1 - Gestión de soportes extraíbles
    - 10.7.3 - Procedimientos de manipulación de la información

    - 12.4.1 - Control del software en explotación
    - 12.5.3 - Restricciones a los cambios en los paquetes de software
- 27002:2013
    - 6.1.1 - Roles y responsabilidades relativas a la seguridad de la información
    - 6.2.1 - Política de dispositivos móviles
    - 8.2.3 - Manejo de activos
    - 8.3.1 - Gestión de soportes extraíbles
    - 12.5.1 - Instalación de software en sistemas operacionales
    - 12.6.2 - Restricciones a la instalación de software
    - 13.1.1 - Controles de red
    - 13.1.2 - Seguridad de los servicios de red
    - 14.2.4 - Restricciones a los cambios en los paquetes de software

39. El concepto de "proceso de autorización" ha desaparecido en la versión 2013 de la norma 27002. Parte de su contenido puede encontrarse en [6.1.1] y parte de las tareas de autorización se encuentran distribuidas distribuidos en los diferentes apartados de la norma 27002, cerca de sus elementos técnicos correspondientes. Con este criterio aparecen recogidos en la tabla anterior el conjunto de puntos a revisar.

40. En el ENS se requiere un proceso integrado de autorización. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7. [OP] MARCO OPERACIONAL

7.1. [OP.PL] PLANIFICACIÓN

7.1.1. [OP.PL.1] ANÁLISIS DE RIESGOS

- 27001:2005
    - 4.2.1 – Establecimiento del SGSI
    - 4.2.2 – Implementación y operación del SGSI
- 27001:2013
    - 6.1 – Acciones para abordar riesgos y oportunidades
    - 6.1.1 - General
    - 6.1.2 – Evaluación de riesgos
    - 6.1.3 – Tratamiento de los riesgos
    - 8.2 - Evaluación de riesgos
    - 8.3 – Tratamiento de los riesgos
- 27002:2005
    - 6.2.1 – Identificación de los riesgos derivados del acceso de terceros
    - 6.2.2 - Tratamiento de la seguridad en la relación con los clientes
    - 10.8.5 - Sistemas de información empresariales

41. El análisis de riesgos no es una medida de protección propiamente dicha, sino parte del proceso de gestión de riesgos que debe regir toda gestión de la seguridad.

42. Así se recoge en el ENS como principio básico (Capítulo II, Artículo 6).

43. Siguiendo un razonamiento análogo, el análisis y gestión de los riesgos aparece dentro de la norma de gestión, 27001.

44. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.1.2. [OP.PL.2] ARQUITECTURA DE SEGURIDAD

- 27002:2005
  - 7.1.1 - Inventario de activos
  - 7.1.2 - Propiedad de los activos
  - 10.6.1 - Controles de red
  - 10.7.4 - Seguridad de la documentación del sistema
  - 12.2.1 - Validación de los datos de entrada
  - 12.2.2 - Control del procesamiento interno
  - 12.2.3 – Integridad de los mensajes
  - 12.2.4 - Validación de los datos de salida
- 27002:2013
  - 8.1.1 - Inventario de activos
  - 8.1.2 - Propiedad de los activos
  - 13.1.1 - Controles de red
  - 14.2.5 - Principios para la ingeniería de sistemas seguros

45. El ENS centraliza en una medida organizativa lo que las normas 27001 y 27002 dejan disperso. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

46. En particular, el requisito del ENS de disponer de un sistema de gestión puede considerarse satisfecho si se dispone de un sistema PDCA (norma 27001:2005) o de un sistema de gestión certificado 27001 (versiones 2005 o 2013) siempre y cuando se cubra todo el alcance requerido por el ENS (ver Ley 11/2007).

7.1.3. [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES

- 27002:2005
  - 12.1.1 - Análisis y especificación de los requisitos de seguridad
- 27002:2013
  - 14.1.1 - Análisis y especificación de los requisitos de seguridad

47. El ENS centraliza en una medida organizativa lo que las normas 27001 y 27002 dejan disperso. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.1.4. [OP.PL.4] DIMENSIONAMIENTO / GESTIÓN DE CAPACIDADES

- 27002:2005
  - 10.3.1 - Gestión de capacidades
- 27002:2013
  - 12.1.3 - Gestión de capacidades

7.1.5. [OP.PL.5] COMPONENTES CERTIFICADOS

- 27002:2005
  - 12.1.1 - Análisis y especificación de los requisitos de seguridad
- 27002:2013
  - No se contempla

48. Este aspecto apenas se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.

7.2. [OP.ACC] CONTROL DE ACCESO

7.2.1. [OP.ACC.1] IDENTIFICACIÓN

- 27002:2005
  - 11.2.1 - Registro de usuario
  - 11.5.2 - Identificación y autenticación de usuario
- 27002:2013
  - 9.2.1 - Altas y bajas de usuarios

49. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.2.2. [OP.ACC.2] REQUISITOS DE ACCESO

- 27002:2005
  - 11.1.1 - Política de control de acceso
  - 11.5.4 - Uso de los recursos del sistema
  - 11.6.1 - Restricción del acceso a la información
  - 12.4.3 - Control de acceso al código fuente de los programas
  - 15.1.5 - Prevención del uso indebido de los recursos de tratamiento de la información
- 27002:2013
  - 9.1.1 - Política de control de acceso
  - 9.1.2 - Acceso a redes y servicios en red
  - 9.4.1 - Restricción del acceso a la información
  - 9.4.4 - Uso de los recursos del sistema con privilegios especiales
  - 9.4.5 - Control de acceso al código fuente de los programas

50. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.2.3. [OP.ACC.3] SEGREGACIÓN DE FUNCIONES Y TAREAS

- 27002:2005
  - 10.1.3 - Segregación de tareas
- 27002:2013
  - 6.1.2 - Separación de tareas

51. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.2.4. [OP.ACC.4] PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

- 27002:2005
  - 8.3.3 - Retirada de los derechos de acceso
  - 11.1.1 - Política de control de acceso
  - 11.2.2 - Gestión de privilegios
  - 11.2.4 - Revisión de derechos de acceso de usuario
- 27002:2013
  - 9.2.2 - Gestión de derechos de acceso de los usuarios
  - 9.2.3 - Gestión de derechos de acceso especiales
  - 9.2.5 - Revisión de derechos de acceso de usuario
  - 9.2.6 - Terminación o revisión de los privilegios de acceso

52. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.2.5. [OP.ACC.5] MECANISMO DE AUTENTICACIÓN

- 27002:2005
  - 11.2.3 - Gestión de contraseñas de usuario
  - 11.3.1 - Uso de contraseñas
  - 11.5.2 - Identificación y autenticación de usuario
  - 11.5.3 - Sistema de gestión de contraseñas
- 27002:2013
  - 9.2.4 - Gestión de la información secreta de autenticación de usuarios
  - 9.3.1 - Uso de la información secreta de autenticación
  - 9.4.3 - Gestión de las contraseñas de usuario

53. La norma 27002 prácticamente sólo trata de contraseñas y secretos compartidos en general.

54. El ENS establece varios modos de autenticación y modula su uso en función de la categoría del sistema. Hay que revisar que se cumple lo requerido por el ENS más allá de lo certificado en relación a la 27002.

7.2.6. [OP.ACC.6] ACCESO LOCAL (LOCAL LOGON)

- 27002:2005
  - 11.5.1 - Procedimientos seguros de inicio de sesión
- 27002:2013
  - 9.4.2 - Procedimientos seguros de inicio de sesión

55. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.2.7. [OP.ACC.7] ACCESO REMOTO (REMOTE LOGIN)

- 27002:2005
  - 11.4.2 - Autenticación de usuario para conexiones externas
- 27002:2013
  - 9.4.2 - Procedimientos seguros de inicio de sesión
  - 10.1.1 - Política de uso de los controles criptográficos
  - 13.1.1 - Controles de red
  - 13.1.2 - Seguridad de los servicios de red
  - 18.1.5 - Regulación de los controles criptográficos

56. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3. [OP.EXP] EXPLOTACIÓN

7.3.1. [OP.EXP.1] INVENTARIO DE ACTIVOS

- 27002:2005
  - 7.1.1 - Inventario de activos
  - 7.1.2 - Propiedad de los activos
- 27002:2013
  - 8.1.1 - Inventario de activos
  - 8.1.2 - Propiedad de los activos

57. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.2. [OP.EXP.2] CONFIGURACIÓN DE SEGURIDAD

- 27002:2005
  - No se contempla explícitamente
- 27002:2013
  - No se contempla explícitamente

58. Los requisitos del ENS no se contemplan explícitamente en las normas 27002. Conviene revisar que se satisfacen lo requerido en el ENS.

7.3.3. [OP.EXP.3] GESTIÓN DE LA CONFIGURACIÓN

- 27002:2005
  - No se contempla explícitamente
- 27002:2013
  - No se contempla explícitamente

59. Los requisitos del ENS no se contemplan explícitamente en las normas 27002. Conviene revisar que se satisfacen lo requerido en el ENS.

7.3.4. [OP.EXP.4] MANTENIMIENTO

- 27002:2005
  - 9.2.4 - Mantenimiento de los equipos
- 27002:2013
  - 11.2.4 - Mantenimiento de los equipos

60. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.5. [OP.EXP.5] GESTIÓN DE CAMBIOS

- 27002:2005
  - 10.1.2 - Gestión de cambios
  - 12.5.1 - Procedimientos de control de cambios
  - 12.5.2 - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
- 27002:2013
  - 12.1.2 - Gestión de cambios
  - 14.2.2 - Procedimientos de control de cambios en el sistema
  - 14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma

61. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.6. [OP.EXP.6] PROTECCIÓN FRENTE A CÓDIGO DAÑINO

- 27002:2005
  - 10.4.1 - Controles contra el código malicioso
  - 10.4.2 - Controles contra el código descargado en el cliente
- 27002:2013

- 12.2.1 - Controles contra el código malicioso

62. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.7. [OP.EXP.7] GESTIÓN DE INCIDENCIAS

- 27002:2005
  - 6.1.6 - Contacto con las autoridades
  - 6.1.7 - Contacto con grupos de especial interés
  - 10.10.5 - Registro de fallos
  - 13.1.1 - Notificación de eventos de seguridad de la información
  - 13.1.2 - Notificación de puntos débiles de seguridad
  - 13.2.2 - Aprendizaje de los incidentes de seguridad de la información
  - 13.2.3 - Recopilación de evidencias
- 27002:2013
  - 6.1.3 - Contacto con las autoridades
  - 6.1.4 - Contacto con grupos de especial interés
  - 16.1.2 - Notificación de eventos de seguridad de la información
  - 16.1.3 - Notificación de puntos débiles de seguridad
  - 16.1.4 - Evaluación y decisión respecto de los eventos de seguridad de la información
  - 16.1.5 - Respuesta a incidentes de seguridad de la información
  - 16.1.6 - Aprendizaje de los incidentes de seguridad de la información
  - 16.1.7 - Recopilación de evidencias

63. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.8. [OP.EXP.8] REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

- 27002:2005
  - 10.10.1 - Registros de auditoría
  - 10.10.2 - Supervisión del uso del sistema
  - 10.10.4 - Registros de administración y operación
- 27002:2013
  - 12.4.1 - Registro de eventos
  - 12.4.3 – Registros de administración y operación

64. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.9. [OP.EXP.9] REGISTRO DE LA GESTIÓN DE INCIDENCIAS

- 27002:2005
  - 13.2.3 - Recopilación de evidencias
- 27002:2013
  - 16.1.5 - Respuesta a incidentes de seguridad de la información
  - 16.1.7 - Recopilación de evidencias

65. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.10. [OP.EXP.10] PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

- 27002:2005

- 10.10.3 - Protección de la información de los registros
- 10.10.6 - Sincronización del reloj
- 15.3.2 - Protección de las herramientas de auditoría de los sistemas de información

- 27002:2013
  - 12.4.2 - Protección de la información de los registros
  - 12.4.4 – Sincronización del reloj

66. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.3.11. [OP.EXP.11] PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

- 27002:2005
  - 12.3.2 - Gestión de claves
- 27002:2013
  - 10.1.2 - Gestión de claves

67. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.4. [OP.EXT] SERVICIOS EXTERNOS

7.4.1. [OP.EXT.1] CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO

- 27002:2005
  - 6.2.3 - Tratamiento de la seguridad en contratos con terceros
  - 10.8.2 - Acuerdos de intercambio
- 27002:2013
  - 13.2.2 - Acuerdos de transferencia de información
  - 15.1.1 - Política de seguridad de la información en las relaciones con proveedores
  - 15.1.2 - Tratamiento de la seguridad en contratos con proveedores
  - 15.1.3 - Cadena de suministro de tecnologías de la información y comunicaciones

68. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.4.2. [OP.EXT.2] GESTIÓN DIARIA

- 27002:2005
  - 10.2.1 - Provisión de servicios
  - 10.2.2 - Supervisión y revisión de los servicios prestados por terceros
  - 10.2.3 - Gestión del cambio en los servicios prestados por terceros
- 27002:2013
  - 15.2.1 - Supervisión y revisión de los servicios prestados por terceros
  - 15.2.2 - Gestión del cambio en los servicios prestados por terceros

69. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.4.3. [OP.EXT.9] MEDIOS ALTERNATIVOS

- 27002:2005
  - No se contempla

- 27002:2013
  - No se contempla

70. Hay que revisar lo requerido en el ENS para satisfacer su cumplimiento. Aunque en las normas 27002 no se trata explícitamente, probablemente sea parte de los controles de continuidad de negocio.

7.5. [OP.CONT] CONTINUIDAD DEL SERVICIO

7.5.1. [OP.CONT.1] ANÁLISIS DE IMPACTO

- 27002:2005
  - 14.1.1 - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
  - 14.1.2 - Continuidad del negocio y evaluación de riesgos
- 27002:2013
  - 17.1.1 - Planificar la continuidad de la seguridad de la información

71. Hay que revisar lo requerido en el ENS para satisfacer su cumplimiento.

7.5.2. [OP.CONT.2] PLAN DE CONTINUIDAD

- 27002:2005
  - 14.1.3 - Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información
  - 14.1.4 - Marco de referencia para la planificación de la continuidad del negocio
- 27002:2013
  - 17.1.2 - Implementar la continuidad de la seguridad de la información

72. Hay que revisar lo requerido en el ENS para satisfacer su cumplimiento.

7.5.3. [OP.CONT.3] PRUEBAS PERIÓDICAS

- 27002:2005
  - 14.1.5 - Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
- 27002:2013
  - 17.1.3 - Verificar, revisar y evaluar la continuidad de la seguridad de la información

73. Hay que revisar lo requerido en el ENS para satisfacer su cumplimiento.

7.6. [OP.MON] MONITORIZACIÓN DEL SISTEMA

7.6.1. [OP.MON.1] DETECCIÓN DE INTRUSIÓN

- 27002:2005
  - No se contempla
- 27002:2013
  - No se contempla de forma explícita

74. La norma 27002:2013 menciona el sistema de detección en varios lugares, pareciendo que se da por supuesto:

12.4.1 – Registro de eventos
12.4.3 – Registros de administración y operación
13.1.2 – Seguridad de los servicios de red

75. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

7.6.2. [OP.MON.2] SISTEMA DE MÉTRICAS

- 27001:2005
  - 4.2.2 – Implementación y operación del SGSI
  - 4.2.3 – Monitorización y revisión del SGSI
- 27001:2013
  - 9 – Evaluación del desempeño
  - 9.1 – Monitorización, medidas, análisis y evaluación

76. El ENS exige varios puntos muy concretos. Hay que revisar si los requisitos del ENS se satisfacen, especialmente en lo relativo al Artículo 35.

8. [MP] MEDIDAS DE PROTECCIÓN

8.1. [MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

8.1.1. [MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO

- 27002:2005
  - 9.1.1 - Perímetro de seguridad física
  - 9.1.2 - Controles físicos de entrada
  - 9.1.3 - Seguridad de oficinas, despachos e instalaciones
  - 9.1.4 - Protección contra las amenazas externas y de origen ambiental
  - 9.1.5 - Trabajo en áreas seguras
  - 9.1.6 - Áreas de acceso público y de carga y descarga
  - 9.2.1 - Emplazamiento y protección de equipos
  - 11.6.2 - Aislamiento de sistemas sensibles
- 27002:2013
  - 11.1.1 - Perímetro de seguridad física
  - 11.1.2 - Controles físicos de entrada
  - 11.1.3 - Seguridad de oficinas, despachos e instalaciones
  - 11.1.4 - Protección contra las amenazas externas y de origen ambiental
  - 11.1.5 - Trabajo en áreas seguras
  - 11.1.6 - Áreas de carga y descarga
  - 11.2.1 - Emplazamiento y protección de equipos

77. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.1.2. [MP.IF.2] IDENTIFICACIÓN DE LAS PERSONAS

- 27002:2005
  - 9.1.2 - Controles físicos de entrada

- 27002:2013
  - 11.1.2 - Controles físicos de entrada

78. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.3. [MP.IF.3] ACONDICIONAMIENTO DE LOS LOCALES

- 27002:2005
  - 9.2.2 - Instalaciones de suministro
  - 9.2.3 - Seguridad del cableado
- 27002:2013
  - 11.2.2 - Instalaciones de suministro
  - 11.2.3 - Seguridad del cableado

79. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.4. [MP.IF.4] ENERGÍA ELÉCTRICA

- 27002:2005
  - 9.2.2 - Instalaciones de suministro
- 27002:2013
  - 11.2.2 - Instalaciones de suministro

80. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.5. [MP.IF.5] PROTECCIÓN FRENTE A INCENDIOS

- 27002:2005
  - 9.1.4 - Protección contra las amenazas externas y de origen ambiental
- 27002:2013
  - 11.1.4 - Protección contra las amenazas externas y de origen ambiental

81. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.6. [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES

- 27002:2005
  - 9.1.4 - Protección contra las amenazas externas y de origen ambiental
- 27002:2013
  - 11.1.4 - Protección contra las amenazas externas y de origen ambiental

82. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.7. [MP.IF.7] REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO

- 27002:2005
  - 9.2.5 - Seguridad de los equipos fuera de las instalaciones
  - 9.2.7 - Retirada de materiales propiedad de la empresa
- 27002:2013
  - 11.2.5 - Retirada de materiales propiedad de la empresa
  - 11.2.6 - Seguridad de los equipos fuera de las instalaciones

83. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.1.8. [MP.IF.9] INSTALACIONES ALTERNATIVAS

- 27002:2005
  - No se contempla
- 27002:2013
  - 17.2.1 - Disponibilidad de los medios de procesamiento de información

84. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.2. [MP.PER] GESTIÓN DEL PERSONAL

8.2.1. [MP.PER.1] CARACTERIZACIÓN DEL PUESTO DE TRABAJO

- 27002:2005
  - 8.1.1 - Funciones y responsabilidades
  - 8.1.2 - Investigación de antecedentes
- 27002:2013
  - 7.1.1 - Investigación de antecedentes

85. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.2.2. [MP.PER.2] DEBERES Y OBLIGACIONES

- 27002:2005
  - 6.1.5 - Acuerdos de confidencialidad
  - 8.1.3 - Términos y condiciones de contratación
  - 8.2.1 - Responsabilidades de la Dirección
  - 8.2.3 - Proceso disciplinario
  - 8.3.1 - Responsabilidad del cese o cambio
  - 8.3.2 – Devolución de activos
- 27002:2013
  - 7.1.2 - Términos y condiciones de contratación
  - 7.2.1 - Responsabilidades de la Dirección
  - 7.2.3 - Proceso disciplinario
  - 7.3.1 - Terminación o cambio de responsabilidades laborales
  - 8.1.4 - Devolución de activos
  - 13.2.4 - Acuerdos de confidencialidad o no divulgación

86. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.2.3. [MP.PER.3] CONCIENCIACIÓN

- 27001:2005
  - 4.2.2 – Implementación y operación del SGSI
  - 5.2.2 – Formación, concienciación y competencias
- 27001:2013
  - 7.3 - Concienciación
- 27002:2005
  - 8.2.2 - Concienciación, formación y capacitación en seguridad de la información

- 27002:2013
  - 7.2.2 - Concienciación, formación y capacitación en seguridad de la información

87. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.2.4. [MP.PER.4] FORMACIÓN

- 27001:2005
  - 4.2.2 – Implementación y operación del SGSI
  - 5.2.2 – Formación, concienciación y competencias
- 27001:2013
  - 7.2 - Competencias
- 27002:2005
  - 8.2.2 - Concienciación, formación y capacitación en seguridad de la información
- 27002:2013
  - 7.2.2 - Concienciación, formación y capacitación en seguridad de la información

88. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.2.5. [MP.PER.9] PERSONAL ALTERNATIVO

- 27002:2005
  - No se contempla
- 27002:2013
  - 17.2.1 - Disponibilidad de los medios de procesamiento de información

89. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.3. [MP.EQ] PROTECCIÓN DE LOS EQUIPOS

8.3.1. [MP.EQ.1] PUESTO DE TRABAJO DESPEJADO

- 27002:2005
  - 11.3.3 - Política de puesto de trabajo despejado y pantalla limpia
- 27002:2013
  - 11.2.9 - Política de puesto de trabajo despejado y pantalla limpia

90. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.3.2. [MP.EQ.2] BLOQUEO DEL PUESTO DE TRABAJO

- 27002:2005
  - 11.3.2 - Equipo de usuario desatendido
  - 11.5.5 - Desconexión automática de sesión
  - 11.5.6 - Limitación del tiempo de conexión
- 27002:2013
  - 11.2.8 - Equipo de usuario desatendido

91. Hay que revisar si los requisitos del ENS se satisfacen.

8.3.3. [MP.EQ.3] PROTECCIÓN DE EQUIPOS PORTÁTILES

- 27002:2005
  - 11.7.1 - Ordenadores portátiles y comunicaciones móviles
- 27002:2013
  - 6.2.1 - Política de dispositivos móviles

92. Hay que revisar si los requisitos del ENS se satisfacen.

8.3.4. [MP.EQ.9] MEDIOS ALTERNATIVOS

- 27002:2005
  - No se contempla
- 27002:2013
  - 17.2.1 - Disponibilidad de los medios de procesamiento de información

93. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.4. [MP.COM] PROTECCIÓN DE LAS COMUNICACIONES

8.4.1. [MP.COM.1] PERÍMETRO SEGURO

- 27002:2005
  - 10.6.2 - Seguridad de los servicios de red
  - 11.4.6 - Control de la conexión a la red
  - 11.4.7 - Control de encaminamiento (routing) de red
- 27002:2013
  - 13.1.2 - Seguridad de los servicios de red

94. El ENS exige varios puntos muy concretos. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.4.2. [MP.COM.2] PROTECCIÓN DE LA CONFIDENCIALIDAD

- 27002:2005
  - 10.6.1 - Controles de red
  - 10.6.2 - Seguridad de los servicios de red
  - 15.1.6 - Regulación de los controles criptográficos
- 27002:2013
  - 10.1.1 - Política de uso de los controles criptográficos
  - 13.1.1 - Controles de red
  - 13.1.2 - Seguridad de los servicios de red
  - 14.1.2 - Aseguramiento de servicios y aplicaciones en redes públicas
  - 18.1.5 - Regulación de los controles criptográficos

95. El ENS exige varios puntos muy concretos. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.4.3. [MP.COM.3] PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

- 27002:2005
  - 10.6.1 - Controles de red
  - 10.6.2 - Seguridad de los servicios de red
  - 11.4.2 - Autenticación de usuario para conexiones externas
  - 11.4.3 - Identificación de los equipos en las redes
  - 11.4.4 - Diagnóstico remoto y protección de los puertos de configuración
- 27002:2013
  - 10.1.1 - Política de uso de los controles criptográficos
  - 13.1.1 - Controles de red
  - 13.1.2 - Seguridad de los servicios de red
  - 14.1.2 - Aseguramiento de servicios y aplicaciones en redes públicas

96. El ENS exige varios puntos muy concretos. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.4.4. [MP.COM.4] SEGREGACIÓN DE REDES

- 27002:2005
  - 11.4.5 - Segregación de las redes
- 27002:2013
  - 13.1.3 - Segregación de redes

97. Hay que revisar si los requisitos del ENS se satisfacen.

8.4.5. [MP.COM.9] MEDIOS ALTERNATIVOS

- 27002:2005
  - No se contempla
- 27002:2013
  - 17.2.1 - Disponibilidad de los medios de procesamiento de información

98. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

8.5. [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

8.5.1. [MP.SI.1] ETIQUETADO

- 27002:2005
  - 7.2.2 - Etiquetado y manipulado de la información
  - 10.7.1 - Gestión de soportes extraíbles
- 27002:2013
  - 8.2.2 - Marcado de la información
  - 8.3.1 - Gestión de soportes extraíbles

99. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.5.2. [MP.SI.2] CRIPTOGRAFÍA

- 27002:2005
  - 10.7.1 - Gestión de soportes extraíbles

- 12.3.1 - Política de uso de los controles criptográficos
- 27002:2013
  - 8.3.1 - Gestión de soportes extraíbles
  - 10.1.1 - Política de uso de los controles criptográficos

100. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.5.3. [MP.SI.3] CUSTODIA

- 27002:2005
  - 10.7.1 - Gestión de soportes extraíbles
- 27002:2013
  - 8.3.1 - Gestión de soportes extraíbles

101. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.5.4. [MP.SI.4] TRANSPORTE

- 27002:2005
  - 10.8.3 - Soportes físicos en tránsito
- 27002:2013
  - 8.3.3 - Transferencia de soportes físicos
  - 11.2.5 - Retirada de materiales propiedad de la empresa

102. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.5.5. [MP.SI.5] BORRADO Y DESTRUCCIÓN

- 27002:2005
  - 9.2.6 - Reutilización o retirada segura de equipos
  - 10.7.2 - Retirada de soportes
- 27002:2013
  - 8.3.2 - Retirada de soportes
  - 11.2.7 - Reutilización o retirada segura de equipos

103. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.6. [MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS (SW)

8.6.1. [MP.SW.1] DESARROLLO DE APLICACIONES

- 27002:2005
  - 10.1.4 - Separación de los recursos de desarrollo, prueba y operación
  - 12.4.2 - Protección de los datos de prueba del sistema
  - 12.4.3 – Control de acceso al código fuente de los programas
  - 12.5.5 - Externalización del desarrollo de software
- 27002:2013
  - 9.4.5 - Control de acceso al código fuente de los programas
  - 12.1.4 - Separación de los entornos de desarrollo, prueba y operación
  - 14.2.1 - Política de desarrollo seguro
  - 14.2.5 - Principios para la ingeniería de sistemas seguros
  - 14.2.6 - Entorno de desarrollo seguro

- 14.2.7 - Externalización del desarrollo de software
- 14.3.1 - Protección de los datos de prueba

104. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.6.2. [MP.SW.2] ACEPTACIÓN Y PUESTA EN SERVICIO

- 27002:2005
  - 10.1.4 - Separación de los recursos de desarrollo, prueba y operación
  - 10.3.2 - Aceptación del sistema
  - 12.4.1 - Control del software en explotación
  - 12.4.2 - Protección de los datos de prueba del sistema
  - 12.5.5 - Externalización del desarrollo de software
  - 12.6.1 - Control de las vulnerabilidades técnicas
- 27002:2013
  - 12.1.4 - Separación de los entornos de desarrollo, prueba y operación
  - 12.5.1 - Instalación de software en sistemas operacionales
  - 12.6.1 - Control de las vulnerabilidades técnicas
  - 14.2.8 - Pruebas de seguridad del sistema
  - 14.2.9 - Pruebas de aceptación del sistema
  - 14.3.1 - Protección de los datos de prueba
  - 14.2.7 - Externalización del desarrollo de software

105. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.7. [MP.INFO] PROTECCIÓN DE LA INFORMACIÓN

8.7.1. [MP.INFO.1] DATOS DE CARÁCTER PERSONAL

- 27002:2005
  - 15.1.4 - Protección de datos e información de carácter personal
- 27002:2013
  - 18.1.4 - Protección de datos e información de carácter personal

106. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.7.2. [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN

- 27002:2005
  - 7.1.2 - Propiedad de los activos
  - 7.2.1 - Directrices de clasificación
- 27002:2013
  - 8.1.2 - Propiedad de los activos
  - 8.2.1 - Clasificación de la información

107. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.7.3. [MP.INFO.3] CIFRADO DE LA INFORMACIÓN

- 27002:2005

    - 12.3.1 - Política de uso de los controles criptográficos
    - 10.6.1 - Controles de red
    - 10.6.2 - Seguridad de los servicios de red
    - 10.8.3 - Soportes físicos en tránsito
    - 10.9.2 - Transacciones en línea
    - 15.1.6 - Regulación de los controles criptográficos
- 27002:2013
    - 10.1.1 - Política de uso de los controles criptográficos
    - 8.3.3 - Transferencia de soportes físicos
    - 13.1.1 - Controles de red
    - 13.1.2 - Seguridad de los servicios de red
    - 18.1.5 - Regulación de los controles criptográficos

108. Los requisitos del ENS se tratan de forma dispersa en las normas 27002. Deberá revisarse que se satisface lo requerido en el ENS.

8.7.4. [MP.INFO.4] FIRMA ELECTRÓNICA

- 27002:2005
    - 10.9.2 - Transacciones en línea
    - 12.3.1 - Política de uso de los controles criptográficos
    - 15.1.6 - Regulación de los controles criptográficos
- 27002:2013
    - 10.1.1 - Política de uso de los controles criptográficos
    - 14.1.3 - Protección de las transacciones
    - 18.1.5 - Regulación de los controles criptográficos

109. En el ENS estos aspectos están muy relacionados con las garantías debidas en el proceso administrativo y la legislación sobre firma electrónica. Deberá cubrirse específicamente lo requerido por el ENS.

8.7.5. [MP.INFO.5] SELLOS DE TIEMPO

- 27002:2005
    - 10.9.2 - Transacciones en línea
- 27002:2013
    - 14.1.3 - Protección de las transacciones

110. Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.

8.7.6. [MP.INFO.6] LIMPIEZA DE DOCUMENTOS

- 27002:2005
    - 12.5.4 - Fugas de información
- 27002:2013
    - No se contempla

111. Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.

8.7.7. [MP.INFO.9] COPIAS DE SEGURIDAD (BACKUP)

- 27002:2005
  - 10.5.1 - Copias de seguridad de la información
- 27002:2013
  - 12.3.1 - Copias de seguridad de la información

112. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.8. [MP.S] PROTECCIÓN DE LOS SERVICIOS

8.8.1. [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

- 27002:2005
  - 10.8.4 - Mensajería electrónica
- 27002:2013
  - 13.2.3 - Mensajería electrónica

113. Conviene repasar los requisitos detallados en el ENS para satisfacer su cumplimiento.

8.8.2. [MP.S.2] PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB

- 27002:2005
  - No se contempla
- 27002:2013
  - No se contempla

114. Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.

8.8.3. [MP.S.8] PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

- 27002:2005
  - 10.3.1 - Gestión de capacidades
- 27002:2013
  - 12.1.3 – Gestión de capacidades

115. Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.

8.8.4. [MP.S.9] MEDIOS ALTERNATIVOS

- 27002:2005
  - No se contempla
- 27002:2013
  - 17.2.1 - Disponibilidad de los medios de procesamiento de información

116. Hay que revisar si los requisitos del ENS se satisfacen, especialmente si se ha empleado la versión de 2005.

9. OTROS CONTROLES

117. Algunos controles de la norma 27002 no tienen reflejo en el ENS.

[27002:2013] 6.1.5 - Seguridad de la información en la gestión de proyectos

Se refiere la norma a que todos los proyectos acometidos por la organización tengan en cuenta la seguridad de la información. Puede decirse que en el ENS este aspecto aparece de forma implícita al ser obligatoria su aplicación a toda información y servicio relacionado con la Ley 11/2007.

[27002:2013] 6.2.2 – Teletrabajo

[27002:2005] 11.7.2 – Teletrabajo

No se cubre explícitamente por el ENS; pero teniendo en cuenta que la información debe estar protegida en todo momento lugar y forma, se aplicarán las medidas correspondientes en cuanto a personas, instalaciones y medios TIC.

[27002:2013] 12.7.1 - Controles de auditoría de los sistemas de información

[27002:2005] 15.3.1 - Controles de auditoría de los sistemas de información

Se refiere la norma a cómo realizar las tareas de auditoría garantizando que el acceso del auditor no merme la confidencialidad, integridad y disponibilidad requerida por el sistema.

[27002:2013] 18.1.3 - Protección de los documentos de la organización

[27002:2005] 15.1.3 - Protección de los documentos de la organización

Se refiere la norma a los documentos que soportan la actividad de la Organización, lo que en una Administración Pública podemos entender como toda información cuya integridad y disponibilidad debe garantizarse a largo plazo.

El ENS entiende que esta es parte de la información que debe protegerse dentro del mandato de la Ley 11/2007 y por tanto se aplicarán las medidas de seguridad oportunas.

[27002:2013] 18.2.1 - Revisión independiente de la seguridad de la información

[27002:2005] 6.1.8 - Revisión independiente de la seguridad de la información

Véase Anexo III – Auditoría de la Seguridad.

Desarrollado en la guía CCN-STIC: 802 – Guía de Auditoría.

[27002:2005] 10.9.1 - Comercio electrónico

[27002:2005] 10.9.3 - Información públicamente disponible

Se refiere la norma a garantías contractuales a tener en cuenta al utilizar Internet como soporte comercial, sea para publicar documentos o para realizar transacciones, protegiendo su confidencialidad, integridad, autenticidad y trazabilidad.

Aunque la administración electrónica no es lo mismo que el comercio electrónico, es cierto que toda la actividad electrónica debe estar adecuadamente fundamentada en legislación de

obligado cumplimiento y que múltiples medidas del ENS permiten proteger dicha información cuando se utiliza la red como vehículo de interacción con los administrados.

Nótese que estos controles se han eliminado de la versión 2013, aunque los aspectos más técnicos se recogen en "14.1.2 - Aseguramiento de servicios y aplicaciones en redes públicas".

ANEXO A. GLOSARIO Y ABREVIATURAS

Ver guía CCN-STIC 800 Glosario de Términos y Abreviaturas del ENS.

ANEXO B. REFERENCIAS

- ENS
  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. BOE de 29 de enero de 2010.
  https://www.ccn-cert.cni.es/publico/ens/ens/index.html
- ISO/IEC 27000:2012 (rev. 2013)
  Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2005 (rev. 2013)
  Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2005 (rev. 2013)
  Information technology – Security techniques – Code of practice for information security management
- Ley 11:2007
  LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- CCN-STIC. Serie 800. Esquema Nacional de Seguridad.