

Guía de Seguridad de las TIC CCN-STIC 808

Verificación del cumplimiento del ENS



Junio 2017

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-033-0

Fecha de Edición: junio de 2017

AENOR, AUDERTIS, BDO y NUNSYS han colaborado en la revisión del presente documento y sus anexos y José Antonio Mañas y Carlos Galán han participado en su realización y modificación.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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 (CNI), 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 (CCN) 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.

El 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 (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 (STIC) 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.

Junio de 2017



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	5
2. OBJETO	6
3. ALCANCE.....	6
4. CÓMO UTILIZAR ESTA GUÍA.....	6
5. VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS	7
5.1 CUMPLIMIENTO DE ARTÍCULOS DEL ENS	9
5.2 ANEXO II MEDIDAS DE SEGURIDAD	14
5.2.1 MARCO ORGANIZATIVO	14
5.2.2 MARCO OPERACIONAL.....	25
5.2.3 MEDIDAS DE PROTECCIÓN	98
ANEXO I. DEFINICIÓN DE TÉRMINOS.....	170
ANEXO II. PLANTILLA DE INFORME DE AUDITORÍA	171
ANEXO III. TABLA DE VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS	175

1. INTRODUCCIÓN

1. Esta guía de auditoría del Esquema Nacional de Seguridad se encuadra dentro de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de la Seguridad) del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre, según lo previsto en el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información¹.
2. Esta guía será de uso para los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación según dispone el artículo 3 del Real Decreto 3/2010 de 8 de enero, del ENS, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
3. Los sistemas de categoría Básica:
 - Requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada dos años o cuando se produzcan modificaciones sustanciales en el sistema.
 - La autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.
 - Un sistema de categoría Básica se puede someter igualmente a una auditoría formal de certificación de la conformidad, siendo esta posibilidad siempre la deseable.
4. Los sistemas de categoría Media o Alta:
 - Precisarán de una auditoría formal para su certificación de la conformidad al menos cada dos años, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria.
 - Se entiende por auditoría formal la realizada por una entidad de certificación acreditada por ENAC o por aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad de acuerdo con la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de

¹ Por Resolución del Secretario de Estado de Función Pública (pendiente de publicación)

Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

- Deberá desarrollarse con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.
5. El RD 3/2010 está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información pero, es posible, que también sean aplicables otros requisitos legales² que el auditor debe tener en cuenta (en la medida que no impliquen un nivel inferior de seguridad requerido por el RD 3/2010), o bien que prescriben la realización de auditorías de las medidas de seguridad pero con objetivos o bien alcances diferentes.
 6. Estos requisitos de auditoría adicionales no están dentro del objeto y alcance de la auditoría requerida por el RD 3/2010. Sin embargo, en determinadas situaciones, la necesidad de una mayor eficiencia en la aplicación de los recursos (tanto del equipo auditor como del personal involucrado en el sistema de información auditado) puede aconsejar la realización conjunta de estas auditorías. Aún en estos casos se deben aplicar las premisas mínimas de esta guía para la realización de estas auditorías.
 7. La presente guía viene a complementar a la guía “CCN-STIC-802 Esquema Nacional de Seguridad – Guía de auditoría”.

2. OBJETO

8. El objeto de esta guía es que sirva tanto de itinerario, como de registro, a aquella persona designada como auditor de los requisitos del Esquema Nacional de Seguridad para un sistema.

3. ALCANCE

9. Esta guía es de aplicación a cualquier entidad que deba cumplir con los preceptos del Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero), con independencia de su naturaleza, dimensión o categoría de sus sistemas.

4. CÓMO UTILIZAR ESTA GUÍA

10. El formato de esta guía pretende que sea una herramienta para el trabajo de campo. Dado que algún espacio reservado para las anotaciones pudiera resultar insuficiente, recomendamos al auditor acompañarse de los medios que necesite para poder anotar o recopilar las evidencias que considere necesarias.
11. En el apartado “Requisito” se especifica el requisito o requisitos que existen para cada medida de seguridad. Cada uno va precedido de una casilla () para marcar:

² Es el caso, por ejemplo, de que el sistema trate datos de carácter personal y haya que aplicar la normativa correspondiente

- a. si lo cumple.
- b. si no lo cumple.

con objeto de elaborar el informe de auditoría para dictaminar sobre el grado de cumplimiento del RD 3/2010.

12. Para conseguir una uniformidad a la hora de realizar la auditoría por parte de diferentes auditores, se proporciona una evidencia modelo que el auditor podrá requerir, aunque esta puede variar en función de las circunstancias.
13. En el apartado “Aplicabilidad – Auditado” se divide en:
 - a. “Aplica”: Marque “Sí” en caso de que la medida de seguridad sea de aplicación al sistema que está auditando. En caso contrario marque “No”. Algunas medidas no permiten marcar “No”, ello se debe a que son medidas que siempre se deben aplicar.
 - b. “Lo audito”: Marque “Sí” en caso de que haya auditado la medida de seguridad, con independencia de que sea de aplicación o no la medida de seguridad (si no es de aplicación la medida de seguridad, la auditoría debe verificar en este caso que el motivo de que no aplique sigue siendo vigente). No es imprescindible auditar todas las medidas de seguridad cada vez que se lleva a cabo una auditoría (consultar qué medidas debe auditar obligatoriamente en la guía “CCN-STIC-802 Esquema Nacional de Seguridad – Guía de Auditoría por lo que deberá marcar “No” si la ha omitido. Aquellas medidas que deben auditarse siempre no permiten marcar “No”).
14. El apartado “Comentarios” se divide en:
 - a. Documento: Puede ser la política, normativa o procedimiento (si es que se encuentra documentada) que documenta cómo está o debe estar implantada la medida de seguridad.
 - b. Muestreo: Permite anotar qué activo o elemento de muestra ha analizado. Por ejemplo, a la hora de verificar la identificación de los usuarios, anotar qué repositorio de usuarios ha revisado.
 - c. Observaciones auditoría: Permite que el auditor tome notas sobre la medida de seguridad, como la persona a la que ha entrevistado, un resumen de lo que le ha contestado, etc.

5. VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS

15. Este apartado se divide en cumplimiento de varios artículos del ENS que se consideran relevante destacarlos y medidas de seguridad del Anexo II, que a su vez se presentan dentro de los grupos en que se clasifican, es decir, marco organizativo, marco operacional y medidas de protección.
16. Por cada uno de los componentes de los anteriores grupos se indicará cómo verificar el correcto cumplimiento con las medidas indicadas en el ENS, haciendo

referencia a aquellas guías que proporcionan información sobre las medidas a aplicar en cada caso.

17. Cabe destacar que las propuestas de verificación son a modo de ejemplo, el auditor deberá adaptar la pregunta al entorno en el que se encuentre y opere el sistema.

5.1 CUMPLIMIENTO DE ARTÍCULOS DEL ENS

RD 3/2010	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
Art. 29	INSTRUCCIONES TÉCNICAS DE SEGURIDAD Y GUÍAS DE SEGURIDAD			
	Básica	<p><input type="checkbox"/> 1.- ¿Conoce y mantiene actualizada la relación de las instrucciones técnicas de seguridad y guías de seguridad que le son de aplicación a su sistema? ¿Dispone de una copia de dichos documentos?</p> <p><i>Evidencia: Dispone de una copia de las ITS y guías que le son de aplicación a su sistema en forma impresa o guardaba en formato electrónico. Conoce donde actualizar la relación y obtener copia de los documentos (p. ej.: portal del CCN: www.ccn-cert.cni.es)</i></p> <p>Consultar ITS y guías: ITS Informe del Estado de la Seguridad ITS de conformidad con el Esquema Nacional de Seguridad. <i>Pendiente de publicar:</i> <i>ITS de auditoría de la seguridad de los sistemas de información</i> <i>ITS de notificación de incidentes de seguridad</i></p>	<p>Aplica: <input type="checkbox"/> Sí</p> <p>Lo audito: <input type="checkbox"/> Sí</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

RD 3/2010	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
Art.35	INFORME DEL ESTADO DE LA SEGURIDAD			
	Básica	<input type="checkbox"/> 1.- ¿Cumplimenta la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad regulada por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas <i>Evidencia: Dispone de acceso a la herramienta INES del portal del CCN y cuenta con una copia del informe individual generado en la última campaña. Dicho informe se encuentra en forma impresa o guardado en formato electrónico.</i> Consultar guías: CCN-STIC-824 Esquema Nacional de Seguridad. Informe del estado de seguridad CCN-STIC-844 INES. Informe Nacional del Estado de la Seguridad. Manual de usuario y Anexos. ITS Informe del Estado de la Seguridad	Aplica: <input type="checkbox"/> Sí Lo audito: <input type="checkbox"/> Sí	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
Art.36	CAPACIDAD DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
	Básica	<input type="checkbox"/> 1.- ¿Notifica al CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team) aquellos incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del RD 3/2010?	Aplica: <input type="checkbox"/> Sí Lo audito: <input type="checkbox"/> Sí	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:

RD 3/2010	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Dispone de registros que muestren la interacción con el CCN-CERT en caso de incidentes de impacto significativo (alto, muy alto o crítico) o alternatively utiliza la herramienta LUCIA de gestión de ciberincidentes.</i></p> <p><i>Además, dispone de una copia de las ITS y guías que le son de aplicación a su sistema en forma impresa o guardaba en formato electrónico. Conoce donde actualizar la relación y obtener copia de los documentos (p. ej. portal del CCN: www.ccn-cert.cni.es)</i></p> <p>Consultar guías: CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de ciberincidentes CCN-STIC-845A LUCIA. Manual de usuario CCN-STIC-845B LUCIA. Manual de usuario con Sistema de Alerta Temprana (SAT) CCN-STIC-845C LUCIA. Manual de instalación. Organismo CCN-STIC-845D LUCIA. Manual de administrador</p> <p>Pendiente de publicar: ITS de auditoría de la seguridad de los sistemas de información ITS de notificación de incidentes de seguridad</p>		<p><u>Observaciones auditoría:</u></p>

RD 3/2010	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
<p>ART 43 ART 44</p>	<p>CATEGORÍAS Y FACULTADES Básica</p>	<p><input type="checkbox"/> 1.- ¿Existe un proceso formal para la determinación de la categoría del sistema de información en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad siguiendo el procedimiento establecido en el Anexo I del RD 3/2010?</p> <p><i>Evidencia: Se dispone de un documento en el que se analiza la valoración que cada responsable de información o servicio, facultado para ello, realiza de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios. Dicha valoración se efectúa atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones, el respeto a la legalidad y los derechos de los ciudadanos siguiendo el procedimiento del Anexo I.</i></p> <p><i>Respecto a las facultades para realizar la valoración y determinar la categoría del sistema</i></p> <p><input type="checkbox"/> 1.1.- ¿El responsable de cada información o servicio dentro del ámbito de su actividad ejerce las facultades para efectuar las valoraciones a las que se refiere el artículo 43, así como su modificación posterior?</p> <p><i>Evidencia: Existe evidencia documental de que la facultad para la</i></p>	<p>Aplica: <input type="checkbox"/> Sí</p> <p>Lo audito: <input type="checkbox"/> Sí</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <p><u>Observaciones auditoría:</u></p>

RD 3/2010	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>valoración de las dimensiones de seguridad de cada información o servicio se aprueba por su responsable. El documento de valoración está aprobado por el responsable de cada información o servicio dentro del ámbito de su actividad.</i></p> <p><input type="checkbox"/> 1.2.- ¿El responsable del sistema ejerce las facultades para efectuar la valoración del sistema a que se refiere el artículo 43 así como su modificación posterior?</p> <p><i>Evidencia: Existe evidencia documental de que la facultad para determinar la valoración del sistema ha sido ejercida por el responsable del sistema.</i></p> <p>Consultar ITS y guías:</p> <p>CCN-STIC 802 Esquema Nacional de Seguridad. Guía de auditoría</p> <p>CCN-STIC 803 Esquema Nacional de Seguridad. Valoración de sistemas</p> <p>CCN-STIC 804 Esquema Nacional de Seguridad. Guía de implantación</p> <p>ITS Informe del Estado de la Seguridad</p> <p>ITS de conformidad con el Esquema Nacional de Seguridad.</p> <p><i>Pendiente de publicar:</i></p> <p><i>ITS de auditoría de la seguridad de los sistemas de información</i></p> <p><i>ITS de notificación de incidentes de seguridad</i></p>		

5.2 ANEXO II MEDIDAS DE SEGURIDAD

5.2.1 MARCO ORGANIZATIVO

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
org	MARCO ORGANIZATIVO			
org.1	Política de seguridad			
	Básica	<input type="checkbox"/> 1.- ¿Dispone de una política de seguridad escrita? <i>Evidencia: La política de seguridad está impresa o guardada en formato electrónico.</i> Respecto a dicha política de seguridad: <input type="checkbox"/> 1.1.- ¿Ha sido aprobada por el órgano superior competente (de acuerdo a lo establecido en el artículo 11 del RD 3/2010)? <i>Evidencia: La política de seguridad fue redactada por un órgano superior o ha sido aprobada (mediante algún registro escrito o electrónico) por el mismo. En caso de que el órgano superior no disponga de política de seguridad, deberá tener una política de seguridad elaborada por el responsable STIC y aprobada por el Comité STIC y el Comité de Seguridad Corporativa. Además, existe un procedimiento de revisión y firma regular (este último si no existe una política de seguridad redactada por un órgano superior).</i>	Aplica: <input type="checkbox"/> Sí Lo audito: <input type="checkbox"/> Sí	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.2.- ¿Precisa los objetivos y misión de la organización? <i>Evidencia: Dentro de la política se indica cuáles son los objetivos genéricos y la misión de la organización.</i></p> <p><input type="checkbox"/> 1.3.- ¿Precisa el marco legal y regulatorio en el que se desarrollarán las actividades? <i>Evidencia: Dentro de la política se indican las leyes que le son de aplicación (LO 15/1999, RD 1720/2007, L39/2015, L40/2015, RD 3/2010, etc.) así como las distintas regulaciones que pudieran existir (ámbito europeo, local, etc.) (Por ejemplo: en un anexo incluir el listado de legislación aplicable).</i></p> <p><input type="checkbox"/> 1.4.- ¿Precisa los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación? <i>Evidencia: Dentro de la política se indican los roles de seguridad (responsable de la información, responsable del servicio, responsable de la seguridad (STIC), responsable del sistema (TIC), administradores, operadores, usuarios, equipo de respuesta ante incidentes, etc.), sus deberes (velar por el cumplimiento de la normativa, estar al tanto de los cambios de la tecnología, realizar el análisis de riesgos, etc.) y el procedimiento para su designación y renovación (cada cuánto se renueva, por qué motivos, quién lo designa, etc.).</i></p> <p><input type="checkbox"/> 1.5.- ¿Precisa la estructura del comité/s para la gestión y</p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización?</p> <p><i>Evidencia: Dentro de la política se indican la existencia de un Comité STIC, su composición (existencia de un responsable STIC, representantes de otros departamentos como seguridad física, seguridad operacional, etc.), su relación con otros elementos de la organización (alta dirección, comité de seguridad corporativa, etc.) y responsabilidad (redacción de la Política de Seguridad de las TIC, creación y aprobación de las normas y procedimientos sobre el uso de las TIC, definición de requisitos de formación del personal TIC, etc.).</i></p> <p><input type="checkbox"/> 1.6.- ¿Precisa las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso?</p> <p><i>Evidencia: Dentro de la política se indica cuál es el criterio para la calificación de la documentación, el procedimiento para su calificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse, etc.</i></p> <p><input type="checkbox"/> 1.7.- ¿La política de seguridad incluye una referencia a la legislación aplicable en materia de tratamiento de datos de carácter personal y existe coherencia entre dicha política y la documentación exigida por tal legislación específica?</p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Dentro de la política se incluye referencia a la legislación aplicable en materia de tratamiento de datos de carácter personal y existe coherencia entre dicha política y la documentación que exige la mencionada legislación sobre tratamiento de datos personales.</i></p> <p><i>Cuando el sistema auditado tenga por objeto el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo y en concreto con el Documento de Seguridad. A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto el tratamiento de datos personales, se tendrá en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.</i></p>		
org.2	Normativa de seguridad			
	Básica	<p><input type="checkbox"/> 1.- ¿Dispone de uno o varios documentos que constituyan la normativa de seguridad escrita?</p> <p><i>Evidencia: La normativa de seguridad está impresa y/o guardada en formato electrónico.</i></p> <p>Respecto a dicha normativa de seguridad:</p> <p><input type="checkbox"/> 1.1.- ¿Precisa el uso correcto de equipos, servicios e</p>	<p>Aplica:</p> <p><input type="checkbox"/> Sí</p> <p>Lo audito:</p> <p><input type="checkbox"/> Sí</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>instalaciones? <i>Evidencia: Existen normativas respecto a la protección de equipos desatendidos, uso del correo electrónico con fines personales, medidas contra el acceso físico no autorizado a las instalaciones, etc. Estas normativas deben indicar cómo localizar los procedimientos relacionados.</i></p> <p><input type="checkbox"/> 1.2.- ¿Precisa lo que se considera uso indebido? <i>Evidencia: Existen normativas que indican lo que se considera un uso indebido de los equipos (p. ej.: utilizar el ordenador para fines personales), los servicios (p. ej.: utilizar Internet para descargar contenidos no autorizados o inapropiados), las instalaciones (p. ej.: comer en la sala de servidores), la información (p. ej.: enviar datos confidenciales mediante correo electrónico sin cifrar), etc.</i></p> <p><input type="checkbox"/> 1.3.- ¿Precisa la responsabilidad del personal con respecto al cumplimiento o violación de estas normas (derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente)? <i>Evidencia: Existen normativas que indican los derechos (p. ej.: acceso al correo electrónico para el ejercicio de sus funciones), deberes (p. ej.: informar de cualquier incidente que afecte a la seguridad de la información) y medidas disciplinarias (referencia a la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público o adaptaciones particulares).</i></p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
org.3	<p><i>Procedimientos de seguridad</i></p> <p>Básica</p>	<p><input type="checkbox"/> 1.- ¿Dispone de uno o varios documentos que constituyan los procedimientos de seguridad escritos?</p> <p><i>Evidencia: Los procedimientos de seguridad están impresos y/o guardados en formato electrónico, los ha elaborado el responsable STIC y están aprobados por el Comité STIC. Además, existe un procedimiento de revisión y firma regular. Deben existir procedimientos para la mayoría de las actividades rutinarias, cuanto más próximo al 100% mejor (p. ej.: sobre el inventariado de activos, la modificación de reglas en el firewall, las tareas de copia de seguridad o backup, el alta de usuarios, etc.).</i></p> <p>Respecto a dichos procedimientos de seguridad:</p> <p><input type="checkbox"/> 1.1.- ¿Precisan cómo llevar a cabo las tareas habituales?</p> <p><i>Evidencia: Cada procedimiento debe cubrir, entre otros, en qué condiciones se aplica, qué se debe hacer, qué registros quedan de las actividades, (p. ej.: el procedimiento de inventario de activos podría indicar “Tras la aprobación del cambio -adición, modificación o supresión- de uno o más activos del inventario, la persona encargada y autorizada para dicho cambio -el administrador de sistemas si es un servidor, el técnico de comunicaciones si es un elemento de red, etc.- deberá anotar en el inventario qué tipo de cambio se ha producido, sobre qué activo, la fecha y su nombre –además de actualizar el detalle del activo-. En caso de encontrar algún problema en este</i></p>	<p>Aplica:</p> <p><input type="checkbox"/> Sí</p> <p>Lo audito:</p> <p><input type="checkbox"/> Sí</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>procedimiento, reportarlo al responsable STIC detallando, mediante el sistema de notificaciones previamente estipulado, cuál ha sido el problema y, al menos, una propuesta de solución”).</i></p> <p><input type="checkbox"/> 1.2.- ¿Precisan quién debe hacer cada tarea? <i>Evidencia: Se asigna cada tarea a un rol (responsable STIC, administrador, operador, etc.) (p. ej.: el procedimiento de inventario de activos podría indicar “Será el administrador de sistemas quien revise cada 6 meses el inventario de activos, si identifica que no ha cambiado ningún activo desde la última revisión, procederá a comprobar que efectivamente no se ha modificado nada dentro del alcance del inventario para asegurar que no ha habido ningún cambio no autorizado ni reportado”).</i></p> <p><input type="checkbox"/> 1.3.- ¿Precisan cómo identificar y reportar comportamientos anómalos? <i>Evidencia: Existe un procedimiento que define qué se entiende por comportamiento anómalo (p. ej.: recibir un mensaje de error de la aplicación), cómo y a quién debe reportarse (p. ej.: debe reportarse qué aplicación estaba usando, qué estaba haciendo y el mensaje de error por correo electrónico a incidencias@organismo.es).</i></p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
org.4	<p>Proceso de autorización</p> <p>Básica</p>	<p><input type="checkbox"/> 1.- ¿Existe un proceso formal para las autorizaciones respecto a los sistemas de información?</p> <p><i>Evidencia: La normativa de seguridad contempla, para cada tipo de componente o actuación, la persona o punto de contacto para su autorización. Existe un modelo de solicitud (formulario) en cualquier formato que contiene: Descripción del elemento (componente) o actuación para la que se solicita la autorización, las actividades para las que se requiere el nuevo componente (motivación), el tiempo para el que se solicita la autorización (que puede ser temporal o permanente), justificación de que no afecta a otras funcionalidades del sistema, un análisis de riesgo conforme a la categoría del sistema (si el nuevo componente introduce posibles vulnerabilidades), justificación de que no viola ninguna normativa de seguridad, información de los procedimientos que son de aplicación así como de la necesidad de desarrollar nuevos si fuese necesario.</i></p> <p><i>A continuación, se exponen los elementos sobre los cuales debe existir un proceso de autorización.</i></p> <p>Respecto a dicho proceso de autorización:</p> <p><input type="checkbox"/> 1.1.- ¿Cubre la utilización de instalaciones, tanto habituales como alternativas?</p> <p><i>Evidencia: La normativa contempla el proceso de autorización de utilización de instalaciones (p. ej.: acceso al CPD, uso de un local</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>alternativo para los servidores de respaldo ante desastres, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable pertinente antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.2.- ¿Cubre la entrada de equipos en producción, en particular, equipos que involucren criptografía? <i>Evidencia: La normativa contempla el proceso de autorización de entrada de equipos en producción, que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.3.- ¿Cubre la entrada de aplicaciones en producción? <i>Evidencia: La normativa contempla el proceso de autorización de entrada de aplicaciones en producción (p. ej.: actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.4.- ¿Cubre el establecimiento de enlaces de comunicaciones</p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>con otros sistemas? <i>Evidencia: La normativa contempla el proceso de autorización de enlaces de comunicaciones con otros sistemas (p. ej.: para el intercambio de expedientes entre un organismo y otro), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.5.- ¿Cubre la utilización de medios telemáticos de comunicación (tanto habituales como alternativos)? <i>Evidencia: La normativa contempla el proceso de autorización de utilización de medios de comunicación (p. ej.: uso de una línea de datos para el acceso a Internet), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.6.- ¿Cubre la utilización de soportes de información? <i>Evidencia: La normativa contempla el proceso de autorización de utilización de soportes de información (p. ej.: cintas de backup, DVD, memorias USB, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p>		

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.7.- ¿Cubre la utilización de equipos móviles? <i>Evidencia: La normativa contempla el proceso de autorización de utilización de equipos móviles (p. ej.: ordenadores portátiles, PDA u otros de naturaleza análoga), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p> <p><input type="checkbox"/> 1.8.- ¿Cubre la utilización de servicios de terceros, bajo contrato o Convenio? <i>Evidencia: La normativa contempla el proceso de utilización de servicios de terceros (p. ej.: gestión de incidentes, gestión del servicio, desarrollo, infraestructura, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.</i></p>		

5.2.2 MARCO OPERACIONAL

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op	MARCO OPERACIONAL			
op.pl	PLANIFICACIÓN			
op.pl.1	Análisis de riesgos			
	<p>Básica</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un análisis de riesgos, al menos, informal? <i>Evidencia: Dispone de un documento aprobado en el que se ha realizado una exposición textual en lenguaje natural del análisis de riesgos. Dicho documento no tiene más de un año desde su aprobación o revisión.</i></p> <p>Respecto a dicho análisis de riesgos:</p> <p><input type="checkbox"/> 1.1.- ¿Identifica los activos más valiosos del sistema? <i>Evidencia: En el documento se identifican los servicios que presta la organización y la información que maneja en referencia al cumplimiento de la Ley 39/2015 (p. ej.: servicio telemático de tramitación de expedientes, etc.), así como los elementos en los que se sustentan (p. ej.: servidores, línea de comunicaciones, aire acondicionado del CPD, oficinas, etc.).</i></p> <p><input type="checkbox"/> 1.2.- ¿Identifica las amenazas más probables? <i>Evidencia: En el documento se identifican las amenazas más probables (p. ej.: incendio, robo, virus informático, ataque informático, etc.).</i></p>	<p>Aplica: <input type="checkbox"/> Sí</p> <p>Lo audito: <input type="checkbox"/> Sí</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Registro:</p> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.3.- ¿Identifica las salvaguardas que protegen de dichas amenazas? <i>Evidencia: En el documento se identifican las salvaguardas de que se disponen para mitigar las amenazas identificadas (p. ej.: extintor, puerta con cerradura, antivirus, cortafuegos, etc.).</i></p> <p><input type="checkbox"/> 1.4.- ¿Identifica los principales riesgos residuales? <i>Evidencia: En el documento se identifican las amenazas para las que no existen salvaguardas, o aquellas para las que el grado de protección actual no es el suficiente (p. ej.: fuga de información en un soporte USB, etc.).</i></p>		
	Media	<p><input type="checkbox"/> 2.- ¿Dispone de un análisis de riesgos, al menos, semi-formal? <i>Evidencia: Dispone de un documento aprobado en el que se ha realizado una exposición textual en lenguaje específico y con una semántica definida (es decir, con tablas) del análisis de riesgos. Dicho documento no tiene más de un año desde su aprobación o revisión.</i></p> <p>Respecto a dicho análisis de riesgos:</p> <p><input type="checkbox"/> 2.1.- ¿Identifica y valora cualitativamente los activos más</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Registro:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>valiosos del sistema? <i>Evidencia: En el documento se identifican los servicios que presta la organización y la información que maneja en referencia al cumplimiento de la Ley 39/2015 (p. ej.: servicio telemático de tramitación de expedientes, etc.), así como los elementos en los que se sustentan (p. ej.: servidores, línea de comunicaciones, aire acondicionado del CPD, oficinas, etc.). Dichos activos (servicios e información) además son valorados cualitativamente (siguiendo los criterios de bajo, medio o alto).</i></p> <p><input type="checkbox"/> 2.2.- ¿Identifica y cuantifica las amenazas más probables? <i>Evidencia: En el documento se identifican las amenazas más probables y estas son cuantificadas (p. ej.: incendio con baja probabilidad, robo con baja probabilidad, virus con alta probabilidad, etc.).</i></p> <p><input type="checkbox"/> 2.3.- ¿Identifica y valora las salvaguardas que protegen de dichas amenazas? <i>Evidencia: En el documento se identifican las salvaguardas de que se disponen para mitigar las amenazas identificadas y su nivel de eficacia (p. ej.: extintor en todos los pasillos, puerta con cerradura sólo en el CPD, antivirus en los servidores pero no en los PCs, etc.).</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 2.4.- ¿Identifica y valora el riesgo residual? <i>Evidencia: En el documento se identifica el nivel de riesgo al que están expuestos los servicios (bajo, medio o alto), conforme a una tabla de equivalencias que tiene en cuenta el valor de los activos, la probabilidad de las amenazas y la eficacia de las salvaguardas.</i></p> <p>Consultar guías: CCN-STIC-410 <i>Análisis de riesgos en sistemas de la Administración</i> CCN-STIC-470x <i>Manual de usuario de PILAR</i></p>		
	Alta	<p><input type="checkbox"/> 3.- ¿Dispone de un análisis de riesgos formal? <i>Evidencia: Dispone de un documento aprobado en el que se ha realizado una exposición formal en lenguaje específico y con un fundamento metodológico reconocido internacionalmente (p. ej.: según MAGERIT, UNE 71504, CRAMM, EBIOS, OCTAVE, etc.) del análisis de riesgos. Dicho documento no tiene más de un año desde su aprobación o revisión. Utiliza una herramienta reconocida de análisis de riesgos (p. ej.: PILAR, CRAMM, EBIOS, etc.).</i></p> <p>Respecto a dicho análisis de riesgos:</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 3.1.- ¿Identifica y valora cualitativamente los activos más valiosos del sistema? <i>Evidencia: En el documento se identifican los servicios que presta la organización y la información que maneja así como los elementos en los que se sustentan (p. ej.: servidores, línea de comunicaciones, aire acondicionado del CPD, oficinas, etc.). Dichos activos (servicios e información) además son valorados cualitativamente (siguiendo los criterios de bajo, medio o alto).</i></p> <p><input type="checkbox"/> 3.2.- ¿Identifica y cuantifica las amenazas posibles? <i>Evidencia: En el documento se identifican las amenazas más probables para cada activo, su frecuencia y degradación resultante (p. ej.: incendio del CPD con baja probabilidad y degradación total, robo del servidor con baja probabilidad y degradación total, virus en el servidor con alta probabilidad y degradación parcial, etc.).</i></p> <p><input type="checkbox"/> 3.3.- ¿Identifica las vulnerabilidades habilitantes de dichas amenazas? <i>Evidencia: En el documento se identifican las vulnerabilidades que habilitan esas amenazas (p. ej.: materiales inflamables, la llave la tienen más de 10 personas, el antivirus no se actualiza con frecuencia, etc.).</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 3.4.- ¿Identifica y valora las salvaguardas adecuadas? <i>Evidencia: En el documento se identifican las salvaguardas de que se disponen para mitigar las amenazas identificadas y su nivel de eficacia (p. ej.: extintor en todos los pasillos, puerta con cerradura sólo en el CPD, antivirus en los servidores pero no en los PCs, etc.), así como la posible necesidad de disponer de más salvaguardas.</i></p> <p><input type="checkbox"/> 3.5.- ¿Identifica y valora el riesgo residual? <i>Evidencia: En el documento se identifica el nivel de riesgo al que están expuestos los servicios y la información (bajo, medio o alto).</i></p> <p>Consultar guías: CCN-STIC-410 <i>Análisis de riesgos en sistemas de la Administración</i> CCN-STIC-470x <i>Manual de usuario de PILAR</i> MAGERIT v3</p>		
op.pl.2	Arquitectura de seguridad Básica	<p><input type="checkbox"/> 1.- ¿Dispone de documentación de las instalaciones? <i>Evidencia: Dispone de un documento que detalla las instalaciones (p. ej.: número de instalaciones, su ubicación, etc.).</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>Respecto a dicha documentación de las instalaciones:</p> <p><input type="checkbox"/> 1.1.- ¿Precisa las áreas? <i>Evidencia: El documento detalla las áreas existentes (p. ej.: CPD, zona de acceso público, zona de carga y descarga, zona de operadores, etc.).</i></p> <p><input type="checkbox"/> 1.2.- ¿Precisa los puntos de acceso? <i>Evidencia: El documento detalla los puntos de acceso (p. ej.: puerta principal, salida de emergencia, etc.).</i></p> <p><input type="checkbox"/> 2.- ¿Dispone de documentación del sistema? <i>Evidencia: Dispone de un inventario de los sistemas de información.</i></p> <p>Respecto a dicha documentación del sistema:</p> <p><input type="checkbox"/> 2.1.- ¿Precisa los equipos? <i>Evidencia: La documentación describe los activos del sistema (p. ej.: servidor de correo, robot de copias de seguridad o backup, etc.).</i></p> <p><input type="checkbox"/> 2.2.- ¿Precisa las redes internas y conexiones al exterior? <i>Evidencia: la documentación describe las redes existentes (p. ej.: red local con direccionamiento 192.168.0.0/24, zona desmilitarizada (DMZ) con direccionamiento 172.16.0.0/24,</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>etc.) y los elementos de conexión al exterior (p. ej.: la red local está separada de Internet mediante un cortafuegos o firewall, etc.).</i></p> <p><input type="checkbox"/> 2.3.- ¿Precisa los puntos de acceso al sistema? <i>Evidencia: La documentación describe los puntos de acceso al sistema (p. ej.: puestos de trabajo, consolas de administración, web de la intranet, etc.).</i></p> <p><input type="checkbox"/> 3.- ¿Dispone de documentación de líneas de defensa? <i>Evidencia: La documentación describe los sistemas de seguridad de que dispone (p. ej.: firewalls, antivirus, antispam, antiphishing, etc.).</i></p> <p>Respecto a dicha documentación de las líneas de defensa:</p> <p><input type="checkbox"/> 3.1.- ¿Precisa los puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet o redes públicas en general? <i>Evidencia: Dicha documentación describe los elementos de interconexión a otras redes (p. ej.: la conexión con Internet se realiza a través de un router, la conexión con otras oficinas se realiza mediante un túnel VPN IPSec, la conexión desde portátiles remotos se realiza mediante VPN SSL, etc.).</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 3.2.- ¿Precisa los cortafuegos, DMZ, etc.? <i>Evidencia: Dicha documentación describe los elementos de defensa en las conexiones a otras redes (p. ej.: la conexión con Internet se realiza a través de un firewall, etc.).</i></p> <p><input type="checkbox"/> 4.- ¿Dispone de documentación del sistema de identificación y autenticación de usuarios? <i>Evidencia: Dispone de un documento que detalla los sistemas de identificación y autenticación de usuarios para cada sistema o servicio.</i></p> <p>Respecto a dicha documentación de identificación y autenticación de usuarios:</p> <p><input type="checkbox"/> 4.1.- ¿Precisa el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga? <i>Evidencia: Dicho documento detalla el mecanismo de autenticación a cada sistema o servicio (p. ej.: el acceso al servicio de tramitación de expedientes es mediante DNle, el acceso a la consola de administrador del servidor es mediante usuario y contraseña, etc.).</i></p> <p><input type="checkbox"/> 4.2.- ¿Precisa de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso (p. ej.:</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>/etc/passwd en Linux, Active Directory en Windows, etc.)? <i>Evidencia: Dicho documento detalla dónde se almacenan las contraseñas (p. ej.: las claves se almacenan cifradas en el fichero /etc/shadow en Linux, Active Directory en Windows, etc.).</i></p> <p>Consultar guías: CCN-STIC-406 Seguridad en redes inalámbricas basadas en 802.11 CCN-STIC-408 Seguridad perimetral – cortafuegos CCN-STIC-412 Requisitos de seguridad de entornos y aplicaciones web</p>		
	Media	<p><input type="checkbox"/> 5.- ¿Dispone de un sistema de gestión relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información? <i>Evidencia: Dispone de un documento que detalla cómo se gestionan los elementos antes enumerados (p. ej.: cómo se da de alta un nuevo usuario, cómo se autoriza la conexión con un sistema externo, cómo se autoriza el acceso a un área restringida, etc.).</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	Alta	<p><input type="checkbox"/> 6.- ¿Dispone de documentación del sistema de gestión con actualización y aprobación periódica? <i>Evidencia: Los documentos detallan con qué frecuencia se revisan (bien explícitamente o implícitamente en los documentos de gestión de cambios), quién es el encargado de la tarea y quién es el responsable de su aprobación.</i></p> <p><input type="checkbox"/> 7.- ¿Está esta documentación aprobada por la Dirección técnica? <i>Evidencia: Los documentos han sido aprobados por la Dirección técnica.</i></p> <p><input type="checkbox"/> 8.- ¿Dispone y tiene documentación de los controles técnicos internos? <i>Evidencia: Dispone de un documento que detalla cómo se controlan los datos una vez en los sistemas (p. ej.: el intercambio de información con otros sistemas va acompañado de hashes para evitar su alteración, etc.).</i></p> <p>Respecto a dicha documentación de los controles técnicos internos:</p> <p><input type="checkbox"/> 8.1.- ¿Precisa la validación de datos de entrada, salida y datos intermedios? <i>Evidencia: En dicho documento se detalla cómo se controlan los</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>datos una vez en los sistemas (p. ej.: validación de rangos en los datos, bloqueo de caracteres no autorizados, etc.).</i>		
op.pl.3	Básica	<p>Adquisición de nuevos componentes</p> <p><input type="checkbox"/> 1.- ¿Existe un proceso formal para planificar la adquisición de nuevos componentes del sistema? <i>Evidencia: Dispone de un procedimiento documentado que detalla los elementos que se deben tener en cuenta antes de la adquisición de nuevos componentes del sistema (p. ej.: adquisición de un servidor, firewall, antivirus, cinta de backup, etc.), que incluye la persona responsable de revisar y mantener este procedimiento. Dispone de un documento que indica las medidas de seguridad requeridas para los nuevos componentes adquiridos y su cumplimiento (p. ej.: dispone de un checklist con los requisitos que debe tener el firewall –cifrado IPSec, stateful packet inspection, etc.- y su correspondiente indicación sobre si lo cubre o no -en cuyo caso se argumenta el motivo- junto con el nombre de la persona que ha realizado la verificación y la fecha de la misma).</i></p> <p>Respecto a dicho proceso de adquisición: <input type="checkbox"/> 1.1.- ¿Atiende las conclusiones del análisis de riesgos [op.pl.1]?</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Dicho procedimiento especifica que en la adquisición de nuevos componentes tiene prioridad la adquisición de los mecanismos de seguridad para el sistema que haya identificado el análisis de riesgos y su plan de acción (p. ej.: el checklist indica si el motivo de algún requisito impuesto al firewall proviene del análisis y gestión de riesgos).</i></p> <p><input type="checkbox"/> 1.2.- ¿Es acorde con la arquitectura de seguridad [op.pl.2]? <i>Evidencia: Dicho procedimiento indica que las adquisiciones deben estar alineadas con la arquitectura de seguridad definida (p. ej.: si se ha definido que la seguridad física está compuesta por una puerta con cerradura para el CPD, la adquisición de una nueva puerta debe obligar a que ésta vuelva a tener cerradura por lo que no valdría una nueva puerta sin un sistema igual o mejor de cierre).</i></p> <p><input type="checkbox"/> 1.3.- ¿Contempla las necesidades técnicas, de formación y de financiación de forma conjunta? <i>Evidencia: Dicho procedimiento contempla que el nuevo componente cumple con las medidas técnicas definidas (p. ej.: si las conexiones deben ser HTTPS, el nuevo componente debe soportar HTTPS), que el personal a cargo del componente</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>dispone de la formación necesaria para su uso o se le proporcionará, y que ha recibido el consentimiento del departamento económico para su adquisición (p. ej.: el checklist contempla que cumpla o no -en cuyo caso se argumenta el motivo- las necesidades técnicas enumeradas, las necesidades de formación –si no están cubiertas actualmente indicará la forma de cubrirlas mediante cursos, manuales, etc. aprobados).</i></p> <p>Consultar guías: CCN-STIC-205 Actividades de seguridad en el ciclo de vida de los sistemas TIC CCN-STIC-400 Manual de seguridad de las TIC CCN-STIC-404 Control de soportes informáticos</p>		
op.pl.4	- D / Medio	<p><input type="checkbox"/> 1.- ¿Antes de la puesta en explotación, se han estudiado las necesidades de dimensionamiento?</p> <p><i>Evidencia: Dispone de un estudio en cualquier formato con dicho análisis, antes de cada adquisición o puesta en explotación, de las necesidades de los medios adicionales o capacidades de los medios existentes, de modo que estos</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>satisfagan los requisitos establecidos. En caso de que no queden satisfechos, se argumenta. Existen evidencias documentales de cada estudio, en el que se refleja quién lo realizó, la fecha y el resultado.</i></p> <p>Respecto a dicho estudio del dimensionamiento:</p> <p><input type="checkbox"/> 1.1.- ¿Cubre las necesidades de procesamiento? <i>Evidencia: Dicho estudio estima las necesidades de procesamiento (p. ej.: la CPU y memoria del dispositivo soportarán el número concurrente de sesiones estimadas).</i></p> <p><input type="checkbox"/> 1.2.- ¿Cubre las necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse? <i>Evidencia: Dicho estudio estima las necesidades de almacenamiento tanto para su funcionamiento como para el tiempo durante el que la información debe mantenerse (p. ej.: se ha calculado el volumen de datos generado cada día, el número de días que se utilizará el servicio y el tiempo que la información deberá estar accesible –tanto on-line como en un backup-, y el dispositivo lo soporta).</i></p> <p><input type="checkbox"/> 1.3.- ¿Cubre las necesidades de comunicación? <i>Evidencia: Dicho estudio estima las necesidades de</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>comunicación (p. ej.: el ancho de banda disponible soporta el volumen de datos a transmitir en cada momento, o que el dispositivo soporta el acceso desde otra ubicación).</i></p> <p><input type="checkbox"/> 1.4.- ¿Cubre las necesidades de personal: cantidad y cualificación profesional? <i>Evidencia: Dicho estudio estima las necesidades de personal necesario para la gestión del mismo (p. ej.: existe personal con dedicación para la gestión del elemento) de forma adecuada (p. ej.: la gestión del elemento se realizará por personal que domina su interfaz de uso y gestión).</i></p> <p><input type="checkbox"/> 1.5.- ¿Cubre las necesidades de instalaciones y medios auxiliares? <i>Evidencia: Dicho estudio estima las necesidades de las instalaciones (p. ej.: el dispositivo cabe por tamaño en el armario de servidores y además quedan bahías libres donde ubicarlo) y los medios auxiliares (p. ej.: las frigorías existentes de aire acondicionado serán suficientes para seguir enfriando el CPD).</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.pl.5	Alta	<p><i>Componentes certificados</i></p> <p><input type="checkbox"/> 1.- ¿Se utilizan sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales?</p> <p><i>Evidencia: Dispone de un listado de modelos para la adquisición de componentes cuya evaluación se haya realizado conforme a normas europeas o internacionales (p. ej.: cumple la ISO/IEC 15408 -Common Criteria-) o una certificación funcional que contemple:</i></p> <ul style="list-style-type: none"> - Diseño, desarrollo, pruebas y revisión del componente con método. - Análisis de vulnerabilidades para ataques de nivel de competencia técnica tan alto como permita la tecnología existente en el campo, o tan alto como permita la normativa de referencia utilizada. - Máximo nivel de confianza que proporcione la normativa utilizada respecto a la prueba de robustez de la seguridad del componente, cuando es utilizado de forma distinta a la especificada por su documentación de uso. - Máximo nivel de confianza que proporcione la normativa utilizada respecto a la resistencia de las funciones de seguridad del producto, que se basen en mecanismos probabilísticos o permutacionales: resistencia a ataques 	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>directos que se ejecuten con información incorrecta pero sin manipular el normal funcionamiento del producto según su diseño.</i></p> <p><i>- Garantizar, al menos documentalente, que el fabricante del producto dispone de procedimientos definidos para el tratamiento de futuras vulnerabilidades que se detecten en el producto.</i></p> <p><i>Existen evidencias de que los componentes han pasado dicha evaluación o certificación.</i></p> <p><input type="checkbox"/> 2.- <i>¿Y están los certificados reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información?</i></p> <p><i>Evidencia: Las certificaciones de los componentes son reconocidas por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Respecto a los componentes de cifra y generación de firma electrónica han sido certificados criptológicamente, en términos de su fortaleza algorítmica, y existe evidencia de ello.</i></p> <p>Consultar guías: CCN-STIC-105 <i>Catálogo de productos de la seguridad de las Tecnológicas de la Información y las Comunicaciones</i> CCN-STIC-813 <i>Componentes Certificados en el ENS</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.acc	CONTROL DE ACCESO			
op.acc.1	Identificación - A, T / Bajo	<input type="checkbox"/> 1.- ¿Cada entidad (usuario o proceso) que accede al sistema tiene asignado un identificador singular? <i>Evidencia: Dispone de un procedimiento documentado para la creación de nuevos usuarios del sistema que especifica que no se puede crear un identificador para varios usuarios. Dispone de una normativa documentada que especifica que los usuarios no pueden compartir su identificador con nadie. La lista de usuarios del sistema no muestra usuarios generales (p. ej.: administración, dirección, sistemas, becario, etc.).</i> Respecto a dicho identificador: <input type="checkbox"/> 1.1.- ¿Cada usuario que accede al sistema tiene asignado distintos identificadores únicos en función de cada uno de los roles que deba desempeñar en el sistema? <i>Evidencia: Dispone de un procedimiento documentado para la creación de nuevos usuarios del sistema que especifica que deben crearse identificadores para cada rol de cada usuario (administración, consulta, invitado, etc.).</i> <input type="checkbox"/> 1.2.- ¿Se puede saber a quién corresponde? <i>Evidencia: Dicho procedimiento contempla el mantener un registro de las entidades responsables de cada identificador.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Existe una relación de los identificadores con sus usuarios (p. ej.: el identificador “webmaster” es de Jorge Pérez, pertenece al grupo “web” y tiene por lo tanto permisos de lectura y escritura en la carpeta \web y de lectura en la carpeta \ftp).</i></p> <p><input type="checkbox"/> 1.3.- ¿Se puede saber qué derechos tiene? <i>Evidencia: Dicho procedimiento contempla el mantener un registro de los derechos de cada entidad. Existe una relación de los identificadores con sus permisos (p. ej.: el identificador “webmaster” pertenece al grupo “web” y tiene por lo tanto permisos de lectura y escritura en la carpeta \web y de lectura en la carpeta \ftp).</i></p> <p><input type="checkbox"/> 1.4.- ¿Se inhabilita el identificador cuando el usuario deja la organización, cesa en la función para la cual se requería la cuenta de usuario o cuando la persona que la autorizó da orden en sentido contrario? <i>Evidencia: Dispone de un procedimiento documentado ligado a la gestión de recursos humanos para avisar a los responsables de la gestión de usuarios en el sistema de los cambios en las responsabilidades de los usuarios. Consultar con recursos humanos cuál ha sido el último cambio y consultar si se ha reflejado el mismo en los usuarios del sistema.</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.5.- ¿El identificador se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que identifica el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad, procedimiento que indica que debe llevarse a cabo en los sistemas previos a su puesta en explotación o ya en producción, lo que se debe hacer una vez pasado dicho periodo y quién debe hacer cada tarea del procedimiento (p. ej.: cuando un empleado deja la organización, su usuario se bloquea durante el tiempo establecido en la política de retención, y no es hasta pasado ese plazo cuando dicho usuario puede eliminarse del sistema). Existe evidencia documental del periodo necesario para atender a las necesidades de trazabilidad de los registros. Tomando un sistema (el muestreo puede ser mayor según se estime conveniente), se analizará cuál es el periodo de retención establecido y se buscarán identificadores que han sido inhabilitados dentro y fuera del periodo de retención, para constatar que se ha procedido conforme al procedimiento.</i></p> <p><input type="checkbox"/> 2.- ¿El nivel de la dimensión de autenticidad del mecanismo de autenticación de los sistemas de información a los que se accede se corresponde con el nivel de seguridad de los</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>sistemas de identificación electrónica? <i>Evidencia: Existe una correspondencia entre el nivel de autenticidad definido y el nivel de seguridad equivalente de acuerdo al artículo 8 del Reglamento nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.</i></p> <p>Consultar guías: Serie CCN-STIC-500 Guías para Entornos Windows Serie CCN-STIC-600 Guías para otros Entornos Serie CCN-STIC-800 Guías del ENS <i>Reglamento Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014.</i></p>		
op.acc.2	<p><i>Requisitos de acceso</i></p> <p>- I, C, A, T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se protegen los recursos del sistema con algún mecanismo que impida su utilización (salvo a las entidades que disfruten de derechos de acceso suficientes)? <i>Evidencia: El sistema antes de su puesta en explotación o ya en producción, cuenta con un mecanismo de control de acceso. Para acceder a cualquier recurso es necesario estar identificado</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>y autenticado previamente (p. ej.: a pesar de que se pueda acceder a un PC sin contraseña luego para usar cualquier aplicación de nivel bajo o superior requiere una identificación y autenticación).</i></p> <p><input type="checkbox"/> 2.- ¿Se establecen los derechos de acceso de cada recurso según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema? <i>Evidencia: La política y normativa de seguridad del sistema especifican quién es el responsable de cada recurso y, por lo tanto, es también responsable de la asignación de autorización y nivel de acceso a cada recurso. Constatar que los derechos de acceso coinciden con los establecidos en la política o normativa.</i></p> <p><input type="checkbox"/> 3.- ¿Incluye el mecanismo la protección frente al acceso a los componentes del sistema y a sus ficheros o registros de configuración? <i>Evidencia: Dispone de evidencia documental (manual de administración, documento desarrollado internamente, etc.) donde se especifica cuáles son los componentes del sistema y sus ficheros o registros de configuración, así como los permisos de usuario que deben establecerse de forma que sólo los usuarios autorizados tengan acceso. Constatar que el acceso a los ficheros de configuración del sistema sólo está autorizado al</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>personal técnico.</i></p> <p>Consultar guías: Serie CCN-STIC-500 <i>Guías para Entornos Windows</i> Serie CCN-STIC-600 <i>Guías para otros Entornos</i> Serie CCN-STIC-800 <i>Guías ENS</i></p>		
op.acc.3	<p><i>Segregación de funciones y tareas</i></p> <p>- I, C, A, T / Medio</p>	<p><input type="checkbox"/> 1.- ¿Existe segregación de funciones y tareas? <i>Evidencia: Consultar funciones incompatibles y solicitar el nombre de las personas que tienen asignadas dichas funciones para constatar que no son las mismas personas.</i></p> <p>Respecto a dicha segregación de funciones y tareas:</p> <p><input type="checkbox"/> 1.1.- ¿Contempla la incompatibilidad de tareas de desarrollo con las de operación? <i>Evidencia: En el esquema de funciones aparecen “desarrollo” y “operación”, y están marcadas como incompatibles entre sí.</i></p> <p><input type="checkbox"/> 1.2.- ¿Contempla la incompatibilidad de tareas de “configuración y mantenimiento del sistema” con las de operación? <i>Evidencia: En el esquema de funciones aparecen “configuración</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>y mantenimiento del sistema” y “operación”, y están marcadas como incompatibles entre sí.</i></p> <p><input type="checkbox"/> 1.3.- ¿Contempla la incompatibilidad de tareas de “auditoría o supervisión” con las de cualquier otra función relacionada con el sistema?</p> <p><i>Evidencia: En el esquema de funciones aparece “auditoría o supervisión del sistema” y está marcada como incompatibles con todas las demás.</i></p> <p>Consultar guías: CCN-STIC-801 ENS Responsables y funciones Resto de serie CCN-STIC-800 Guías del ENS</p>		
op.acc.4	<p>Proceso de gestión de derechos de acceso</p> <p>- I, C, A, T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se limitan los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?</p> <p><i>Evidencia: La política y normativa de seguridad especifican que a cada usuario sólo se le proporcionarán los privilegios mínimos para cumplir sus obligaciones (p. ej.: un usuario encargado de las altas de nuevos trámites y que no tiene responsabilidad sobre la gestión de dichos trámites no debe ser capaz de acceder a la gestión de los mismos). Existe evidencia documental de cuáles son los privilegios que debe tener cada</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>usuario en función de sus obligaciones. Constatar que la información de muestreo está accesible sólo a usuarios cuyos privilegios (obligaciones) coinciden con la anterior evidencia documental.</i></p> <p><input type="checkbox"/> 2.- ¿Puede sólo y exclusivamente el personal con competencia para ello conceder, alterar o anular la autorización de acceso a los recursos conforme a los criterios establecidos por su responsable?</p> <p><i>Evidencia: Dispone de evidencia documental en la que se relaciona quién es el responsable de los recursos, y en quién delega la responsabilidad de conceder, alterar o anular el acceso a los recursos (está asignada a personal concreto y no a todos o cualquiera en la organización).</i></p> <p>Consultar guías: CCN-STIC-801 ENS Responsables y funciones Resto de serie CCN-STIC-800 Guías ENS</p>		
op.acc.5	<p><i>Mecanismo de autenticación</i></p> <p>- I, C, A, T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se encuentra identificado el mecanismo de autenticación en cada sistema?</p> <p><i>Evidencia: Dispone de un procedimiento para enumerar, de los sistemas previos a su puesta en explotación o ya en producción, el mecanismo de autenticación, y se identifica el responsable de</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>esta tarea. Existe un listado de sistemas que requieren autenticación y su mecanismo de autenticación correspondiente (p. ej.: la intranet requiere autenticación mediante usuario y contraseña, el correo electrónico requiere autenticación mediante usuario y contraseña).</i></p> <p>Respecto a las credenciales utilizadas:</p> <p><input type="checkbox"/> 1.1.- Si utilizan contraseñas ¿cumplen las reglas básicas de calidad?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que especifica que deben utilizar contraseñas de al menos una determinada longitud marcada por la política de la entidad, que contengan caracteres alfabéticos y numéricos, que no sean de fácil conjetura (fechas significativas, números de teléfono, matrículas de coche, nombres de familiares o amigos, etc.), ni reutilizar contraseñas de servicios personales. El mecanismo de gestión de credenciales no permite utilizar contraseñas que no cumplan esta política (p. ej.: la política de contraseñas de Windows no permite crear claves que incumplan esta política).</i></p> <p><input type="checkbox"/> 1.2.- ¿Se activa una vez que esté bajo el control efectivo del usuario?</p> <p><i>Evidencia: Dicha política o normativa establece que la cuenta del usuario no se habilita hasta que éste haya confirmado la</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>recepción de la credencial.</i></p> <p><input type="checkbox"/> 1.3.- ¿Están las credenciales bajo el control exclusivo del usuario? <i>Evidencia: Dicha política o normativa establece que las credenciales sólo las tiene el usuario (p. ej.: establece la responsabilidad del usuario de no compartir su credencial). En caso de tratarse de una contraseña, ésta sólo la conoce el usuario (p. ej.: la contraseña se almacena en el sistema de forma cifrada).</i></p> <p><input type="checkbox"/> 1.4.- ¿Ha confirmado el usuario que ha recibido las credenciales, y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida? <i>Evidencia: Existe un registro de cada usuario confirmando la recepción de la credencial y en el mismo se le informa de esos aspectos.</i></p> <p><input type="checkbox"/> 1.5.- ¿Se cambian las credenciales con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)? <i>Evidencia: Dispone de una política de seguridad documentada</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>que especifica la periodicidad en el cambio de las credenciales. Existe evidencia del cambio de las credenciales dentro del periodo establecido en la política (p. ej.: la política de contraseñas de Windows obliga al cambio de credencial pasado el tiempo establecido, existe un histórico en el que se indica cuál fue la fecha del último cambio de la credencial de cada usuario y se encuentra dentro del tiempo establecido, etc.).</i></p> <p><input type="checkbox"/> 1.6.- ¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema? <i>Evidencia: Dispone de un procedimiento documentado ligado a la gestión de recursos humanos para avisar a los responsables de la gestión de usuarios en el sistema de los cambios en las relaciones con los usuarios. Consultar con recursos humanos cuál ha sido la última finalización de relación y consultar si se ha reflejado el mismo en los usuarios del sistema.</i></p> <p>Consultar guías: CCN-STIC-807 <i>Criptología de Empleo en el ENS</i> Resto serie CCN-STIC-800</p>		
	- I, C, A, T / Medio	<p><input type="checkbox"/> 2.- ¿Se utiliza doble factor de autenticación? <i>Evidencia: Constatar que se emplea doble factor de autenticación: algo que se sabe (contraseñas o claves</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>concertadas); algo que se tiene (certificados software, tokens físicos unipersonales, etc.); y/o algo que se es (elementos biométricos).</i></p> <p><input type="checkbox"/> 3.- Si utilizan contraseñas, ¿cumplen las políticas rigurosas de calidad y renovación?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que aplica el recurso, por lo que obliga a utilizar contraseñas de al menos una determinada longitud marcada por la política de la entidad que contengan caracteres alfabéticos y numéricos, que no se repitan caracteres consecutivamente. La política y normativa de seguridad especifican que, además, no se deben utilizar contraseñas de fácil conjetura (fechas significativas, números de teléfono, matrículas de coche, nombres de familiares o amigos, etc.), ni reutilizar contraseñas de servicios personales. Dispone de una política o normativa de seguridad documentada que especifica la periodicidad en el cambio de las credenciales. El mecanismo de gestión de credenciales obliga a utilizar contraseñas de una longitud determinada, que contengan caracteres alfabéticos y numéricos, que no se repitan caracteres consecutivamente y contempla dicha periodicidad (p. ej.: el servidor LDAP no permite usar una clave de menos de determinado número de caracteres, además de que obliga a modificar la contraseña con la periodicidad</i></p>	<p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>estipulada).</i></p> <p><input type="checkbox"/> 4.- ¿Las credenciales utilizadas han sido obtenidas tras un registro previo? <i>Evidencia: Constatar que las credenciales han sido obtenidas de manera presencial, telemática mediante certificado electrónico cualificado o bien telemática mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.</i></p>		
	- I, C, A, T / Alto	<p><input type="checkbox"/> 5.- ¿Se suspenden las credenciales tras un periodo definido de no utilización? <i>Evidencia: Dispone de una política o normativa documentada para la revisión de credenciales que no se estén utilizando, en la que especifica el responsable y la periodicidad, igualmente ésta indica el periodo máximo de inactividad de una credencial antes de ser suspendido. Existe evidencia de la fecha de último uso de las credenciales.</i></p> <p>Respecto a los tokens:</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 6.- ¿El algoritmo está acreditado o certificado? <i>Evidencia: Dispone de un procedimiento documentado para la adquisición de componentes hardware que empleen algoritmos acreditados por el Centro Criptológico Nacional. Existe evidencia documental de los algoritmos utilizados en los tokens, indicando que han sido acreditados por el CCN y si están certificados.</i></p> <p><input type="checkbox"/> 7.- ¿Las credenciales utilizadas han sido obtenidas tras un registro previo? <i>Evidencia: Constatar que las credenciales han sido obtenidas de manera presencial o telemática mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.</i></p>		
op.acc.6	<p>Acceso local (local logon)</p> <p>- I, C, A, T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se previene la revelación de información del sistema? <i>Evidencia: Dispone de un mecanismo para que los sistemas antes de entrar en explotación o los ya existentes sean configurados de forma que no revelen información del sistema antes de un acceso autorizado. Los diálogos de acceso (al puesto local dentro de la propia instalación de la organización,</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>al servidor, al dominio de red, etc.) no revelan información sobre el sistema al que se está accediendo (p. ej.: un mensaje inadecuado previo al inicio de sesión sería “Bienvenido a los sistemas del Ayuntamiento del Tomillar, va a acceder a un sistema de nivel crítico en el que se almacena información sobre todos los ciudadanos de la comarca.”, mientras que uno adecuado sería “El acceso a este sistema está restringido a personal autorizado, se le informa que su uso deberá ceñirse al autorizado en la política de seguridad y su acceso quedará registrado”. Mensajes inadecuados de error en el acceso serían “Usuario inexistente” o “Contraseña incorrecta”, mientras que uno adecuado sería “Datos incorrectos”).</i></p> <p><input type="checkbox"/> 2.- ¿Se limita el número de intentos fallidos de acceso? <i>Evidencia: Dispone de una política o normativa documentada que especifica el número máximo de intentos fallidos de acceso, especificando qué acción tomar llegado el caso. El sistema aplica dicha política (p. ej.: tras 5 intentos de acceso fallidos bloquea la cuenta del usuario).</i></p> <p><input type="checkbox"/> 3.- ¿Se registran los accesos con éxito y los fallidos? <i>Evidencia: Dispone de una política o normativa documentada que especifica que se deben registrar tanto los accesos con éxito como fallidos. Comprobar que el sistema de registro</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>almacena tanto los accesos con éxito como los fallidos.</i></p> <p><input type="checkbox"/> 4.- ¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener el acceso? <i>Evidencia: Dispone de una política o normativa documentada que especifica que se debe informar al usuario de sus obligaciones inmediatamente después de obtener el acceso. Una vez habiendo accedido con éxito al sistema, éste muestra un aviso con las obligaciones del usuario.</i></p>		
	- I, C, A, T / Medio	<p><input type="checkbox"/> 5.- ¿Informa el sistema al usuario del último acceso con su identidad con éxito? <i>Evidencia: Dispone de un mecanismo que especifica que se debe informar al usuario del último acceso con su identidad con éxito, una vez habiendo obtenido acceso. Una vez habiendo accedido con éxito al sistema, éste muestra la fecha y hora del último acceso con éxito de ese usuario.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
	- I, C, A, T / Alto	<p><input type="checkbox"/> 6.- ¿Se limita el horario, fechas y lugar desde donde se accede? <i>Evidencia: Dispone de un mecanismo que indica el horario, fechas y lugar desde donde está autorizado el acceso. Existen mecanismos para aplicar dicha política o normativa. Comprobar si hay algún registro de acceso con éxito que</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>incumpla dicha política o normativa.</i></p> <p><input type="checkbox"/> 7.- ¿Se han establecido puntos en los que el sistema requerirá una renovación de la autenticación del usuario? <i>Evidencia: Dispone de un mecanismo que indica los puntos en los que el sistema requerirá una renovación de la autenticación del usuario. Verificar que esto se produce (p. ej.: se reutilizan automáticamente las credenciales de inicio de sesión en el PC para el acceso a la intranet, pero para acceder a la información de la nómina en la intranet vuelve a pedir las credenciales).</i></p>		<p><u>Observaciones auditoría:</u></p>
op.acc.7	<p>Acceso remoto (<i>remote login</i>)</p> <p>- I, C, A, T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se garantiza la seguridad del sistema cuando acceden remotamente usuarios u otras entidades? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los accesos realizados fuera de las propias instalaciones de la organización, a través de redes de terceros, deben cumplir los requisitos de las medidas [op.acc.6] y [mp.com.3].</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <p><u>Observaciones auditoría:</u></p>
	<p>- I, C, A, T / Medio</p>	<p><input type="checkbox"/> 2.- ¿Está documentado lo que puede hacerse remotamente? <i>Evidencia: Dispone de una política o normativa documentada que regula las actividades que pueden realizarse remotamente.</i></p> <p><input type="checkbox"/> 3.- ¿Se han autorizado previamente los accesos remotos? <i>Evidencia: Dispone de una política o normativa documentada</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>que especifica que los accesos remotos deben ser autorizados previamente, indicando la persona que puede autorizar el acceso. Existe evidencia documental de los accesos autorizados, por quién y durante qué periodo.</p>		<p><u>Observaciones auditoría:</u></p>
op.exp	EXPLOTACIÓN			
op.exp.1	Inventario de activos			
	Básica	<p><input type="checkbox"/> 1.- ¿Dispone de un inventario del sistema? Evidencia: Dispone de un inventario de los elementos que componen el sistema, en el que se detalla su identificador, fabricante y modelo (p. ej.: “JUPITER” - Cisco 2128, “ORION” - Dell PowerEdge R420, etc.).</p> <p>Respecto a dicho inventario:</p> <p><input type="checkbox"/> 1.1.- ¿Identifica la naturaleza de los elementos? Evidencia: Cada elemento del inventario tiene especificado de qué tipo es (p. ej.: el elemento “JUPITER” indica que es un router, el elemento “ORION” indica que es un servidor, etc.).</p> <p><input type="checkbox"/> 1.2.- ¿Identifica a los responsables de los elementos? Evidencia: Cada elemento del inventario tiene especificado quién es su responsable (p. ej.: el responsable del router es el responsable de comunicaciones).</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<input type="checkbox"/> 1.3.- ¿Se mantiene actualizado? <i>Evidencia: Dispone de un procedimiento documentado que especifica el responsable y la frecuencia de su revisión y/o actualización. El inventario refleja que la fecha de última revisión y/o actualización concuerda con la especificada en el procedimiento.</i> Consultar guías: Serie CCN-STIC-800		
op.exp.2	Configuración de seguridad Básica	<input type="checkbox"/> 1.- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación? <i>Evidencia: Dispone de un procedimiento documentado que indica las actividades a realizar en los sistemas (perfil de seguridad) para su configuración segura previa a su entrada en operación. Dicho procedimiento está avalado por una autoridad reconocida (p. ej.: plantillas de seguridad y recomendaciones de bastionado del CCN. Existe evidencia documental (p. ej.: checklist) de la fortificación realizada a los sistemas, indicando la persona que lo realizó y la fecha y la versión del procedimiento que utilizó.</i> Respecto a dicho procedimiento de bastionado: <input type="checkbox"/> 1.1.- ¿Indica que se retiren las cuentas y contraseñas	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>estándar? <i>Evidencia: El procedimiento indica que se retiren las cuentas y contraseñas estándar (p. ej.: los servidores Linux no deben tener la cuenta “root”, los servidores Windows no deben tener la cuenta “administrador” ni “invitado”, etc.). Solicitar el listado de usuarios para comprobar que no existen cuentas que se han debido retirar según el procedimiento.</i></p> <p><input type="checkbox"/> 1.2.- ¿Indica que el sistema proporcione la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad? <i>Evidencia: El procedimiento indica que se desactiven las funcionalidades no requeridas, ni necesarias, ni de interés o inadecuadas, ya sean gratuitas, de operación, administración o auditoría (p. ej.: si se adquiere un firewall para proteger el perímetro y este proporciona la funcionalidad de acceso remoto mediante VPN IPSec, si dicha funcionalidad añadida no es necesaria ni ha sido solicitada por el responsable deberá haber sido deshabilitada), así como que éstas queden documentadas y el motivo de que se hayan deshabilitado.</i></p> <p><input type="checkbox"/> 2.- Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. ¿indica el sistema esa posibilidad</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>al usuario, y tiene éste que dar su consentimiento expreso asumiendo el riesgo? <i>Evidencia: Dispone de un procedimiento documentado para registrar qué situaciones pueden poner en riesgo la seguridad y asegurar que estas requieren el consentimiento expreso del usuario. Si el usuario realiza una acción que puede poner en riesgo la seguridad pero la organización la consiente bajo la responsabilidad del usuario (p. ej.: exportar un listado de datos de carácter personal para un tratamiento específico conocido por la organización, pero que requiere crear un fichero temporal que debe cumplir las mismas medidas de seguridad que el fichero original), el usuario tendrá que aceptar conscientemente esa posibilidad, su responsabilidad y consecuencias (p. ej.: en ese caso debe aparecerle al usuario una ventana de advertencia, que por defecto tendrá marcada la opción de “no continuar”, informando de esto al usuario y solicitándole la aceptación de las condiciones). Consultar si quedan registros de estos consentimientos de los usuarios.</i></p> <p><input type="checkbox"/> 3.- ¿La configuración por defecto es segura? <i>Evidencia: Por defecto, la configuración del sistema es segura (p. ej.: en caso de que el usuario no haya especificado una clave para un servicio, esta no estará vacía, sino que tendrá una clave preconfigurada –que no sea estándar-).</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: Serie CCN-STIC-500 Guías para Entornos Windows Serie CCN-STIC-600 Guías para otros Entornos Serie CCN-STIC-800 Guías ENS		
op.exp.3	Gestión de la configuración Media	<input type="checkbox"/> 1.- ¿Se gestiona de forma continua la configuración? <i>Evidencia: Cumple los requisitos de las medidas [op.acc.4], [op.exp.2], [op.exp.4] y [op.exp.7]. Dispone de un procedimiento documentado que indica la frecuencia y motivos por los que se debe modificar la configuración del sistema e incluye: la aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema bajo la nueva configuración, y la retención de la configuración previa por un tiempo preestablecido. Consultar si se dispone de copias de seguridad de la configuración actual y la inmediata anterior de los diferentes componentes.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
op.exp.4	Mantenimiento Básica	<input type="checkbox"/> 1.- ¿Dispone de un plan de mantenimiento del equipamiento físico y lógico? <i>Evidencia: Dispone de un procedimiento documentado que indica los componentes a revisar, responsable de la revisión y evidencias a generar. Solicitar evidencias de la ejecución del</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>plan.</i></p> <p>Respecto a dicho plan de mantenimiento:</p> <p><input type="checkbox"/> 1.1.- ¿Atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas? <i>Evidencia: Dispone de las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. El procedimiento refleja dichas especificaciones.</i></p> <p><input type="checkbox"/> 1.2.- ¿Efectúa un seguimiento continuo de los anuncios de defectos? <i>Evidencia: Dispone de mecanismos para el seguimiento continuo de los anuncios de defectos (p. ej.: suscripción a lista de correo de avisos de defectos por parte del fabricante o un proveedor de este tipo de anuncios). Dispone de un procedimiento documentado que indica quién y con qué frecuencia monitorizar esos anuncios.</i></p> <p><input type="checkbox"/> 1.3.- ¿Dispone de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones, teniendo en cuenta el cambio en el riesgo de cara a su priorización? <i>Evidencia: Dispone de un procedimiento documentado que indica quién y con qué frecuencia monitorizar esos anuncios, así</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>como el procedimiento para analizar, priorizar (en función del cambio en el riesgo derivado por la aplicación o no de la recomendación) y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. Dicho procedimiento contempla el proceso para reportar los cambios que pudieran ser necesarios.</p>		
op.exp.5	<p>Gestión de cambios</p> <p>Media</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un control continuo de cambios realizados en el sistema?</p> <p>Evidencia: Dispone de un procedimiento documentado que indica los motivos por los que se debe cambiar un componente del sistema e incluye: la aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema tras el cambio, y la retención de una copia del componente previo por un tiempo preestablecido. Consultar si se dispone de copias de seguridad de la versión del software actual y la inmediata anterior de los diferentes componentes. Este procedimiento se encuentra enlazado con el procedimiento de actualización del inventario de activos, de actualización de los procedimientos operativos relacionados con el componente cambiado y de actualización del plan de continuidad del negocio (si aplica).</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Respecto a dicho control de cambios:</i></p> <p><input type="checkbox"/> 1.1.- <i>¿Analiza todos los cambios anunciados por el fabricante o proveedor para determinar su conveniencia para ser incorporados o no?</i></p> <p><i>Evidencia: Dispone de evidencias del análisis de todos los cambios anunciados, así como del motivo de su aplicación o no.</i></p> <p><input type="checkbox"/> 1.2.- <i>¿Antes de poner en producción una nueva versión o una versión parcheada se comprueba en un equipo que no esté en producción (equivalente al de producción en los aspectos que se comprueban) que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario?</i></p> <p><i>Evidencia: Dicho procedimiento contempla la realización y el registro de pruebas previas a la puesta en producción del cambio (que, quién, cómo y cuándo). Consultar el último cambio realizado, y hacer muestreo, si se considera.</i></p> <p><input type="checkbox"/> 1.3.- <i>¿Se planifican los cambios para reducir el impacto sobre la prestación de los servicios afectados?</i></p> <p><i>Evidencia: Dicho procedimiento contempla la ventana de tiempo en que el cambio afecta en menor medida a los servicios relacionados, realizándose el cambio en dicha ventana si así se</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>estima oportuno. Consultar el último cambio realizado y ver si se realizó en la ventana de tiempo estipulada.</i></p> <p><input type="checkbox"/> 1.4.- <i>¿Se determina mediante análisis de riesgos si los cambios son relevantes para la seguridad del sistema? En caso de que el cambio implique una situación de riesgo de nivel alto ¿es aprobado el cambio explícitamente de forma previa a su implantación?</i></p> <p><i>Evidencia: Dicho procedimiento contempla la actualización previa al cambio del análisis de riesgos (que contempla la situación tras el cambio), la persona responsable de dicha actualización y, en caso de que el riesgo resultante sea alto, requerirá la aprobación explícita del cambio por parte del propietario. Consultar el impacto de los cambios en el análisis de riesgos.</i></p>		
op.exp.6	<p>Protección frente a código dañino</p> <p>Básica</p>	<p><input type="checkbox"/> 1.- <i>¿Dispone de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y “malware” en general)?</i></p> <p><i>Evidencia: Dispone de un procedimiento documentado que indica, entre las actividades a realizar en los sistemas (perfil de seguridad) para su configuración segura previa a su entrada en</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>operación ([op.exp.2]), el uso de mecanismos de prevención frente a código dañino para todos los equipos (servidores y puestos de trabajo). Dispone de un procedimiento documentado que define la reacción frente a código dañino. Consultar si este tipo de sistemas disponen de herramientas de prevención de código dañino.</i></p> <p>Respecto a dichos mecanismos frente a código dañino:</p> <p><input type="checkbox"/> 1.1.- ¿Siguen un mantenimiento conforme a las recomendaciones del fabricante?</p> <p><i>Evidencia: Dispone de las recomendaciones del fabricante. Las opciones de configuración aplicadas son las recomendadas por el fabricante (p. ej.: análisis de ejecución de programas, análisis de correo entrante y saliente, bloqueo automático de código dañino, etc.), así como las referentes a frecuencia de actualización; en caso contrario está documentado el motivo. Comprobar la gestión ante posibles ataques, infecciones, etc...</i></p>		<p><u>Observaciones auditoría:</u></p>
op.exp.7	<p>Gestión de <u>incidentes</u></p> <p>Media</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema?</p> <p><i>Evidencia: Dispone de un procedimiento documentado para la gestión de incidentes. Consultar incidentes de este tipo y, si no</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>existe ninguno y ha pasado mucho tiempo desde que se implantó el procedimiento, consultar si se ha analizado el motivo por el que no se ha detectado ningún incidente (p. ej.: porque no se han producido incidentes de seguridad, o porque el personal desconoce el procedimiento y por lo tanto no los reporta, etc.).</i></p> <p>Respecto a dicho procedimiento:</p> <p><input type="checkbox"/> 1.1.- ¿Incluye el reporte tanto de incidentes, como de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación?</p> <p><i>Evidencia: Dicho procedimiento contempla el reporte tanto de incidentes como de eventos de seguridad como debilidades (p. ej.: aumento considerable de logs de error, ralentización del servicio, etc.), bien sean internos o provenientes de servicios prestados por terceras partes, así como el detalle del proceso de escalado de la notificación (p. ej.: un usuario final debe comunicar el incidente al centro de soporte, este analiza si es un incidente de seguridad, en cuyo caso lo reporta al técnico responsable de estos incidentes, etc.). Se dispone de sistemas de notificación automatizada de incidentes.</i></p> <p><i>Consultar si existen incidentes reportados de estos tipos y si se ha seguido el proceso de escalado de la notificación.</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.2.- ¿Incluye la toma de medidas urgentes, contemplando la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros (según convenga al caso)? <i>Evidencia: Dicho procedimiento contempla la toma de medidas urgentes en base a un procedimiento de valoración de la urgencia, y quién debe tomar esas decisiones. Como resultado de dicha valoración se contemplan las medidas a tomar entre las que se encuentran la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y la protección de los registros (según convenga). Consultar si se han tomado este tipo de medidas y si se ha cumplido el procedimiento.</i></p> <p><input type="checkbox"/> 1.3.- ¿Incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente? <i>Evidencia: Dicho procedimiento contempla la asignación de recursos para investigar las causas del incidente, analizar las consecuencias y resolver el incidente. Consultar si se han tomado este tipo de medidas y si se ha cumplido el procedimiento.</i></p> <p><input type="checkbox"/> 1.4.- ¿Incluye el aviso a las partes interesadas (internas y externas)? <i>Evidencia: Dicho procedimiento contempla el aviso a las partes</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>interesadas tanto internas (p. ej.: avisar a los usuarios de la organización de la indisponibilidad o degradación de un servicio y el tiempo estimado de resolución) como externas (p. ej.: avisar a los ciudadanos u otros organismos relacionados con la organización de la indisponibilidad o degradación de un servicio y el tiempo estimado de resolución). Cuando el incidente se deba a defectos en el equipamiento o tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados o que pudieran causar problemas similares en otras organizaciones, el procedimiento contempla la notificación de los mismos al CERT competente (al CCN-CERT en el caso de organismos del sector público de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categoría de los sistemas en cumplimiento del artículo 36 del ENS). Existe evidencia documental de que se tienen identificadas a las partes interesadas a avisar en caso de incidencia.</i></p> <p><input type="checkbox"/> 1.5.- ¿Incluye medidas de prevención de la repetición del incidente? <i>Evidencia: Dicho procedimiento contempla, dentro de la investigación de las causas, las medidas necesarias para evitar que el incidente vuelva a producirse. Este procedimiento está</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>ligado al de “[op.exp.3] Gestión de la configuración”, “[op.exp.5] Gestión de cambios” y “[op.exp.2] Configuración de seguridad”. Consultar si como resultado de un incidente se ha determinado que era necesario modificar un procedimiento para que no volviera a ocurrir y efectivamente se ha modificado el mismo.</i></p> <p><input type="checkbox"/> 1.6.- ¿Incluye en los procedimientos de usuario la identificación y forma de tratar el incidente? <i>Evidencia: Dispone de un procedimiento documentado para la gestión de incidentes orientado al usuario final, de forma que este sepa identificar y resolver los incidentes más comunes. Consultar a un usuario final para constatar que conoce este procedimiento.</i></p> <p><input type="checkbox"/> 1.7.- ¿Incluye el actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes? <i>Evidencia: El procedimiento de gestión de incidentes contempla su revisión periódica o a raíz de la identificación de posibles mejoras en el mismo.</i></p> <p><input type="checkbox"/> 1.8.- En caso de afectar el incidente a ficheros con datos de carácter personal ¿contempla su gestión además lo dispuesto</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>en la legislación vigente de tratamiento de datos de carácter personal? <i>Evidencia: Dicho procedimiento establece el identificar si el incidente afecta a ficheros con datos de carácter personal y, en caso de que así sea, está alineado o integrado con el de gestión de incidentes de la legislación aplicable de tratamiento de datos de carácter personal (relacionado con [mp.info.1]). Verificar registros de incidentes.</i></p> <p>Consultar guías: CCN-STIC-403 <i>Gestión de incidentes de seguridad</i> CCN-STIC-817 <i>Gestión de Incidentes de Seguridad</i> CCN-STIC-845A <i>LUCIA. Manual de Usuario</i> CCN-STIC-845B <i>LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT)</i> CCN-STIC-845C <i>LUCIA. Manual Instalación Organismo</i> CCN-STIC-845D <i>LUCIA. Manual de Administrador</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.exp.8	<p>Registro de la actividad de los usuarios</p> <p>- T / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se registran todas las actividades de los usuarios en el sistema especialmente activando los registros de actividad en los servidores?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que indica que se deben registrar todas las actividades de los usuarios en el sistema. Existen mecanismos para aplicar dicha política o normativa y dichos mecanismos están activados.</i></p> <p>Respecto a dichos registros:</p> <p><input type="checkbox"/> 1.1.- ¿La determinación de las actividades a registrar y su nivel de detalle se determina en base al análisis de riesgos del sistema?</p> <p><i>Evidencia: La política o normativa los establece en base al resultado del análisis de riesgos ([op.pl.1]).</i></p> <p><input type="checkbox"/> 1.2.- ¿Indican quién realiza la actividad, ¿cuándo la realiza y sobre qué información, sea cual sea el usuario?</p> <p><i>Evidencia: Dicha política o normativa establece qué se debe registrar quién realiza la actividad, cuándo la realiza y sobre qué información. Dispone de un procedimiento documentado relacionado con “[op.exp.2] Configuración de seguridad” en el que se detalla los mecanismos a utilizar para mantener el reloj del sistema en hora. Consultar si los mecanismos de registro</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>almacenan esta información (p. ej.: la lectura por un humano de ese registro podría ser que el usuario user34 el 16-10-2010 a las 14:59:37 modificó la tupla 328 de la base de datos “trámites”).</i></p> <p><input type="checkbox"/> 1.3.- ¿Incluye la actividad de los operadores y administradores del sistema? <i>Evidencia: Dicha política o normativa establece que se debe registrar la actividad de los operadores y administradores del sistema. Consultar si los mecanismos de registro almacenan los accesos a la configuración del sistema de forma que los propios operadores y administradores no puedan modificarlos.</i></p> <p><input type="checkbox"/> 1.4.- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados? <i>Evidencia: Dicha política o normativa establece que se debe registrar tanto las actividades realizadas con éxito como los intentos fracasados. Consultar si los mecanismos de registro almacenan ambos.</i></p> <p>Consultar guías:</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-434 Herramientas para análisis de ficheros de log		
	- T / Medio	<input type="checkbox"/> 1.- ¿Se revisan informalmente los registros de actividad en busca de patrones anormales? <i>Evidencia: Dicha política o normativa establece que se debe revisar periódicamente los registros de actividad para detectar posibles acciones sospechosas o ilícitas. Consultar posibles resultados de estas revisiones informales.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
	- T / Alto	<input type="checkbox"/> 3.- ¿Se dispone de un sistema automático de recolección de registros y correlación de eventos? <i>Evidencia: Dispone de una consola de seguridad centralizada que revise y centralice los registros de actividad automáticamente. Existen herramientas para analizar los registros en busca de actividades fuera de lo normal. Comprobar el resultado del análisis y posibles actividades inusuales.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.exp.9	Registro de la gestión de incidentes			
	Media	<p><input type="checkbox"/> 1.- ¿Se registran todas las actuaciones relacionadas con la gestión de incidentes ([op.exp.7])? <i>Evidencia: Dispone de un procedimiento documentado para la gestión de incidentes que incluye mantener un registro de todas las actuaciones relacionadas con la gestión de las mismas. Existe evidencia documental de los registros generados durante la gestión de incidentes.</i></p> <p>Respecto a dicho registro de los incidentes:</p> <p><input type="checkbox"/> 1.1.- ¿Se registran el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente? <i>Evidencia: El procedimiento de gestión de incidentes ([op.exp.7]) cubre el registro de estas acciones. Este procedimiento está ligado al de “[op.exp.3] Gestión de la configuración” y “[op.exp.5] Gestión de cambios”. Existe evidencia documental de estos registros.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se registran aquellas evidencias que puedan, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos?</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: En la determinación de la composición y detalle de estas evidencias se ha recurrido a asesoramiento legal especializado, y se ha implantado conforme a sus recomendaciones. Dispone de un procedimiento documentado para la retención de evidencias que puedan sustentar o hacer frente a una demanda judicial tras un incidente. Consultar si el personal responsable de estas actividades conoce el procedimiento y dispone de los medios para ponerlos en práctica.</i></p> <p><input type="checkbox"/> 2.- ¿Se revisa la determinación de los eventos auditables en base al análisis de los incidentes?</p> <p><i>Evidencia: Dispone de un procedimiento documentado para el análisis de los incidentes que alimente la determinación de qué eventos deben ser auditados.</i></p> <p>Consultar guías: CCN-STIC-817 Gestión de ciberincidentes CCN-STIC-845A LUCIA. Manual de Usuario CCN-STIC-845B LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT) CCN-STIC-845C LUCIA. Manual Instalación Organismo CCN-STIC-845D LUCIA. Manual de Administrador</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.exp.10	-T / Alto	<p><i>Protección de los registros de actividad</i></p> <p><input type="checkbox"/> 1.- ¿Se encuentran protegidos los registros del sistema? <i>Evidencia: Dispone de un inventario de los registros de actividad, donde además se recoge el personal autorizado a su acceso, modificación o eliminación. Dispone de un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención.</i></p> <p>Respecto a dichos registros:</p> <p><input type="checkbox"/> 1.1.- ¿Está determinado el periodo de retención de los mismos? <i>Evidencia: Dispone de un procedimiento documentado del periodo de retención de los mismos, que establece además del periodo de retención de evidencias tras un incidente. El inventario de registros recoge el periodo de retención de los mismos. Dispone de un procedimiento documentado para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen). Consultar si la antigüedad de los registros concuerda con el periodo de retención establecido.</i></p> <p><input type="checkbox"/> 1.2.- ¿La fecha y hora de los mismos está asegurada? <i>Evidencia: Dispone de mecanismos para garantizar la fecha y hora de su generación conforme a [mp.info.5]. Constatar que la</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>fecha y hora de diversos sistemas, sobre todo de aquellos que generan o almacenan registros de actividad, es la correcta.</i></p> <p><input type="checkbox"/> 1.3.- ¿Se encuentran protegidos frente a su modificación o eliminación por personal no autorizado? <i>Evidencia: Dispone de mecanismos que impiden el acceso, modificación o eliminación de registros o configuración de la generación de los mismos por personal no autorizado. Consultar la lista de accesos autorizados y constatar que no hay ninguna incompatibilidad conforme a lo establecido en “[op.acc.3] Segregación de funciones y tareas”.</i></p> <p><input type="checkbox"/> 1.4.- ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos? <i>Evidencia: Dispone de una política o normativa de seguridad que determina los niveles de seguridad a aplicar a las copias de seguridad, si existen, de los registros alineada con los requisitos establecidos a los registros en vivo. Constar que las medidas de seguridad aplicadas a las copias de seguridad cumplen lo indicado en dicha política o normativa.</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.exp.11	<p><i>Protección de claves criptográficas</i></p> <p>Básica</p>	<p><input type="checkbox"/> 1.- ¿Se protegen las claves criptográficas durante todo su ciclo de vida? <i>Evidencia: Dispone de un procedimiento documentado para su protección durante su generación, transporte al punto de explotación (p. ej.: entrega en mano, uso de contenedores físicos seguros o criptográficos, doble canal –clave y datos de activación por separado-), custodia durante la explotación, archivo posterior a su retirada de explotación activa y destrucción final (p. ej.: eliminación de original y copias). Consultar si se cumple dicho procedimiento.</i></p> <p><input type="checkbox"/> 2.- ¿Se utilizan medios de generación aislados de los medios de explotación? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los medios de generación deben estar aislados de los medios de explotación. Consultar si se generan conforme a dicha política o normativa.</i></p> <p><input type="checkbox"/> 3.- ¿Las claves retiradas de operación que deban ser archivadas, lo son en medios aislados de los de explotación? <i>Evidencia: Dispone de una política o normativa documentada que especifica que las claves retiradas de operación que deban ser archivadas, lo son en medios aislados de los de explotación.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Consultar si se archivan en contenedores físicos seguros (p. ej.: en una caja fuerte) o en contenedores criptográficos.</i></p> <p>Consultar guías: CCN-STIC-807 Criptografía de empleo en el ENS</p>		
	<p>Media</p>	<p><input type="checkbox"/> 4.- ¿Se utilizan medios de generación y custodia en explotación evaluados o dispositivos criptográficos certificados? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los medios de generación y custodia en explotación deben haber sido evaluados o tratarse de dispositivos criptográficos certificados conforme a [op.pl.5]. Consultar la evaluación o certificación de los medios de generación.</i></p> <p><input type="checkbox"/> 5.- ¿Los medios de generación y custodia en explotación emplean algoritmos acreditados por el CCN? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los medios de generación deben emplear algoritmos acreditados por el CCN. Consultar la acreditación de los algoritmos.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<input type="checkbox"/> 6.- ¿Los medios de custodia en explotación están protegidos? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los medios de custodia en explotación deben emplear tarjeta inteligente protegida por contraseña. Solicitar una tarjeta inteligente y observar su uso.</i>		
op.ext	SERVICIOS EXTERNOS			
op.ext.1	Contratación y acuerdos de nivel de servicio			
	Media	<input type="checkbox"/> 1.- ¿Se han analizado los riesgos de la contratación de servicios externos? <i>Evidencia: El análisis de riesgos identifica los riesgos asociados al proveedor externo.</i> Previamente a la utilización de recursos externos se ha establecido: <input type="checkbox"/> 1.1.- ¿Las características del servicio prestado? <i>Evidencia: Dispone de un procedimiento documentado de pasos previos a la contratación de servicios externos que requiere el detalle por parte del proveedor de las características del servicio a prestar, y estos satisfacen los requisitos de servicio y seguridad requeridos y aprobados previamente. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de las características del servicio.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.2.- ¿Lo que se considera calidad mínima y las consecuencias de su incumplimiento? <i>Evidencia: Dicho procedimiento requiere también el detalle de lo que se considera calidad mínima y las consecuencias para el proveedor de su incumplimiento. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de la calidad mínima exigida (acuerdo de nivel de servicio) y las consecuencias de su incumplimiento y posibles penalizaciones en su caso.</i></p> <p><input type="checkbox"/> 1.3.- ¿Las responsabilidades de las partes? <i>Evidencia: Dicho procedimiento requiere también el establecimiento de las funciones o roles, obligaciones y responsabilidades de cada parte. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de las responsabilidades de las partes.</i></p> <p>Consultar guías: CCN-STIC-823 <i>Utilización de Servicios en la nube</i></p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
op.ext.2	<p>Gestión diaria</p> <p>Media</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio? <i>Evidencia: Dispone de un procedimiento documentado que define la frecuencia de medición del cumplimiento de las obligaciones de servicio, el responsable de dicha medición y el protocolo de actuación en caso de incumplimiento. El seguimiento requerido podría estar incluido en el contrato (informes a realizar, revisiones, monitorización...) Consultar los resultados de las mediciones.</i></p> <p><input type="checkbox"/> 2.- ¿Dispone de un procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado? <i>Evidencia: Dicho procedimiento contempla un protocolo de actuación en caso de incumplimiento o degradación en la calidad acordada en [op.ext.1]. Consultar si se ha detectado algún incumplimiento de las obligaciones de servicio y qué actuación se ha llevado a cabo.</i></p> <p><input type="checkbox"/> 3.- ¿Se han establecido el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo? <i>Evidencia: Dispone de un procedimiento documentado que define el mecanismo y los procedimientos de coordinación para</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo (p. ej.: si el proveedor externo se ocupa del mantenimiento de un servidor, se tendrá que acordar cómo podrá acceder al CPD para sus labores in-situ de mantenimiento, o si el proveedor externo proporciona servicios de conectividad y estos deben sufrir un corte por una tarea de su mantenimiento se debe acordar en qué momento se llevará a cabo, etc.). Consultar si se está cumpliendo el procedimiento.</i></p> <p><input type="checkbox"/> 4.- ¿Se han establecido el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres? <i>Evidencia: El procedimiento de gestión de incidentes sobre el servicio externo estará relacionado con el definido en [op.exp.7]. Consultar si se está cumpliendo el procedimiento.</i></p>		
op.ext.9	<p>Medios alternativos</p> <p>- D / Alto</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un plan para reemplazar el servicio por medios alternativos en caso de indisponibilidad del servicio contratado? <i>Evidencia: Dispone de un plan para reemplazar el servicio por medios alternativos en caso de indisponibilidad del servicio contratado dentro del plazo acordado en el plan de continuidad de la organización ([op.cont]). En caso de que el plan cuente</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>con disponer de medios alternativos, consultar si se dispone de los medios alternativos (p. ej.: servidor de sustitución, switch de sustitución, CPD alternativo, etc.).</i></p> <p><input type="checkbox"/> 2.- ¿El servicio alternativo ofrece las mismas garantías de seguridad que el servicio habitual? <i>Evidencia: Las características del servicio alternativo incluyen las mismas garantías de seguridad que el servicio habitual.</i></p> <p><input type="checkbox"/> 3.- ¿El plan de reemplazamiento de servicios se vertebra dentro del plan de continuidad de la organización? <i>Evidencia: El “[op.cont.2] Plan de continuidad” contempla el uso de medios alternativos.</i></p>		
<i>op.cont</i>	CONTINUIDAD DEL SERVICIO			
<i>op.cont.1</i>	Análisis del impacto			
	- D / Medio	<p><input type="checkbox"/> 1.- ¿Se ha realizado un análisis de impacto? <i>Evidencia: Dispone de un mecanismo para el análisis de impacto de una contingencia en la continuidad del servicio, este contempla el responsable del mismo, su revisión periódica o actualización tras cambios en los sistemas (ligado a [op.exp.3], [op.exp.4] y [op.exp.5]). En caso de que el mecanismos se refleje en un procedimiento documentado consultar el último análisis de impacto, así como el hecho que haya motivado su</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>posible revisión o actualización.</i></p> <p>Respecto a dicho análisis de impacto:</p> <p><input type="checkbox"/> 1.1.- ¿Identifica los requisitos de disponibilidad de cada servicio?</p> <p><i>Evidencia: Dicho análisis de impacto identifica los requisitos de disponibilidad de cada servicio (medido como el impacto de una interrupción durante un cierto periodo de tiempo). Entre esos requisitos se encuentra la identificación del tiempo máximo de datos que se pueden perder, lo que se tiene contemplado en la frecuencia de las copias de seguridad y su gestión.</i></p> <p><input type="checkbox"/> 1.2.- ¿Identifica los elementos que son críticos para la prestación de cada servicio?</p> <p><i>Evidencia: Dicho análisis de impacto identifica los elementos que son críticos para la prestación de cada servicio, bien sean propios o proporcionados por externos.</i></p> <p>Consultar guías: Serie CCN-STIC-470 Manual de usuario de PILAR</p>		
op.cont.2	Plan de continuidad - D / Alto	<input type="checkbox"/> 1.- ¿Dispone de un plan de continuidad? <i>Evidencia: Dispone de un plan de continuidad que establece las acciones a ejecutar en caso de interrupción de los servicios</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento:

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>prestados con los medios habituales. Dicho plan contempla su revisión periódica o actualización tras cambios en los sistemas (ligado a [op.exp.3], [op.exp.4] y [op.exp.5]), los servicios y su calidad.</i></p> <p>Respecto a dicho plan:</p> <p><input type="checkbox"/> 1.1.- ¿Identifica funciones, responsabilidades y actividades a realizar?</p> <p><i>Evidencia: Dicho plan define quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y evaluar las consecuencias, quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis y quiénes se encargan de reconstruir el sistema de información (recuperación del desastre), definiendo para cada función las actividades a realizar. Estas funciones no son incompatibles según [op.acc.3], o en caso de serlo está motivado y aprobado por la Dirección. En caso de que las funciones se hayan asignado a roles, existe un documento que permite identificar los roles con las personas nominales. Las personas aceptan formalmente sus obligaciones en el plan.</i></p> <p><input type="checkbox"/> 1.2.- ¿Existe una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios?</p> <p><i>Evidencia: Dicho plan identifica los medios alternativos que</i></p>	<p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>serán necesarios para poder seguir prestando los servicios: instalaciones alternativas ([mp.if.9]), comunicaciones alternativas ([mp.com.9]), equipamiento alternativo ([mp.eq.9]), personal alternativo ([mp.per.9]) y recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto ([mp.info.9] y [mp.cont.1]). En caso de que el plan cuente con disponer de medios alternativos, consultar si se dispone de los medios alternativos (p. ej.: servidor de sustitución, switch de sustitución, CPD alternativo, etc.).</i></p> <p><input type="checkbox"/> 1.3.- ¿Están los medios alternativos planificados y materializados en acuerdos o contratos con los proveedores correspondientes? <i>Evidencia: Dicho plan contempla los acuerdos o contratos firmados con los proveedores correspondientes necesarios para la continuidad del servicio de forma que la coordinación de todos los elementos alcance la restauración en el plazo estipulado. Existen documentos para establecer puntos de contacto, obligaciones y canales de comunicación con los proveedores para la sincronización de la recuperación de un desastre. Consultar los contratos.</i></p> <p><input type="checkbox"/> 1.4.- ¿Han recibido las personas afectadas por el plan la</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>formación específica relativa a su papel en el mismo? <i>Evidencia: Dicho plan identifica las necesidades de formación del personal involucrado en el mismo, así como la planificación de su impartición. Consultar registros de asistencia o recepción de la formación.</i></p> <p><input type="checkbox"/> 1.5.- ¿Es parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad? <i>Evidencia: Se han identificado los posibles planes de continuidad existentes en la organización, y en caso de existir se han integrado con éste. Dispone de un procedimiento documentado para la actualización de cualquier parte del plan de continuidad que afecte a los ya existentes.</i></p>		
op.cont.3	<p>Pruebas periódicas</p> <p>- D /Alto</p>	<p><input type="checkbox"/> 1.- ¿Se realizan pruebas periódicas para localizar y corregir, en su caso, los errores o deficiencias que puedan existir en el plan de continuidad? <i>Evidencia: Dispone de un procedimiento documentado que indica la responsabilidad de la elaboración de un plan de pruebas, la frecuencia en la ejecución de dicho plan, la forma de llevar a cabo las pruebas, los integrantes en las mismas, la elaboración del informe resultante tras las pruebas, el análisis</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>de dicho informe y la elaboración de un plan de mejoras (tanto en medios como en procedimientos, concienciación o formación de las personas implicadas). Consultar el informe de la última prueba y, si se han identificado acciones de mejora, que las mismas se hayan ejecutado.</p>		
op.mon	MONITORIZACIÓN DEL SISTEMA			
op.mon.1	Detección de intrusión			
	<p>Media</p>	<p><input type="checkbox"/> 1.- ¿Dispone de herramientas de detección o prevención de intrusión?</p> <p><i>Evidencia: Dispone de herramientas de detección o prevención de intrusión que se encuentran operativas. Dispone de un documento de análisis de ubicación de estas herramientas y su correcta configuración (p. ej.: recomendaciones del fabricante respecto a los sistemas a monitorizar, protocolos a inspeccionar, etc.), atendiendo al análisis de riesgos. Dispone de un procedimiento documentado que indica la frecuencia de su actualización (relacionado con [op.exp.4]), la responsabilidad en la atención a las alarmas, y la frecuencia y responsabilidad en la revisión y análisis de los registros.</i></p> <p>Consultar guías: CCN-STIC-432 Seguridad Perimetral - Detección de Intrusos CCN-STIC-434 Herramientas de análisis de logs CCN-STIC-435 Herramientas de Monitorización de Tráfico</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-818 <i>Herramientas de seguridad</i> CCN-STIC-953 <i>Recomendaciones empleo herramienta Snort</i>		
op.mon.2	Sistema de métricas Baja	<input type="checkbox"/> 1.- ¿Se recopilan los datos necesarios atendiendo a la categoría del Sistema para conocer el grado de implantación de las medidas de seguridad y en su caso para proveer el informe anual requerido en el artículo 35 del ENS de acuerdo con la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad (ITS INES)? <i>Evidencia: Dispone de un mecanismo para la asignación de la responsabilidad en la recopilación de los datos solicitados que en general, estarán referidos a identificación de la entidad, datos generales, organización de la seguridad, procesos críticos, concienciación y formación, gestión de incidentes, recursos y presupuestos, auditoría, indicadores críticos de riesgo y medidas de seguridad, según lo descrito en la guía de seguridad CCN-STIC-815 sobre Métricas e Indicadores para el Esquema Nacional de Seguridad. En la guía CCN-STIC 824 ENS Informe del Estado de Seguridad, para cada dato solicitado se contempla el objetivo que se pretende medir, el origen de la información, el procedimiento de recogida y tratamiento de los</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>datos, la frecuencia de recogida de datos y de presentación de resultados y los criterios de valoración de los indicadores resultantes a efectos de reaccionar y tomar decisiones. Se dispone de acceso a la herramienta INES (Informe Nacional del Estado de la Seguridad). Existe evidencia documental de dichos datos.</i></p> <p>Respecto a dichos valores:</p> <p><input type="checkbox"/> 1.1.- ¿Miden el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35 Informe del estado de la seguridad?</p> <p><i>Evidencia: Existe un conjunto de datos e indicadores para medir el grado de implantación de las medidas de seguridad. Consultar los valores, su frecuencia de actualización y las medidas tomadas a cabo a raíz de su análisis. Consultar el último informe del estado de seguridad.</i></p> <p>Consultar guías:</p> <p>CCN-STIC-815 Métricas e indicadores CCN-STIC-824 Informe nacional del estado de seguridad CCN-STIC-827 Gestión y uso de dispositivos móviles CCN-STIC-844 INES – Informe Nacional del Estado de Seguridad - Manual de Usuario</p>		

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	Media	<p><input type="checkbox"/> 1.2.- ¿Permiten valorar el sistema de gestión de incidentes? <i>Evidencia: Existe un conjunto de datos e indicadores asociados de acuerdo a la ITS Inés para valorar el sistema de gestión de incidentes que permita conocer: el número de incidentes de seguridad tratados; el tiempo empleado para cerrar el 50% de los incidentes; y el tiempo empleado para cerrar el 90% de los incidentes. La herramienta del CCN LUCIA (gestión de ciberincidentes) permite valorar el sistema de gestión de incidentes.</i></p> <p>Consultar guías: CCN-STIC-815 Métricas e indicadores CCN-STIC-817 Gestión de Ciberincidentes CCN-STIC-845A – LUCIA. Manual de Usuario CCN-STIC-845B – LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT) CCN-STIC-845C – LUCIA. Manual Instalación Organismo CCN-STIC-845D – LUCIA. Manual de Administrador CCN-STIC-824 Informe nacional del estado de seguridad CCN-STIC-844 INES – Informe Nacional del Estado de Seguridad - Manual de Usuario</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
	Alta	<p><input type="checkbox"/> 1.3.- ¿Miden la eficiencia de las medidas de seguridad incluyendo recursos consumidos?</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p>

Aptdo.	Categoría – Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Existe un conjunto de valores indicados en la ITS Inés para medir la eficiencia de las medidas de seguridad incluyendo recursos consumidos. Consultar los recursos de las horas y presupuestos consumidos, los valores, su frecuencia de actualización y las medidas tomadas a cabo a raíz de su análisis.</i></p>	<p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

5.2.3 MEDIDAS DE PROTECCIÓN

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp	MEDIDAS DE PROTECCIÓN			
mp.if	PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS			
mp.if.1	Áreas separadas y con control de acceso			
	Baja	<input type="checkbox"/> 1.- ¿El equipamiento ha sido instalado en áreas separadas específicas para su función? <i>Evidencia: Dispone de una política o normativa documentada que especifica que los sistemas se encuentran en áreas separadas específicas para su función (p. ej.: los servidores se encuentran en una sala independiente). Dispone de un inventario donde se indican las salas separadas existentes. Examinar dichas salas y constatar que cumplen la política o normativa.</i> Respecto a dichas áreas separadas: <input type="checkbox"/> 1.2.- ¿Se controlan los accesos? <i>Evidencia: Dispone de una política o normativa documentada que especifica que el acceso a las áreas separadas se encuentra controlado (p. ej.: para acceder a la sala de servidores es necesario tener la llave de la puerta de acceso, que es la única vía de acceso) y vigilado (p. ej.: dispone de una cámara de vigilancia que controla el acceso a la sala, o la cerradura es electrónica y registra el código de acceso independiente de cada persona que accede, o el procedimiento de acceso especifica que</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>la persona que accede pone su nombre y firma en un listado de entradas, etc.). Examinar el acceso a dichas salas y constatar que cumplen la política o normativa.</p>		
mp.if.2	<p>Identificación de las personas</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Se dispone de un mecanismo de control de acceso a los locales donde hay equipamiento que forme parte del sistema de información? <i>Evidencia: Dispone de un mecanismo que establece un control de acceso a los locales especificados</i> Respecto a dicho control de acceso:</p> <p><input type="checkbox"/> 1.1.- ¿Se identifican a todas las personas que accedan a estos locales? <i>Evidencia: Dispone de un procedimiento documentado que especifica que cada persona que accede debe ser identificada. Constatar este hecho solicitando acceso a los registros correspondientes.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se registran las entradas y salidas de personas? <i>Evidencia: Dicho procedimiento, que cumple los requisitos de la legislación vigente de tratamiento de datos de carácter personal, especifica que para cada persona debe quedar registrada inequívocamente junto con su fecha y hora de entrada y salida, así como la persona o mecanismo por el que se realiza el</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>registro. Consultar el registro de accesos.</i>		
<i>mp.if.3</i>	<p>Acondicionamiento de los locales</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Los locales donde se ubican los sistemas de información y sus componentes disponen de las adecuadas condiciones de temperatura y humedad?</p> <p><i>Evidencia: Dispone de elementos adecuados en el local para mantener las adecuadas condiciones de temperatura y humedad y que se encuentren en los márgenes especificados por los fabricantes de los equipos. Consultar si hay aire acondicionado, termómetro e higrómetro en el CPD, si se monitorizan de forma periódica y si se encuentran en los valores recomendados.</i></p> <p>Respecto a dichos locales:</p> <p><input type="checkbox"/> 1.1.- ¿Cuentan con protección frente a las amenazas identificadas en el análisis de riesgos?</p> <p><i>Evidencia: Dicho local cuenta con protección frente a las amenazas identificadas en el análisis de riesgos tanto de índole natural como derivadas del entorno o con origen humano, accidental o deliberado (complementando [mp.if.1], [mp.if.4], [mp.if.5], [mp.if.6] y [mp.if.7]. Consultar las medidas existentes (p. ej.: prohibiendo la existencia de material innecesario en el</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>local, en particular material inflamable (papel, cajas, etc.) o que pueda ser causa de otros incidentes (fuentes de agua, plantas, etc.), y evitando que el propio local sea una amenaza o que provoque otras amenazas si el análisis de riesgos ha identificado como amenaza un incendio, se debe disponer de salvaguardas para ello como extintores, sensores de humo, etc.).</i></p> <p><input type="checkbox"/> 1.2.- ¿Cuentan con protección del cableado frente a incidentes fortuitos o deliberados?</p> <p><i>Evidencia: Se contempla la protección del cableado mediante su etiquetado (para poder determinar las conexiones de cada cable físico), protección (para evitar tropiezos) y control (para evitar la existencia de cableado fuera de uso). Constatar la existencia de estas medidas.</i></p>		
mp.if.4	Energía eléctrica - D / Bajo	<p><input type="checkbox"/> 1.- ¿Se dispone de las tomas eléctricas necesarias?</p> <p><i>Evidencia: El local debe contar con las tomas eléctricas necesarias. Consultar que se cumple (p. ej.: enchufes con toma de tierra, cantidad de enchufes suficiente para no tener que recurrir a multiplicadores en cascada que superen la potencia eléctrica máximas recomendadas, etc.).</i></p> <p><input type="checkbox"/> 2.- ¿Se garantiza el suministro de potencia eléctrica?</p> <p><i>Evidencia: El local debe contar con la potencia eléctrica necesaria. Dispone de un análisis de la potencia eléctrica</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>necesaria, que se actualiza antes de la adquisición de nuevos componentes. Consultar si el contrato de suministro cubre la potencia eléctrica necesaria.</i></p> <p><input type="checkbox"/> 3.- ¿Se garantiza el correcto funcionamiento de las luces de emergencia? <i>Evidencia: El local debe contar con luces de emergencia y un mecanismo para comprobar el correcto funcionamiento de las luces de emergencia. Constatar que existen luces de emergencia. Existe evidencia documental de la revisión de las luces de emergencia.</i></p>		
	- D / Medio	<p><input type="checkbox"/> 4.- ¿Se garantiza el suministro de potencia eléctrica en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información? <i>Evidencia: El local debe contar con un sistema de alimentación ininterrumpida (compuesto por Sistema de Alimentación Ininterrumpida y, en caso de ser necesario, grupo electrógeno) para todo el sistema que garantice el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información. Consultar si el SAI cumple con los requisitos identificados en el análisis de la potencia eléctrica necesaria. Consultar los registros de las pruebas que se hayan llevado a cabo para constatar que el SAI soporta el tiempo necesario para</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>la terminación ordenada. ¿Cada cuánto se realizan las pruebas? ¿Se realiza pruebas de carga o vacío? ¿Cada cuánto se cambian las baterías?</i>		
mp.if.5	Protección frente a incendios - D / Bajo	<input type="checkbox"/> 1.- ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incendios fortuitos o deliberados? <i>Evidencia: Los locales cuentan con protección frente a incendios conforme a la normativa industrial pertinente (p. ej.: disponer de carteles para evacuación, extintores, materiales no inflamables, etc.). Dispone de la normativa industrial pertinente y se encuentra aplicada.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
mp.if.6	Protección frente a inundaciones - D / Medio	<input type="checkbox"/> 1.- ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incidentes fortuitos o deliberados causados por el agua? <i>Evidencia: Los locales se protegen frente a incidentes fortuitos o deliberados causados por el agua (p. ej.: que el CPD no sea recorrido por tuberías de agua, que existan sumideros de agua en el CPD, etc.) conforme al nivel de riesgo identificado. Se ha realizado un estudio de la ubicación física del local para conocer el riesgo real de problemas por causa natural o por el entorno en</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>el que se encuentra (p. ej.: si se encuentra en una ubicación con casos de inundación se puede recomendar el cambio de ubicación o disponer de bombas de achique, etc.)</i>		
<i>mp.if.7</i>	Baja	<input type="checkbox"/> 1.- ¿Se lleva un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento? <i>Evidencia: Se especifica el tipo de equipamiento (incluyendo al menos servidores, portátiles, equipos de comunicaciones y soportes de información) que a su entrada o salida debe ser registrado. El registro debe reflejar: fecha y hora, identificación inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registro. Consultar que el registro de entrada y salida de equipamiento cumple lo especificado.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u> <u>Observaciones auditoría:</u>
<i>mp.if.9</i>	- D /Alta	<input type="checkbox"/> 1.- ¿Está garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles? <i>Evidencia: Consultar la existencia de las instalaciones alternativas (p. ej.: contrato con un proveedor de instalaciones alternativas disponibles en el plazo previsto en el "[op.cont.2]</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>Plan de continuidad</i> ”).		<u>Observaciones auditoría:</u>
<i>mp.per</i>	GESTIÓN DEL PERSONAL			
<i>mp.per.1</i>	<i>Caracterización del puesto de trabajo</i>			
	Media	<input type="checkbox"/> 1.- ¿Se ha caracterizado cada puesto de trabajo? <i>Evidencia: Dispone de una política o normativa documentada que contiene la caracterización de cada puesto de trabajo en materia de seguridad.</i> Respecto a dicha caracterización: <input type="checkbox"/> 1.1.- ¿Define las responsabilidades relacionadas con cada puesto de trabajo? <i>Evidencia: Dicha política o normativa define las responsabilidades relacionadas con cada puesto de trabajo (relacionado con [op.acc.3]), basándose en el análisis de riesgos en la medida en que afecta a cada puesto de trabajo. Revisar la relación de personas asignadas a cada tipo de puesto de trabajo.</i> <input type="checkbox"/> 1.2.- ¿Define los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad? <i>Evidencia: Dicha política o normativa define los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>trabajo, en particular en términos de confidencialidad.</i></p> <p><input type="checkbox"/> 2.- ¿Los requisitos del puesto de trabajo se tienen en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias?</p> <p><i>Evidencia: Dicha política o normativa contempla los requisitos del puesto de trabajo en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias. Consultar la caracterización de un puesto de trabajo, la persona que lo ostenta y sus referencias y comprobar que concuerdan.</i></p>		
mp.per.2	<p>Deberes y obligaciones</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Se informa a cada persona que trabaja en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que especifica la forma de informar a cada persona que trabaja en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, así como la forma de recabar su aceptación explícita y firmada. Dispone de un documento para cada perfil con sus deberes y responsabilidades. Consultar dichos documentos (información y aceptación de deberes y</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>responsabilidades) firmados.</i></p> <p>Respecto a dicha información de deberes y responsabilidades:</p> <p><input type="checkbox"/> 1.1.- ¿Se especifican las medidas disciplinarias a que haya lugar? <i>Evidencia: Dicho documento informa de las medidas disciplinarias a que haya lugar. Obtener evidencia de referencia a convenios o al Estatuto de los trabajadores o a la ley de función pública aplicable.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se especifica que cubre tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de término de la asignación o traslado a otro puesto de trabajo? <i>Evidencia: Dicho documento informa de que las obligaciones se mantienen tanto en el periodo durante el cual se desempeña el puesto como posteriormente, en caso de término de la asignación o traslado a otro puesto de trabajo.</i></p> <p><input type="checkbox"/> 1.3.- ¿Se especifica que el deber de confidencialidad respecto de los datos a los que tenga acceso cubre el periodo durante el cual se desempeña el puesto como en caso de término de la asignación o traslado a otro puesto de trabajo? <i>Evidencia: Dicho documento informa de que las obligaciones de confidencialidad se mantienen tanto en el periodo durante el</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>cual se desempeña el puesto como posteriormente, en caso de término de la asignación o traslado a otro puesto de trabajo.</i></p> <p><input type="checkbox"/> 2.- ¿Se han establecido, en el caso de personal contratado a través de un tercero, los deberes y obligaciones del personal? <i>Evidencia: Dispone de una normativa documentada que especifica los deberes y obligaciones del personal contratado a través de un tercero. Existe evidencia documental de la exigencia de esta normativa (p. ej.: aparece reflejada la normativa en el contrato con el tercero).</i></p> <p>Respecto del personal contratado a través de un tercero:</p> <p><input type="checkbox"/> 2.1.- ¿Se han establecido los deberes y obligaciones de cada parte? <i>Evidencia: Dispone de una normativa documentada que enumera los deberes y obligaciones de cada parte. Existe evidencia documental de la exigencia de esta normativa (p. ej.: aparece reflejada la normativa en el contrato con el tercero).</i></p> <p><input type="checkbox"/> 2.2.- ¿Se ha establecido el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones? <i>Evidencia: Dispone de un procedimiento documentado que define la resolución de incidentes relacionados con el incumplimiento de</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>las obligaciones por parte del personal del tercero. Tiene identificada a la persona de contacto en el tercero para la resolución de este tipo de incidentes.</i></p>		
<p><i>mp.per.3</i></p>	<p>Concienciación Baja</p>	<p><input type="checkbox"/> 1.- ¿Se realizan acciones para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos? <i>Evidencia: Dispone de un procedimiento documentado que indica el responsable de la elaboración del plan de concienciación, así como su periodicidad y contenido. Consultar dicho plan y los registros de su ejecución.</i></p> <p>Respecto a dicha concienciación:</p> <p><input type="checkbox"/> 1.1.- ¿Forma parte del contenido la normativa de seguridad relativa al buen uso de los sistemas? <i>Evidencia: El contenido del plan de concienciación incluye la normativa de seguridad relativa al buen uso de los sistemas.</i></p> <p><input type="checkbox"/> 1.2.- ¿Forma parte del contenido la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado? <i>Evidencia: El contenido del plan de concienciación incluye la</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.</i></p> <p><input type="checkbox"/> 1.3.- ¿Forma parte del contenido el procedimiento de reporte de <i>incidentes</i> de seguridad, sean reales o falsas alarmas? <i>Evidencia: El contenido del plan de concienciación incluye el procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.</i></p>		
mp.per.4	<p>Formación</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Se forma regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones? <i>Evidencia: Dispone de un plan de formación en el que se identifica el responsable de su elaboración, las necesidades formativas de cada puesto de trabajo, así como la planificación en la impartición de la formación necesaria y la frecuencia con la que debe actualizar su formación.</i></p> <p>Respecto a dicha formación: <input type="checkbox"/> 1.1.- ¿Cubre la configuración de sistemas? <i>Evidencia: Dicho plan tiene contenidos formativos relativos a la configuración de sistemas.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<input type="checkbox"/> 1.2.- ¿Cubre la detección y reacción a incidentes? <i>Evidencia: Dicho plan tiene contenidos formativos relativos a la detección y reacción a incidentes.</i> <input type="checkbox"/> 1.3.- ¿Cubre la gestión de la información en cualquier soporte en el que se encuentre? <i>Evidencia: Dicho plan tiene contenidos formativos relativos a la gestión de la información en cualquier soporte en el que se encuentre, al menos en lo que se refiere a almacenamiento, transferencia, copia, distribución y destrucción.</i>		
mp.per.9	Personal alternativo - D /Alto	<input type="checkbox"/> 1.- ¿Está garantizada la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual? <i>Evidencia: Dispone de un procedimiento documentado que identifica las personas que se pueden hacer cargo de las funciones en caso de indisponibilidad del personal habitual, en relación con el "[op.cont.2] Plan de continuidad". Estas personas están localizables y conocen los procedimientos necesarios.</i> Respecto a dicho personal alternativo: <input type="checkbox"/> 1.1.- ¿Está sometido a las mismas garantías de seguridad que el personal habitual? <i>Evidencia: El personal alternativo está sometido a las mismas</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>garantías de seguridad que el personal habitual.</i>		
<i>mp.eq</i>	PROTECCIÓN DE LOS EQUIPOS			
<i>mp.eq.1</i>	Puesto de trabajo despejado			
	Baja	<input type="checkbox"/> 1.- ¿Se exige que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento? <i>Evidencia: Dispone de una política o normativa documentada que indica que los puestos de trabajo deben permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Inspeccionar visualmente algún puesto de trabajo.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
	Media	<input type="checkbox"/> 2.- ¿Se guarda este material en lugar cerrado cuando no se está utilizando? <i>Evidencia: Dicha política o normativa indica que el material se guardará en lugar cerrado cuando no se esté utilizando. Observar si los usuarios disponen de lugares donde guardar bajo llave este material.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.eq.2	- A /Medio	<p><input type="checkbox"/> 1.- ¿El puesto de trabajo se bloquea al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso?</p> <p><i>Evidencia: Dispone de un mecanismo relacionado con [op.exp.2] que define el periodo de inactividad tras el cual se bloquea automáticamente el puesto de trabajo desde el que se accede a servicios o datos de nivel medio o superior (requiriendo una nueva autenticación del usuario para reanudar la actividad en curso). Dicha configuración no es modificable por el usuario (en relación con [op.exp.3]). Constatar que se cumple.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
	- A /Alto	<p><input type="checkbox"/> 2.- ¿Pasado un cierto tiempo, superior al anterior, se cancelan las sesiones abiertas desde dicho puesto de trabajo?</p> <p><i>Evidencia: Pasado un cierto tiempo, superior al anterior, se cancelan las sesiones abiertas desde dicho puesto de trabajo. Constatar que se cumple.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.eq.3	<p>Protección de equipos portátiles</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Son protegidos adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que especifica las medidas de seguridad que deben cumplir los equipos que abandonen las instalaciones de la organización (p. ej.: cuando se encuentren desatendidos se fijarán mediante un candado especial Kensington, dispondrán de identificadores que permitirán su devolución en caso de extravío pero sin identificar el tipo de contenido que albergan, etc.). Dicho procedimiento especifica la aplicación de lo previsto en [mp.si.5] borrado y destrucción al desmantelarlo. Los equipos portátiles deben cumplir lo establecido en [op.acc.5] mecanismo de autenticación. Constatar que se cumple el procedimiento.</i></p> <p>Respecto a los equipos portátiles:</p> <p><input type="checkbox"/> 1.1.- ¿Se lleva un inventario de los mismos junto con una identificación de la persona responsable del mismo?</p> <p><i>Evidencia: Dispone de un procedimiento documentado de inventario de equipos portátiles que recoge la identificación de la persona responsable del mismo. Consultar dicho inventario.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.2.- ¿Se ha establecido un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones? <i>Evidencia: Dispone de un procedimiento documentado para la comunicación, al servicio de gestión de incidentes, de pérdidas o sustracciones, y el personal responsable de los equipos portátiles lo conoce.</i></p> <p><input type="checkbox"/> 1.3.- ¿Se ha limitado la información y los servicios accesibles a los mínimos imprescindibles, en el ámbito de operación del servidor, cuando un equipo portátil se conecta remotamente a través de redes que no estén bajo control de la organización? <i>Evidencia: Dispone de un procedimiento documentado para protección de las conexiones de red (p. ej.: un sistema de protección perimetral que minimice la visibilidad desde el exterior y un firewall personal). Constatar que se cumple el procedimiento para conexiones a través de Internet y otras redes que no sean de confianza.</i></p> <p><input type="checkbox"/> 1.4.- ¿Se requiere autorización previa de los responsables de la información y servicios accesibles a través de Internet y otras redes que no sean de confianza? <i>Evidencia: Dispone de política o normativa documentada que exija autorización previa para conexiones de equipos portátiles a</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>través de Internet y otras redes que no sean de confianza.</i></p> <p><input type="checkbox"/> 1.5.- ¿Se evita, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización? <i>Evidencia: Dispone de política o normativa documentada que evita en lo posible que los equipos portátiles contengan claves de acceso remoto a la organización. Se han identificado los casos en los que esta política o normativa no se puede aplicar y están aprobados por la Dirección.</i></p>		
	Alta	<p><input type="checkbox"/> 1.6.- ¿Se le ha dotado de detectores de violación que permitan saber si el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente? <i>Evidencia: Dispone de detectores de violación que permitan saber si el equipo ha sido manipulado (p. ej.: pegatinas que se alteran al manipularlas), en cuyo caso se activan los procedimientos previstos de gestión del incidente.</i></p> <p><input type="checkbox"/> 1.7.- ¿Se protege la información de nivel alto almacenada en el disco mediante cifrado? <i>Evidencia: Dicha política o normativa establece el uso de medios criptográficos. Dispone de medios criptográficos (relacionados con [mp.si.2]) para la protección de la información almacenada.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.eq.9	<p>Medios alternativos</p> <p>- D / Medio</p>	<p><input type="checkbox"/> 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos de tratamiento de la información en caso de indisponibilidad de los medios habituales?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que identifica los medios alternativos existentes y su disponibilidad en caso de indisponibilidad de los habituales, en relación con el "[op.cont.2] Plan de continuidad". Estos medios existen y están disponibles.</i></p> <p>Respecto a dichos medios alternativos:</p> <p><input type="checkbox"/> 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales?</p> <p><i>Evidencia: Dicho procedimiento contempla que los medios alternativos están sometidos a las mismas garantías de seguridad que los habituales.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento?</p> <p><i>Evidencia: Dicho procedimiento identifica el tiempo máximo para que los equipos alternativos entren en funcionamiento en relación con [op.cont.2] y se encuentra aprobado por su responsable. Consultar la última prueba que garantice la entrada en funcionamiento en el tiempo establecido.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.com	PROTECCIÓN DE LAS COMUNICACIONES			
mp.com.1	Perímetro seguro			
	Baja	<input type="checkbox"/> 1.- ¿Dispone de cortafuegos que separe la red interna del exterior? <i>Evidencia: Dispone de un perímetro concreto, delimitado y acotado, reflejado en la arquitectura del sistema ([op.pl.2]). Todo el tráfico con el exterior pasa a través del cortafuegos. Sólo se permite el tráfico que ha sido previamente autorizado. Ver el firewall y el esquema de red.</i> Consultar guías: CCN-STIC-408 Seguridad perimetral (cortafuegos) CCN-STIC-419 Configuración segura con IPtables <u>Serie CCN-STIC-500 Guías para Entornos Windows</u> <u>Serie CCN-STIC-600 Guías para otros Entornos</u> <u>Serie CCN-STIC-800 Guías ENS</u>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>
	Alta	Respecto a dicho cortafuegos: <input type="checkbox"/> 1.1.- ¿El sistema de cortafuegos consta de dos o más equipos de diferente fabricante dispuestos en cascada? <i>Evidencia: Se cuenta con dos o más equipos de diferente fabricante dispuestos en cascada. Ver los firewalls y el esquema de red.</i> <input type="checkbox"/> 1.2.- ¿Se dispone de sistemas redundantes?	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>Evidencia: Los firewalls deben ser redundantes. Ver la configuración de los firewalls.</i>		
mp.com.2	Protección de la confidencialidad - C / Medio	<p><input type="checkbox"/> 1.- ¿Se emplean redes privadas virtuales (VPN³) cuando la comunicación discurre por redes fuera del propio dominio de seguridad?</p> <p><i>Evidencia: Las comunicaciones que discurren por redes fuera del propio dominio de seguridad utilizan VPN con métodos criptográficos que garanticen la confidencialidad de la información transmitida. La protección de la clave de cifrado cumple [op.exp.11]. Consultar el mecanismo VPN utilizado. Consultar el listado de personal con acceso a las VPN (Altas, bajas y modificaciones en su caso)</i></p> <p>Respecto a esas VPN:</p> <p><input type="checkbox"/> 1.1.- ¿Emplean algoritmos acreditados por el CCN?</p> <p><i>Evidencia: Dispone de un inventario de algoritmos criptográficos empleados. Los algoritmos criptográficos han sido acreditados por el CCN.</i></p> <p>Consultar guías:</p>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

³ Virtual Private Network

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	<p style="background-color: yellow;">CCN-STIC-406 Seguridad en Redes Inalámbricas</p> <p style="background-color: red;">- C /Alto</p>	<p>CCN-STIC-416 Seguridad de redes privadas virtuales</p> <p>CCN-STIC-807 Criptografía</p> <p>CCN-STIC-816 Seguridad en Redes Inalámbricas</p> <p><input type="checkbox"/> 1.2.- ¿Se emplean preferentemente dispositivos hardware en el establecimiento y utilización de la VPN? <i>Evidencia: Uso de dispositivos hardware en el establecimiento y utilización de la VPN. En caso de no utilización de dispositivos hardware debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan dispositivos hardware o, en caso contrario, si está aprobado por el responsable.</i></p> <p><input type="checkbox"/> 1.3.- ¿Se emplean productos certificados? <i>Evidencia: Uso de productos certificados (en relación con [op.pl.5] componentes certificados). Consultar si se utilizan productos certificados.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
mp.com.3	<p>Protección de la autenticidad y de la integridad</p> <p style="background-color: lightgreen;">- I, A / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se asegura la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna? <i>Evidencia: Dispone de una política o normativa documentada que obliga a asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (relacionado con [op.acc.5] mecanismos de</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>autenticación). Existe evidencia documental de que se ha constatado la autenticidad del otro extremo, por el procedimiento que se haya establecido, antes de intercambiar información alguna.</i></p> <p><input type="checkbox"/> 2.- ¿Se previenen ataques activos (alteración de la información en tránsito, inyección de información espuria o secuestro de la sesión por una tercera parte), garantizando que al menos serán detectados, y se activarán los procedimientos previstos de tratamiento del incidente? <i>Evidencia: Dispone de una política o normativa documentada que especifica el uso de mecanismos para la prevención de ataques activos y, en caso de ocurrir, su detección con la consiguiente activación de los procedimientos previstos de tratamiento del incidente. Consultar qué mecanismo se emplea y si está activado y revisar posibles incidentes resueltos.</i></p> <p><input type="checkbox"/> 3.- ¿Se utilizan mecanismos de autenticación de los previstos en la normativa de aplicación? <i>Evidencia: Dispone de una política o normativa documentada que especifica los mecanismos de autenticación utilizados.</i></p> <p>Consultar guías: CCN-STIC-416 Seguridad de redes privadas virtuales</p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-807 Criptografía		
	- I, A / Medio	<p><input type="checkbox"/> 4.- ¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad? <i>Evidencia: Las comunicaciones que discurren por redes fuera del propio dominio de seguridad utilizan VPN con métodos criptográficos que garanticen la confidencialidad de la información transmitida. La protección de la clave de cifrado cumple [op.exp.11]. Consultar el mecanismo VPN utilizado.</i></p> <p>Respecto a esas VPN:</p> <p><input type="checkbox"/> 4.1.- ¿Emplean algoritmos acreditados por el CCN? <i>Evidencia: Dispone de un inventario de algoritmos criptográficos empleados. Los algoritmos criptográficos han sido acreditados por el CCN.</i></p> <p><input type="checkbox"/> 4.2.- Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. ¿se utilizan claves concertadas? <i>Evidencia: En el caso de que se utilicen claves concertadas verificar que se dispone de una política o normativa</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>documentada que especifica la aplicación de exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.</i>		
	- I, A / Alto	<p><input type="checkbox"/> 4.3.- ¿Se emplean preferentemente dispositivos hardware en el establecimiento y utilización de la VPN? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de dispositivos hardware en el establecimiento y utilización de la VPN. En caso de no utilización de dispositivos hardware debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan dispositivos hardware o, en caso contrario, si está aprobado por el responsable.</i></p> <p><input type="checkbox"/> 4.4.- ¿Se emplean productos certificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5. Consultar si se utilizan productos certificados o, en caso contrario, si está aprobado por el responsable.</i></p> <p><input type="checkbox"/> 4.5.- Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. ¿Se utilizan claves concertadas? <i>Evidencia: En el caso de que se utilicen claves concertadas verificar que dispone de una política o normativa documentada</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>que especifica la aplicación de exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.</p>		
mp.com.4	<p>Segregación de redes Alta</p>	<p><input type="checkbox"/> 1.- ¿Se encuentra la red segmentada? <i>Evidencia: Se dispone de un mecanismo para que la red se encuentre segmentada. Dispone de segmentos concretos, delimitados y acotados, reflejados en la arquitectura del sistema ([op.pl.2]), bien sean físicos o lógicos. Sólo se permite el tráfico entre segmentos que ha sido previamente autorizado.</i></p> <p>Respecto a dichos segmentos:</p> <p><input type="checkbox"/> 1.1.- ¿Existe control de entrada de los usuarios que llegan a cada segmento? <i>Evidencia: Se establece el control de entrada de los usuarios que llegan a cada segmento. Dispone de un inventario de los usuarios que llegan a cada segmento.</i></p> <p><input type="checkbox"/> 1.2.- ¿Existe control de salida de la información disponible en cada segmento? <i>Evidencia: Se establece el control de salida de la información en cada segmento. Dispone de control de salida de la información disponible en cada segmento.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.3.- ¿Está el punto de interconexión particularmente asegurado, mantenido y monitorizado? <i>Evidencia: Esta particularmente asegurado, mantenimiento y monitorización del punto de interconexión entre segmentos como en [mp.com.1]perímetro seguro.</i></p> <p>Consultar guías: CCN-STIC-408 Seguridad perimetral (cortafuegos) CCN-STIC-419 Configuración segura con IPTables Serie CCN-STIC-500 Guías para Entornos Windows Serie CCN-STIC-600 Guías para otros Entornos CCN-STIC-641 Seguridad en equipos de comunicaciones routers Cisco Serie CCN-STIC-800 Guías ENS</p>		
mp.com.9	Medios alternativos - D / Alto	<p><input type="checkbox"/> 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos de comunicación en caso de indisponibilidad de los medios habituales? <i>Evidencia: Hay identificación de los medios alternativos existentes y su disponibilidad en caso de fallo de los habituales, en relación con el “[op.cont.2] Plan de continuidad”. Estos medios existen y están disponibles.</i></p> <p>Respecto a dichos medios alternativos:</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales? <i>Evidencia: Los medios alternativos están sometidos a las mismas garantías de seguridad que los habituales.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento? <i>Evidencia: Se identifica el tiempo máximo para que los equipos alternativos entren en funcionamiento en relación con [op.cont.2] y se encuentra aprobado por su responsable. Consultar la última prueba que garantice la entrada en funcionamiento en el tiempo establecido.</i></p>		
<i>mp.si</i>	PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN			
<i>mp.si.1</i>	Etiquetado - C / Bajo	<p><input type="checkbox"/> 1.- ¿Se encuentran etiquetados los soportes de información? <i>Evidencia: Dispone de un procedimiento documentado para el etiquetado de los soportes de información, tanto el que permanece en los locales de la organización como el que sale a otros destinos, que establece la persona responsable del etiquetado. Consultar si los soportes tienen el etiquetado</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>correspondiente conforme al procedimiento.</i></p> <p>Respecto a dicho etiquetado:</p> <p><input type="checkbox"/> 1.1.- ¿Revela el contenido? <i>Evidencia: Dicho procedimiento especifica que el etiquetado no debe revelar el contenido. Constatar que el etiquetado no revela el contenido (p. ej.: la etiqueta no contiene palabras tipo “datos financieros”, “datos del personal”, etc. sino un código no interpretable por personal ajeno al procedimiento).</i></p> <p><input type="checkbox"/> 1.2.- ¿Indica el nivel de seguridad de la información contenida de mayor calificación? <i>Evidencia: Dicho procedimiento especifica que el etiquetado debe indicar el nivel de seguridad de la información contenida de mayor calificación. Constatar que el etiquetado indica dicho nivel de seguridad.</i></p> <p><input type="checkbox"/> 1.3.- ¿Pueden los usuarios entender el significado de las etiquetas, bien mediante simple inspección, bien mediante recurriendo a un repositorio que lo explique? <i>Evidencia: Dicho procedimiento especifica cómo etiquetar los soportes y cómo leer la etiqueta. Esta información forma parte del plan de concienciación [mp.per.3] y de formación [mp.per.4], con lo que conocen y aplican además los procedimientos</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>asociados a cada nivel de información.</i></p> <p><input type="checkbox"/> 1.4.- ¿Se aplica tanto a aquellos en soporte electrónico como no electrónico (que hayan sido causa o consecuencia directa de la información electrónica dentro del alcance del ENS)?</p> <p><i>Evidencia: Los procedimientos referidos a la protección de la información almacenada y en tránsito reflejan las medidas a aplicar, según la naturaleza del soporte (electrónico o no).</i></p>		
mp.si.2	<p>Criptografía</p> <p>- I, C / Medio</p>	<p><input type="checkbox"/> 1.- ¿Se aplican mecanismos criptográficos, en particular, a todos los dispositivos removibles (CD, DVD, discos USB, u otros de naturaleza análoga) que garanticen la confidencialidad e integridad de la información contenida?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que indica el uso de mecanismos criptográficos que garantizan la confidencialidad e integridad de la información contenida (relacionado con [mp.eq.3]). Constatar que se utilizan mecanismos criptográficos en los dispositivos removibles.</i></p> <p>Consultar guías: CCN-STIC-807 Criptografía CCN-STIC-437 Herramientas de Cifrado Software CCN-STIC-955B Recomendaciones de Empleo de GPG</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	- I, C / Alto	<p>Respecto a dichos mecanismos criptográficos:</p> <p><input type="checkbox"/> 1.1.- ¿Emplean algoritmos acreditados por el CCN? <i>Evidencia: Dispone de un inventario de algoritmos criptográficos empleados. Los algoritmos criptográficos han sido acreditados por el CCN.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se emplean productos certificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5] componentes certificados). Consultar si se utilizan productos certificados o, en caso contrario, si está aprobado por el responsable.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
mp.si.3	Custodia Baja	<p><input type="checkbox"/> 1.- ¿Se aplica la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización? <i>Evidencia: Dispone de un procedimiento documentado para el control de los soportes de información, tanto de aquellos en soporte electrónico como no electrónico (que hayan sido causa o consecuencia directa de la información electrónica dentro del alcance del ENS). Dispone de un inventario de todos los soportes de información en uso, indicando su etiqueta, ubicación física y quién es el responsable del mismo. Consultar el inventario.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>Respecto a dicho control:</p> <p><input type="checkbox"/> 1.1.- ¿Garantiza el control de acceso con medidas físicas, lógicas o ambas?</p> <p><i>Evidencia: Dicho procedimiento contempla el control de acceso a los soportes de información con medidas físicas ([mp.if.1] y [mp.if.7]), lógicas ([mp.si.2]) o ambas. Consultar los controles implantados.</i></p> <p><input type="checkbox"/> 1.2.- ¿Garantiza que se respeten las exigencias de mantenimiento del fabricante, en especial en lo referente a temperatura, humedad y otros agresores medioambientales?</p> <p><i>Evidencia: Dicho procedimiento identifica las exigencias de mantenimiento del fabricante y establece su aplicación (relacionado con [mp.if.3]). Constatar que se aplican.</i></p>		<p><u>Observaciones auditoría:</u></p>
mp.si.4	<p>Transporte</p> <p>Baja</p>	<p><input type="checkbox"/> 1.- ¿Dispone de un registro de salida que identifica al transportista que recibe el soporte para su traslado?</p> <p><i>Evidencia: Dispone de un registro de transportistas autorizados. Dispone de un procedimiento documentado que registra cada salida de un soporte (tanto de aquellos electrónicos como no electrónicos -que hayan sido causa o consecuencia directa de la</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>información electrónica dentro del alcance del ENS-) de las instalaciones de la organización. Dicho registro almacena tanto la etiqueta como el transportista encargado de su traslado. Consultar los registros.</i></p> <p><input type="checkbox"/> 2.- ¿Dispone de un registro de entrada que identifica al transportista que lo entrega? <i>Evidencia: Dispone de un procedimiento documentado que registra cada llegada de un soporte (tanto de aquellos electrónicos como no electrónicos -que hayan sido causa o consecuencia directa de la información electrónica dentro del alcance del ENS-) a las instalaciones de la organización. Dicho registro almacena tanto la etiqueta como el transportista encargado de su traslado. Consultar los registros.</i></p> <p><input type="checkbox"/> 3.- ¿Utiliza medios de protección criptográfica correspondientes al nivel de calificación de la información contenida de mayor nivel? <i>Evidencia: Dispone de un procedimiento documentado que especifica el uso de los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel. Constatar que se utilizan medios de protección criptográfica.</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>Respecto a dicha protección criptográfica:</p> <p><input type="checkbox"/> 3.1.- ¿Gestiona las claves de forma segura?</p> <p><i>Evidencia: Dicho procedimiento establece los pasos para la gestión segura de las claves. Las claves se gestionan conforme a lo especificado en [op.exp.11].</i></p>		
mp.si.5	<p>Borrado y destrucción</p> <p>- C / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización, son borrados de forma segura?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que especifica quién o en qué circunstancia se debe proceder al borrado, quién debe realizarlo y el método de borrado seguro de los soportes (discos de equipos portátiles en aplicación de la medida [mp.eq.3], discos duros de todo tipo de equipos, discos removibles, PDA, CD, DVD, cinta magnética, papel impreso, cinta de papel, microfilm, memoria RAM, CMOS, EEPROM, tarjetas de memoria, tarjetas inteligentes, componentes de impresoras, etc.). Constatar que se dispone de los medios especificados para el borrado seguro y que se realiza conforme al procedimiento.</i></p> <p>Consultar guías: CCN-STIC-400 Manual de seguridad de las TIC CCN-STIC-404 Control de soportes informáticos</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-818 Herramientas de seguridad		
	- C / Medio	<p><input type="checkbox"/> 2.- ¿Se destruyen de forma segura los soportes cuando la naturaleza del soporte no permita un borrado seguro? <i>Evidencia: Dispone de un procedimiento documentado que indica el tipo de soporte que no permite un borrado seguro y especifica la forma de destruir dicho soporte de forma segura. Consultar el histórico de soportes y el registro de cuáles han sido eliminados.</i></p> <p><input type="checkbox"/> 3.- ¿Se destruyen de forma segura los soportes según el tipo de la información contenida? <i>Evidencia: Dispone de un procedimiento documentado que la forma de destruir un soporte según el tipo de la información contenida. Consultar el histórico de soportes para constatar cuáles han sido eliminados.</i></p> <p><input type="checkbox"/> 4.- ¿Se emplean productos certificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). Consultar si se utilizan productos certificados o, en caso contrario, si está aprobado por el responsable.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.sw	<i>PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS</i>			
mp.sw.1	<i>Desarrollo de aplicaciones</i>			
	Media	<p><input type="checkbox"/> 1.- ¿Se desarrollan aplicaciones sobre un sistema diferente y separado del de producción? <i>Evidencia: Dispone de una política o normativa documentada que indica que el desarrollo de aplicaciones se realiza sobre un sistema diferente y separado del de producción. Dispone de un inventario que identifica qué servidores se utilizan para desarrollo.</i></p> <p><input type="checkbox"/> 2.- ¿Existen herramientas o datos de desarrollo en el entorno de producción? <i>Evidencia: Dicha política o normativa establece que en el entorno de producción no pueden existir herramientas o datos de desarrollo. Constatar que no existen herramientas de desarrollo en el entorno de producción (p. ej.: no hay compiladores en los sistemas de producción). Verificar la separación de entornos de desarrollo y operación: Características, requisitos y configuración de estos.</i></p> <p><input type="checkbox"/> 3.- ¿Aplica una metodología de desarrollo reconocida? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de una metodología de desarrollo conocida (p. ej.: METRICA). Existe evidencia documental del uso de la</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>metodología de desarrollo (p. ej.: METRICA establece la elaboración de una serie de documentos, constatar que se han elaborado).</i></p> <p>Respecto a dicha metodología de desarrollo:</p> <p><input type="checkbox"/> 3.1.- ¿Toma en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida? <i>Evidencia: Dicha metodología de desarrollo toma en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.</i></p> <p><input type="checkbox"/> 3.2.- ¿Trata específicamente los datos usados en pruebas? <i>Evidencia: Dicha metodología de desarrollo trata específicamente los datos usados en pruebas.</i></p> <p><input type="checkbox"/> 3.3.- ¿Permite la inspección del código fuente? <i>Evidencia: Dicha metodología de desarrollo permite la inspección del código fuente.</i></p> <p><input type="checkbox"/> 3.4.- ¿Incluye normas de programación segura? <i>Evidencia: Dicha metodología de desarrollo incluye normas de programación segura.</i></p> <p><input type="checkbox"/> 4.- ¿Los mecanismos de identificación y autenticación son</p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>parte integral del diseño del sistema? <i>Evidencia: Dispone de una política o normativa documentada respecto al diseño de un sistema que contempla los mecanismos de identificación y autenticación.</i></p> <p><input type="checkbox"/> 4.1.- ¿Y los mecanismos de protección de la información tratada? <i>Evidencia: Dicha política o normativa respecto al diseño contempla los mecanismos de protección de la información tratada.</i></p> <p><input type="checkbox"/> 4.2.- ¿Y la generación y tratamiento de pistas de auditoría? <i>Evidencia: Dicha política o normativa respecto al diseño contempla la generación y tratamiento de pistas de auditoría. Consultar el diseño de un desarrollo.</i></p> <p><input type="checkbox"/> 5.- ¿Se realizan las pruebas anteriores a la implantación o modificación de los sistemas de información con datos reales? <i>Evidencia: Dispone de una política o normativa documentada que indica que las pruebas se realizan con datos ficticios o de datos reales disociados o enmascarados, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente. Existe evidencia que en el entorno de desarrollo no existen datos reales, o de lo contrario está aprobado por el</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>responsable.</i> Consultar guías: CCN-STIC-205 Actividades seguridad ciclo vida CIS METRICA v3		
mp.sw.2	Aceptación y puesta en servicio Baja	<input type="checkbox"/> 1.- ¿Dispone de un plan de pruebas antes de pasar a producción para comprobar el correcto funcionamiento de la aplicación? <i>Evidencia: Dispone de un procedimiento documentado para la elaboración y ejecución de un plan de pruebas de una aplicación. Existe evidencia documental del plan de pruebas ejecutado y su resultado.</i> Respecto a dichas pruebas: <input type="checkbox"/> 1.1.- ¿Comprueba que se cumplen los criterios de aceptación en materia de seguridad? <i>Evidencia: Dicho plan contempla pruebas de aceptación en materia de seguridad.</i> <input type="checkbox"/> 1.2.- ¿Comprueba que no se deteriora la seguridad de otros componentes del servicio? <i>Evidencia: Dicho plan contempla pruebas para constatar que no se deteriora la seguridad de otros componentes del servicio.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <hr/> <u>Observaciones auditoría:</u>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.3.- ¿Se realizan en un entorno aislado? <i>Evidencia: Dicho plan contempla que las pruebas se realizan en un entorno aislado (pre-producción).</i></p> <p><input type="checkbox"/> 1.4.- ¿Utilizan datos reales? <i>Evidencia: Dicho plan contempla que las pruebas se realizan con datos ficticios o datos reales disociados o enmascarados, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente.</i></p> <p>Consultar guías: METRICA v3</p>		
	Media	<p><input type="checkbox"/> 2.- ¿Previamente a la entrada en servicio, se le realiza un análisis de vulnerabilidades? <i>Evidencia: Dicho plan contempla la ejecución de un análisis de vulnerabilidades. Consultar los resultados y, si estos han identificado alguna vulnerabilidad, ver cómo se ha resuelto.</i></p> <p><input type="checkbox"/> 2.1.- ¿Y se le realiza una prueba de penetración? <i>Evidencia: Dicho plan contempla la ejecución de una prueba de penetración. Consultar los resultados y, si estos han identificado alguna vulnerabilidad, ver cómo se ha resuelto.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	Alta	<p><input type="checkbox"/> 2.2.- ¿Y un análisis de coherencia en la integración en los procesos? <i>Evidencia: Dicho plan contempla la ejecución de un análisis de coherencia en la integración en los procesos. Consultar los resultados.</i></p> <p><input type="checkbox"/> 2.3.- ¿Y se considera la oportunidad de realizar una auditoría de código fuente? <i>Evidencia: Dicho plan contempla la oportunidad de realizar una auditoría de código fuente. Consultar los resultados, o en caso de que no se haya realizado consultar los motivos para ello.</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
mp.info	PROTECCIÓN DE LA INFORMACIÓN			
mp.info.1	Datos de carácter personal			
	Baja	<p><input type="checkbox"/> 1.- ¿Se ha identificado si el sistema trata datos de carácter personal? <i>Evidencia: Dispone de un procedimiento documentado para identificar si el sistema trata datos de carácter personal. Consultar el resultado del procedimiento.</i></p> <p><input type="checkbox"/> 2.- En caso de tratar datos de carácter personal ¿se aplica la normativa vigente? <i>Evidencia: Se dispone de documentación relativa al cumplimiento de la regulación de tratamiento o protección de datos, así como clausulados de protección de datos con propietarios de los datos,</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>encargados de tratamiento y entes a los que se cedan datos personales de acuerdo a la legislación aplicable. Comprobar estos extremos. Verificar el documento de seguridad de protección de datos o equivalente.</i></p> <p>Consultar guías: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal Real Decreto 1720/2007, de 21 de diciembre, del Reglamento de Desarrollo de la L.O. 15/1999 Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre. Reglamento (UE) 2016/679 del parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.</p>		
mp.info.2	<p>Calificación de la información</p> <p>- C / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Se califica la información conforme a lo establecido legalmente sobre la naturaleza de la misma?</p> <p><i>Evidencia: Dispone de un procedimiento documentado para identificar la legalidad existente y aplicable respecto a la calificación de la información, que alimenta el esquema formal de calificación de la información conforme a lo establecido</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>legalmente sobre la naturaleza de la misma, de forma coherente con otros sistemas de clasificación propios del entorno en el que desarrolla su actividad la organización. Dicho procedimiento establece las responsabilidades para adscribir inicialmente una cierta información a una cierta calificación y para posibles recalificaciones posteriores. Consultar si la información impresa o disponible en las aplicaciones recogen su calificación.</i></p> <p><input type="checkbox"/> 2.- ¿Establece la política de seguridad quién es el responsable de cada información manejada por el sistema? <i>Evidencia: Dispone de una política de seguridad documentada que especifica quién es el responsable de cada información manejada por el sistema.</i></p> <p><input type="checkbox"/> 3.- ¿Recoge la política de seguridad, directa o indirectamente, los criterios que en la organización determinan el nivel de seguridad requerido? <i>Evidencia: Dicha política recoge los criterios que en la organización determinan el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I del ENS.</i></p> <p><input type="checkbox"/> 4.- ¿El responsable de cada información sigue los criterios determinados en la política de seguridad para asignar a cada</p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>información el nivel de seguridad requerido y es responsable de su documentación y aprobación formal? <i>Evidencia: Dispone de un procedimiento documentado que debe seguir el responsable de cada información para asignar a cada información el nivel de seguridad requerido y establecido en la política de seguridad. También define que es su responsabilidad el elaborar la documentación y aprobación formal.</i></p> <p><input type="checkbox"/> 5.- ¿El responsable de cada información en cada momento tiene en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a la política de seguridad? <i>Evidencia: Dicha política contempla que el responsable de cada información en cada momento tiene en exclusiva la potestad de modificar el nivel de seguridad requerido. Para la información existente, consultar el histórico de cambios en su nivel de seguridad, así como la fecha, y persona responsable del cambio.</i></p> <p>Consultar guías: CCN-STIC-001 Seguridad de las TIC que manejan información nacional clasificada en la Administración</p>		
	- C / Medio	<p><input type="checkbox"/> 6.- ¿Existen procedimientos que describan en detalle la forma en que se ha de etiquetar y tratar la información? <i>Evidencia: Dispone de un procedimiento documentado que describe la forma en que se ha de etiquetar y tratar la</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito:</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>información, en función del nivel de seguridad que se requiere. Constatar que el etiquetado y tratamiento de la información se corresponde con el procedimiento.</i></p> <p>Respecto a dicho tratamiento de la información:</p> <p><input type="checkbox"/> 6.1.- ¿Contempla su control de acceso? <i>Evidencia: Cumple [op.acc].</i></p> <p><input type="checkbox"/> 6.2.- ¿Contempla su almacenamiento? <i>Evidencia: Cumple [mp.si.3] y [mp.si.2].</i></p> <p><input type="checkbox"/> 6.3.- ¿Contempla la realización de copias? <i>Evidencia: Cumple [mp.info.9].</i></p> <p><input type="checkbox"/> 6.4.- ¿Contempla el etiquetado de soportes? <i>Evidencia: Cumple [mp.si.1].</i></p> <p><input type="checkbox"/> 6.5.- ¿Contempla su transmisión telemática? <i>Evidencia: Cumple [mp.com].</i></p> <p><input type="checkbox"/> 6.6.- ¿Y contempla cualquier otra actividad relacionada con dicha información? <i>Evidencia: Consultar qué otra actividad relacionada con la información realiza la organización, y si esta se realiza conforme</i></p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>a una política, normativa y procedimientos documentados, aprobados y revisados.</i>		
mp.info.3	<p>Cifrado</p> <p>- C / Alto</p>	<p><input type="checkbox"/> 1.- ¿Se cifra la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que indica que la información con un nivel alto en confidencialidad se cifra tanto durante su almacenamiento (conforme a [mp.si.2], bien sea como cifrado de ficheros, cifrado de directorios, discos virtuales cifrados o cifrado de datos en base de datos) como durante su transmisión (conforme a [mp.com.2]). Dispone de un procedimiento documentado que determina cómo cifrar correctamente la información en función de su clasificación y el medio en el que se almacena. Se cumple [op.exp.11]. Existen mecanismos para aplicar dicho procedimiento (p. ej.: GnuPG, VPN IPSec, etc.) y la información está, efectivamente, cifrada.</i></p> <p><i>Respecto a la criptografía:</i></p> <p><input type="checkbox"/> 1.1.- ¿Contempla el uso de criptografía en comunicaciones?</p> <p><i>Evidencia: Cumple [mp.com.2].</i></p>	<p>Aplica:</p> <p><input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito:</p> <p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.2.- ¿Contempla el uso de criptografía en los soportes de información? <i>Evidencia: Cumple [mp.si.2].</i></p> <p><input type="checkbox"/> 2.- ¿Permanece sólo en claro la información con un nivel alto en confidencialidad mientras se está haciendo uso de ella? <i>Evidencia: Dicha política o normativa indica que la información con un nivel alto en confidencialidad permanece en claro sólo mientras se está haciendo uso de ella.</i></p> <p>Consultar guías: CCN-STIC-807 Criptografía CCN-STIC-955B Recomendaciones empleo GPG</p>		
mp.info.4	<p>Firma electrónica</p> <p>- I, A / Bajo</p>	<p><input type="checkbox"/> 1.- ¿Dispone de una Política de Firma Electrónica aprobada por el órgano superior competente que corresponda? <i>Evidencia: Dispone de una Política de Firma Electrónica aprobada por el órgano superior competente que corresponda, y se cumple [op.exp.11] protección de claves criptográficas.</i></p> <p><input type="checkbox"/> 2.- ¿Se firman electrónicamente los documentos que requieren capacidad probatoria según la ley de procedimiento administrativo común de las Administraciones Públicas? <i>Evidencia: Dispone de un procedimiento documentado para</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>identificar los documentos que requieren capacidad probatoria según la ley de procedimiento administrativo. Estos documentos se firman electrónicamente.</i></p> <p><input type="checkbox"/> 3.- En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, ¿se incorporan medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio? <i>Evidencia: Dispone de un procedimiento documentado para identificar los mecanismos de firma electrónica alternativos y sus garantías respecto a prevención de repudio. Se debe usar el procedimiento previsto en el punto 5 del artículo 27 (medidas compensatorias).</i></p> <p>Consultar guías: CCN-STIC-405 Algoritmos y parámetros de firma electrónica segura CCN-STIC-807 Criptografía Reglamento 910/2014, de 23 de julio, sobre identificación electrónica y servicios de confianza (eIDAS)</p>		
	- I, A / Medio	<p><input type="checkbox"/> 4.- Si se emplean sistemas de firma electrónica avanzada, ¿se emplean certificados cualificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados cualificados. En caso de</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado:</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>utilización de certificados no cualificados debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan certificados cualificados o, en caso contrario, si está aprobado por el responsable.</i></p> <p><input type="checkbox"/> 5.- ¿Se emplean preferentemente certificados reconocidos? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados reconocidos. En caso de utilización de certificados no reconocidos debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan productos certificados o, en caso contrario, si está aprobado por el responsable.</i></p> <p><input type="checkbox"/> 6.- ¿Se emplean algoritmos acreditados por el CCN? <i>Evidencia: Dispone de un inventario de algoritmos criptográficos empleados. Los algoritmos criptográficos han sido acreditados por el CCN.</i></p> <p><input type="checkbox"/> 7.- ¿Se garantiza la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella soporte, sin perjuicio de que se pueda ampliar ese periodo de acuerdo con lo que establezca la política de firma electrónica y de certificados que sea de aplicación?</p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Dispone de un procedimiento documentado para firmar. Dispone de un procedimiento documentado para identificar el tiempo requerido por la actividad administrativa durante el que se deberá poder verificar y validar la firma electrónica. Dispone de un procedimiento documentado para verificar y validar firmas cuyos mecanismos soportan dicha vigencia (p. ej.: consultas OCSP, CRL, etc.). Constatar que se cumple dicho procedimiento.</i></p> <p>Respecto a la verificación y validación de la firma electrónica:</p> <p><input type="checkbox"/> 7.1.- ¿Se adjunta a la firma, o se referencia, el certificado?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que contempla adjuntar o referenciar en la firma el certificado. Constatar que se adjunta a la firma, o se referencia, el certificado.</i></p> <p><input type="checkbox"/> 7.2.- ¿Se adjuntan a la firma, o se referencian, los datos de verificación y validación?</p> <p><i>Evidencia: Dicho procedimiento contempla adjuntar o referenciar en la firma los datos de verificación y validación. Constatar que se adjuntan a la firma, o se referencian, los datos de verificación y validación.</i></p> <p><input type="checkbox"/> 7.3.- ¿Se protegen la firma, el certificado y los datos de</p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>verificación y validación con un sello de tiempo? <i>Evidencia: Dicho procedimiento contempla acompañar la firma, el certificado y los datos de verificación y validación con un sello de tiempo. Constatar que acompañan a la firma, el certificado y los datos de verificación y validación con un sello de tiempo.</i></p> <p><input type="checkbox"/> 7.4.- ¿Verifica y valida el organismo que recaba documentos firmados la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad el certificado, los datos de verificación y validación, y el sello de tiempo? <i>Evidencia: Dicho procedimiento contempla validar la firma del documento firmado recabado, recibida en el momento de la recepción, anexando o referenciando sin ambigüedad el certificado, los datos de verificación y validación, y el sello de tiempo. Constatar que, en caso de recabar documentos firmados, se verifica y valida la firma anexando o referenciando sin ambigüedad el certificado, los datos de verificación y validación, y el sello de tiempo.</i></p> <p><input type="checkbox"/> 7.5.- ¿La firma electrónica de documentos por parte de la Administración anexa o referencia sin ambigüedad el certificado, los datos de verificación y validación, y el sello de tiempo? <i>Evidencia: Dicho procedimiento contempla el certificado, los datos de verificación y validación, y el sello de tiempo. Constatar</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<i>que, en caso de firmar documentos, se anexa o referencia sin ambigüedad el certificado, los datos de verificación y validación, y el sello de tiempo.</i>		
	- I, A / Alto	<input type="checkbox"/> 8.- ¿Se emplean certificados cualificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados cualificados. Constatar el uso de estos certificados.</i> <input type="checkbox"/> 9.- ¿Se emplean dispositivos cualificados de creación de firma? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de dispositivos cualificados de creación de firma.</i> <input type="checkbox"/> 10.- ¿Se emplean productos certificados? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). Consultar si se utilizan productos certificados.</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
mp.info.5	Sellos de tiempo			
	- T / Alto	<input type="checkbox"/> 1.- ¿Se aplican sellos de tiempo (fechado electrónico) a aquella información que sea susceptible de ser utilizada como evidencia en el futuro? <i>Evidencia: Dispone de un procedimiento documentado para identificar y establecer el tiempo de retención de la información</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>que sea susceptible de ser utilizada como evidencia en el futuro, o que requiera capacidad probatoria según la ley de procedimiento administrativo. Dispone de un procedimiento documentado para fechar electrónicamente. Dispone de un procedimiento documentado para verificar y validar fechados cuyos mecanismos soportan dicha vigencia. Se fechan electrónicamente los documentos cuya fecha y hora de entrada o salida deba acreditarse fehacientemente.</i></p> <p><input type="checkbox"/> 2.- ¿Los datos pertinentes para la verificación posterior de la fecha son tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad? <i>Evidencia: Dispone de un procedimiento documentado para el tratamiento de los datos pertinentes para la verificación posterior de la fecha y lo son con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad. Constatar el tratamiento seguro conforme a este procedimiento para la verificación posterior de la fecha.</i></p> <p><input type="checkbox"/> 3.- ¿Se renuevan regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte? <i>Evidencia: Dispone de un procedimiento documentado para el</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>tratamiento de los datos pertinentes para la verificación posterior de la fecha con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad. Dicho procedimiento contempla el fechado electrónico de las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable, también contempla alternativamente el uso de formatos de firma avanzada que incluya fechado. Dispone de un procedimiento para identificar la duración del sello de tiempo en función del tiempo requerido por el proceso administrativo al que da soporte. Constatar que los sellos de tiempo que lo requerían han sido renovados conforme al procedimiento.</i></p> <p><input type="checkbox"/> 4.- ¿Se utilizan productos certificados o servicios externos admitidos? <i>Evidencia: Cumple [op.pl.5] o [op.exp.10].</i></p> <p><input checked="" type="checkbox"/> 5.- ¿Se emplean “sellos cualificados de tiempo electrónicos” acordes a la normativa europea en la materia? <i>Evidencia: Dispone de un procedimiento documentado para el empleo de sellos cualificados de tiempo electrónicos, basado en la normativa europea.</i></p> <p>Consultar guías:</p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-807 Criptografía Reglamento 910/2014, de 23 de julio, sobre identificación electrónica y servicios de confianza (eIDAS)		
mp.info.6	Limpieza de documentos - C / Bajo	<input type="checkbox"/> 1.- ¿Existe un procedimiento para limpiar (retirar la información contenida en campos ocultos, meta-datos, comentarios o revisiones) todos los documentos que van a ser transferidos a otro dominio de seguridad, salvo cuando dicha información sea pertinente para el receptor del documento? <i>Evidencia: Dispone de un procedimiento documentado que identifica el destino del documento y, si va a ser transferido a otro dominio de seguridad o publicado electrónicamente, indica cómo limpiar el documento. Dispone de herramientas evaluadas para limpiar los documentos.</i> <i>Consultar guías:</i> CCN-STIC 835 Borrado de metadatos en el marco del ENS.	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo: <u>Observaciones auditoría:</u>
mp.info.9	Copias de seguridad (backup) - D / Bajo	<input type="checkbox"/> 1.- ¿Realizan copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada? <i>Evidencia: Dispone de un procedimiento documentado por el que el responsable de la información determina la frecuencia con la</i>	Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No	<u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>que deben realizarse las copias, el periodo de retención durante el que mantenerlas, realización y eliminación de los backups. Dispone de mecanismos de backup (p. ej.: unidad de cinta, cintas, disco duro para almacenamiento de copias, aplicación de backup, etc.) y de eliminación segura (p. ej.: software de eliminación segura, desmagnetizador, etc.). Consultar que los backups existen y se realizan conforme al procedimiento.</i></p> <p>Respecto a dichas copias de seguridad:</p> <p><input type="checkbox"/> 1.1.- ¿Abarcan la información de trabajo de la organización? <i>Evidencia: Dicho procedimiento contempla que todos los responsables de la información de la organización determinen su necesidad de copias de seguridad. Constatar que los backups almacenan esta información.</i></p> <p><input type="checkbox"/> 1.2.- ¿Abarcan las aplicaciones en explotación, incluyendo los sistemas operativos? <i>Evidencia: Dicho procedimiento contempla que todos los responsables de sistemas de la organización determinen su necesidad de copias de seguridad. Este procedimiento está ligado a [op.exp.3] gestión de la configuración, [op.exp.4] Mantenimiento y [op.exp.5] gestión de cambios. Constatar que los backups almacenan esta información.</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 1.3.- ¿Abarcan los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga? <i>Evidencia: Dicho procedimiento contempla que todos los responsables de sistemas de la organización determinen su necesidad de copias de seguridad. Este procedimiento está ligado a [op.exp.1 inventario de activos], [op.exp.2] configuración de la seguridad, [op.exp.3] gestión de la configuración, [op.exp.4] Mantenimiento y [op.exp.5] gestión de cambios. Constatar que los backups almacenan esta información.</i></p> <p><input type="checkbox"/> 1.4.- ¿Abarcan las claves utilizadas para preservar la confidencialidad de la información? <i>Evidencia: Dicho procedimiento contempla que todos los responsables de sistemas de la organización determinen su necesidad de copias de seguridad. Este procedimiento está ligado a [op.exp.11]Protección de claves criptológicas y [mp.info.3] cifrado. Constatar que los backups almacenan esta información.</i></p> <p><input type="checkbox"/> 1.5.- ¿Disfrutan de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad? <i>Evidencia: Dicho procedimiento contempla que los backups disfruten de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>trazabilidad, tanto en su acceso, almacenamiento como transporte. Este procedimiento está ligado a [op.acc] control de accesos, [op.exp.9] registro de la gestión de incidentes y [op.exp.10]protección de los registros de actividad y, en caso de utilizar cifrado, con [op.exp.11 Protección de claves criptológicas]. Constatar que las medidas de seguridad son las pertinentes.</i></p> <p><input type="checkbox"/> 1.6.- ¿Existe un proceso de autorización para la recuperación de información de las copias de seguridad? <i>Evidencia: Dispone de un procedimiento documentado para la solicitud de recuperación de un backup, la identificación del responsable de la información y su autorización por escrito. Consultar las últimas restauraciones de información y constatar que han sido autorizadas por su responsable.</i></p> <p><input type="checkbox"/> 1.7.- ¿Se verifica regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad? <i>Evidencia: Dispone de un procedimiento documentado para la realización de pruebas de restauración del backup, que indica quién debe hacerlo, la frecuencia; manteniendo los requisitos de seguridad establecidos para la información original restaurada. Dispone de un plan de pruebas de respaldo que cubre, a lo largo</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>del tiempo, todos los ámbitos de los que se realizan backups. Consultar que se han llevado a cabo los planes de pruebas, y resultado de los mismos y si ha sido necesario realizar algún cambio.</i></p> <p><input type="checkbox"/> 1.8.- ¿Se conservan en lugar(es) suficientemente independiente(s) de la ubicación normal de la información en explotación como para que los incidentes previstos en el análisis de riesgos no se den simultáneamente en ambos lugares?</p> <p><i>Evidencia: Dispone de un procedimiento documentado que identifica las amenazas previstas por el análisis de riesgos y establece, en caso de ser necesario, un lugar independiente del de explotación para el almacenamiento de los backups que permita cumplir con el “[op.cont.2] Plan de continuidad” establecido.</i></p>		
<i>mp.s</i>	PROTECCIÓN DE LOS SERVICIOS			
<i>mp.s.1</i>	Protección del correo electrónico (e-mail)			
	Baja	<p><input type="checkbox"/> 1.- ¿La información que se distribuye por medio de correo electrónico se protege, tanto en el cuerpo de los mensajes como en los anexos?</p> <p><i>Evidencia: Dispone de un procedimiento documentado para la protección, acorde a su nivel de clasificación, de la información que se distribuye por medio de correo electrónico y se protege,</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u></p> <p><input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>tanto en el cuerpo de los mensajes como en los anexos (relacionado con [mp.info.6] limpieza de documentos). Consultar que los correos electrónicos cumplen con el procedimiento.</i></p> <p><input type="checkbox"/> 2.- ¿Se protege la información de encaminamiento de mensajes y establecimiento de conexiones? <i>Evidencia: Dispone de una política o normativa documentada que especifica la protección del encaminamiento de mensajes (p. ej.: protegiendo el servidor DNS y su configuración, impidiendo que el usuario final modifique la configuración de la cuenta de correo –como el servidor de correo-) y establecimiento de conexiones (p. ej.: impidiendo que el usuario final pueda conectarse a un servidor de correo que no sea el corporativo, como pudiera ser con reglas en el cortafuegos).</i></p> <p><input type="checkbox"/> 3.- ¿Se protege a la organización frente a problemas que se materializan por medio del correo electrónico, como del correo no solicitado (spam)? <i>Evidencia: Dispone de una política o normativa documentada que especifica que la organización debe ser protegida frente al spam. Dispone de un sistema anti-spam debidamente configurado y mantenido (p. ej.: un sistema anti-spam antes del servidor de correo, o un sistema anti-spam en el puesto de usuario).</i></p>		<p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>Respecto a la protección frente a problemas por el e-mail:</p> <p><input type="checkbox"/> 3.1.- ¿Se protege frente a programas dañinos (virus, gusanos, troyanos, espías u otros de naturaleza análoga) relacionado con op.exp.6 Protección frente a código dañino? <i>Evidencia: Dispone de una política o normativa documentada que especifica que la organización debe ser protegida frente a programas dañinos en el e-mail. Dispone de un sistema anti-virus debidamente configurado y mantenido (p. ej.: un sistema anti-virus en el servidor de correo, o un sistema anti-virus en el puesto de usuario).</i></p> <p>Respecto a la protección frente a problemas por el e-mail:</p> <p><input type="checkbox"/> 3.2.- ¿Se protege frente a código móvil de tipo “applet”? <i>Evidencia: Dispone de una política o normativa documentada que especifica que la organización debe ser protegida frente a código móvil en el e-mail. Dispone de un sistema anti-virus que contempla código móvil debidamente configurado y mantenido (p. ej.: un sistema anti-virus en el servidor de correo, o un sistema anti-virus en el puesto de usuario).</i></p> <p><input type="checkbox"/> 4.- ¿Se han establecido normas de uso del correo electrónico? <i>Evidencia: Dispone de una normativa documentada que especifica el uso correcto y autorizado del correo electrónico.</i></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Constatar que se sigue la normativa.</i></p> <p>Respecto a dicha norma de uso del e-mail:</p> <p><input type="checkbox"/> 4.1.- ¿Contempla limitaciones al uso como soporte de comunicaciones privadas? <i>Evidencia: Dicha normativa especifica las limitaciones al uso como soporte de comunicaciones privadas.</i></p> <p><input type="checkbox"/> 4.2.- ¿Se llevan a cabo actividades de concienciación y formación relativas al uso del correo electrónico? <i>Evidencia: Dispone de plan de formación y concienciación que cubre el uso del correo electrónico (relacionado con [mp.per.3] concienciación y [mp.per.4] formación). Consultar los resultados de la ejecución del plan de formación y concienciación.</i></p> <p>Consultar guías: Serie CCN-STIC-500 Guías para Entornos Windows Serie CCN-STIC-600 Guías para otros Entornos CCN-STIC-682 Configuración segura de Sendmail CCN-STIC-814 Seguridad en el Servicio de Correo</p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
mp.s.2	<p data-bbox="367 459 913 491"><i>Protección de servicios y aplicaciones web</i></p> <p data-bbox="367 501 427 533">Baja</p>	<p data-bbox="571 501 1422 612"><input type="checkbox"/> 1.- ¿Se encuentran protegidos los subsistemas dedicados a la publicación de información frente a las amenazas que les son propias?</p> <p data-bbox="571 619 1422 772"><i>Evidencia: Dispone de una política o normativa documentada que especifica las medidas de seguridad con que deben contar los servidores web, conforme a lo identificado en el análisis de riesgos. Constatar que se aplican dichas medidas.</i></p> <p data-bbox="571 813 1422 925"><input type="checkbox"/> 2.- Cuando la información tenga algún tipo de control de acceso ¿se garantiza la imposibilidad de acceder a la información obviando la autenticación?</p> <p data-bbox="571 932 1422 1203"><i>Evidencia: Dispone de una política o normativa documentada que especifica, desde la etapa de diseño, que aquella información para la que es requerida autenticación no puede ser accedida sin dicha autenticación. El sistema aplica dicha política (p. ej.: una información que requiere la autenticación del usuario no está accesible por otra vía que no requiera autenticación, como un buscador interno).</i></p> <p data-bbox="571 1244 1041 1276">Respecto a dicho control de acceso:</p> <p data-bbox="571 1283 1422 1362"><input type="checkbox"/> 2.1.- ¿Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado?</p> <p data-bbox="571 1369 1422 1394"><i>Evidencia: Dispone de una política o normativa documentada</i></p>	<p data-bbox="1444 501 1601 533">Aplica:</p> <p data-bbox="1444 539 1601 571"><input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p data-bbox="1444 619 1601 651">Lo audito:</p> <p data-bbox="1444 657 1601 689"><input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p data-bbox="1691 501 1825 533"><u>Registros:</u></p> <p data-bbox="1691 539 1915 571"><input type="checkbox"/> Documento:</p> <p data-bbox="1691 619 1892 651"><input type="checkbox"/> Muestreo:</p> <hr/> <p data-bbox="1691 737 2027 769"><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>que especifica el protocolo de acceso a utilizar, y no permite que se utilice otro. El sistema aplica dicha política (p. ej.: las páginas a las que se debe acceder mediante HTTPS no están accesibles mediante HTTP).</i></p> <p><input type="checkbox"/> 2.2.- ¿Se previenen ataques de manipulación de URL? <i>Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir ataques de manipulación de URL⁴. El sistema aplica dicha política (p. ej.: no es posible acceder a páginas que requieren haber visitado antes otras páginas en el proceso).</i></p> <p><input type="checkbox"/> 2.3.- ¿Se previenen ataques de manipulación de las cookies de los usuarios? <i>Evidencia: Dicha política o normativa especifica el uso de mecanismos para proteger las cookies frente a su manipulación. El sistema aplica dicha política (p. ej.: la información de las cookies se almacena cifrada).</i></p> <p><input type="checkbox"/> 2.4.- ¿Se previenen ataques de inyección de código? <i>Evidencia: Dicha política o normativa especifica el uso de</i></p>		

⁴ Uniform Resource Locator

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>mecanismos para impedir ataques de inyección de código. El sistema aplica dicha política (p. ej.: las aplicaciones no permiten recibir código no saneado, el servidor web no permite introducir caracteres no autorizados por la aplicación, el servidor no devuelve mensajes de error descriptivos, etc.).</i></p> <p><input type="checkbox"/> 3.- ¿Se previenen intentos de escalado de privilegios? <i>Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir intentos de escalado de privilegios. El sistema aplica dicha política (p. ej.: no es posible acceder a información del sistema que pueda ser utilizada para la escalada de privilegios, no es posible ejecutar acciones haciéndose pasar por otro usuario, etc.).</i></p> <p><input type="checkbox"/> 4.- ¿Se previenen ataques de “cross site scripting”? <i>Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir ataques de “cross site scripting”. El sistema aplica dicha política (p. ej.: no es posible introducir información en la página web que se muestre tal cual posteriormente al usuario, no es posible cargar contenidos Adobe Flash desde ubicaciones externas al servidor, etc.).</i></p> <p><input type="checkbox"/> 5.- ¿Se previenen ataques de manipulación de “proxys” o “cachés”?</p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir ataques de manipulación de “proxies” o “cachés”. El sistema aplica dicha política en caso de hacer uso de esas tecnologías (p. ej.: no es posible suplantar sesiones de otros usuarios).</i></p> <p><input type="checkbox"/> 6.- ¿Se realizan auditorías de seguridad y pruebas de penetración? <i>Evidencia: Se cumple [mp.sw.2].</i></p> <p><input type="checkbox"/> 7.- ¿Se emplean certificados de autenticación de sitio web acordes a la normativa europea en la materia? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados de autenticación de sitio web. En caso no utilizar certificados de autenticación web debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan certificados de autenticación de sitio web o, en caso contrario, si está aprobado por el responsable.</i></p> <p>Consultar guías: <u>Serie CCN-STIC-500 Guías para Entornos Windows</u> <u>Serie CCN-STIC-600 Guías para otros Entornos</u> <u>CCN-STIC-812 Seguridad en Servicios Web</u></p>		

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
	Alta	<p><input type="checkbox"/> 8.- ¿Se emplean certificados cualificados de autenticación de sitio web acordes a la normativa europea en la materia? <i>Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados cualificados de autenticación de sitio web. En caso de utilización de certificados no cualificados debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan certificados cualificados de autenticación de sitio web o, en caso contrario, si está aprobado por el responsable.</i></p> <p><i>Consultar guías:</i> Reglamento 910/2014, de 23 de julio, sobre identificación electrónica y servicios de confianza (eIDAS)</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>
mp.s.8	<p><i>Protección frente a la denegación de servicio</i></p> <p>- D / Medio</p>	<p><input type="checkbox"/> 1.- ¿Se ha planificado y dotado al sistema de capacidad suficiente para atender a la carga prevista con holgura? <i>Evidencia: Dispone de un procedimiento para identificar la carga que puede soportar el sistema. Se ha contrastado la carga que puede soportar el sistema con la carga prevista ([op.pl.4] dimensionamiento/gestión de capacidades) y es suficiente.</i></p> <p><input type="checkbox"/> 2.- ¿Se han desplegado tecnologías para prevenir los ataques</p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo auditado: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p>conocidos de denegación de servicio (Denial of Service (DoS))? <i>Evidencia: Dispone de una política o normativa documentada que indica el despliegue de tecnologías para prevenir los ataques de DoS. El sistema aplica dicha política (p. ej.: dispone de un firewall con identificación y protección frente a DoS).</i></p> <p>Consultar guías: CCN-STIC-412 Requisitos de seguridad de entornos y aplicaciones web CCN-STIC-434 Herramientas para el análisis de ficheros de log Serie CCN-STIC-500 Guías para Entornos Windows Serie CCN-STIC-600 Guías para otros Entornos CCN-STIC-820 Guía de protección contra Denegación de Servicio CCN-STIC-953 Recomendaciones empleo herramienta Snort</p>		
	- D / Alto	<p><input type="checkbox"/> 3.- ¿Se ha establecido un sistema de detección de ataques de denegación de servicio? <i>Evidencia: Dispone de una política o normativa documentada que indica el establecimiento de un sistema de detección de ataques de denegación de servicio. Existen mecanismos para aplicar dicha política o normativa (p. ej.: un dispositivo de detección de DoS, un monitor con aviso en caso de detectar un número de peticiones superior o inferior a lo habitual, un monitor con aviso en caso de detectar un consumo de ancho de banda de comunicaciones superior al habitual, etc.).</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento:</p> <p><input type="checkbox"/> Muestreo:</p> <hr/> <p><u>Observaciones auditoría:</u></p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><input type="checkbox"/> 4.- ¿Se ha establecido un procedimiento de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones? <i>Evidencia: Dispone de un procedimiento documentado que indica el procedimiento de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.</i></p> <p><input type="checkbox"/> 5.- ¿Se impide el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros? <i>Evidencia: Dispone de una política o normativa documentada que indica el establecimiento de un sistema que impide el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros. Existen mecanismos para aplicar dicha política o normativa (p. ej.: bloquear un número elevado de conexiones concurrentes, bloquear el envío de grandes cantidades de información, etc.).</i></p>		
mp.s.9	Medios alternativos - D / Alto	<p><input type="checkbox"/> 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos para prestar los servicios en caso de indisponibilidad de los medios habituales? <i>Evidencia: Dispone de un procedimiento documentado que identifica los medios alternativos existentes y su disponibilidad en caso de indisponibilidad de los habituales, en relación con el</i></p>	<p>Aplica: <input type="checkbox"/> Sí <input type="checkbox"/> No</p> <p>Lo audito: <input type="checkbox"/> Sí <input type="checkbox"/> No</p>	<p><u>Registros:</u> <input type="checkbox"/> Documento: <input type="checkbox"/> Muestreo:</p>

Aptdo.	Categoría - Dimensiones / Nivel	Requisito	Aplicabilidad - Auditado	Comentarios
		<p><i>“[op.cont.2] Plan de continuidad”. Estos medios existen y están disponibles.</i></p> <p>Respecto a dichos medios alternativos:</p> <p><input type="checkbox"/> 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales?</p> <p><i>Evidencia: Dispone de una política o normativa documentada que establece la obligatoriedad de aplicar las mismas garantías de seguridad a los medios alternativos que a los medios habituales. Los medios alternativos están sometidos a las mismas garantías de seguridad que los habituales.</i></p> <p><input type="checkbox"/> 1.2.- ¿Se ha establecido un tiempo máximo para que los medios alternativos entren en funcionamiento?</p> <p><i>Evidencia: Dicho procedimiento identifica el tiempo máximo para que los medios alternativos entren en funcionamiento en relación con [op.cont.2]. Consultar la última prueba que garantice la entrada en funcionamiento en el tiempo establecido.</i></p>		<p><u>Observaciones auditoría:</u></p>

<p>Firma: _____</p> <p>Auditor: _____</p>	<p style="text-align: center;">Verificación del cumplimiento del ENS</p> <p>Fecha y hora de inicio: ____/____/____.____:____</p> <p>Fecha y hora de fin: ____/____/____.____:____</p>
---	---

ANEXO I. DEFINICIÓN DE TÉRMINOS

Término	Descripción
CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
Firewall	Cortafuegos
Plan de seguridad	Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos (CCN-STIC-410).
Router	Enrutador
Switch	Conmutador
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TIC	Tecnologías de la Información y las Comunicaciones
VPN	Red privada virtual

ANEXO II. PLANTILLA DE INFORME DE AUDITORÍA

Esta plantilla está diseñada para ser utilizada para la redacción del informe de auditoría externa del ENS que es obligatoria para los sistemas de categoría media y alta, y voluntaria para los de básica. Puede así mismo ser utilizado para la redacción del informe de autoevaluación requerido para los sistemas de categoría básica.

INFORME DE AUDITORÍA

1. Introducción

Esta auditoría sobre el grado de cumplimiento del Esquema Nacional de Seguridad se encuadra de los requisitos del Artículo 34 (Auditoría de la Seguridad) y del Anexo III (Auditoría de la Seguridad) del Real Decreto 3/2010, de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Cargo	Nombre completo	Firma	Fecha
Auditor Jefe o Líder del equipo auditor		/...../.....
Responsable de la Seguridad		/...../.....
Responsable del Sistema		/...../.....

2. Tipo de auditoría

[En caso de tratarse de una auditoría ordinaria] Se trata de una auditoría ordinaria.

[En caso de tratarse de una auditoría extraordinaria] Se trata de una auditoría extraordinaria con motivo de modificaciones sustanciales en el sistema de información

.....

3. Objetivo

Dar cumplimiento a lo establecido en el Artículo 34 y en el Anexo III del RD 3/2010 y, por lo tanto, verificar el cumplimiento de los requisitos establecidos por el RD 3/2010 del ENS.

4. Alcance

El alcance de la presente auditoría se ciñe a [*identificar el/los sistema/s auditado/s*], de categoría , de [*identificar el organismo propietario del sistema auditado*]

Áreas organizativas, módulo o funciones del sistema de información cubiertas por la auditoría.....

[*Indicar si ha habido limitaciones al alcance o durante la realización de pruebas o revisiones*]

5. Resumen ejecutivo

[*Indicar las fortalezas y deficiencias identificadas, resumiendo los aspectos más relevantes o las áreas de acción más significativas, y el grado de cumplimiento. Utilizar en todo momento lenguaje no técnico*]

6. Criterio metodológico utilizado

Para la ejecución de la presente auditoría se ha seguido el criterio metodológico [*identificar tanto el proceso metodológico aplicado como la tipología de pruebas realizadas*]

7. Legislación que afecta al sistema de información

Para la ejecución de la presente auditoría se ha tenido en cuenta la legislación que afecta al sistema de información objeto de la misma a fecha de la auditoría, que es:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [*si aplica la LOPD*].

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [*si aplica la LOPD*].
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
-

8. Equipo auditor

El equipo auditor ha estado compuesto por:

- Auditor jefe o líder del equipo auditor:
- Auditor: [*repetir por cuantos auditores haya habido*]
- Experto técnico: [*repetir por cuantos expertos haya habido*]

9. Personal entrevistado

Durante la auditoría se ha entrevistado a:

- [*nombre del puesto, repetir por cuantos perfiles entrevistados haya habido*]

10. Fecha y lugar de realización

La auditoría comenzó el de de 2.0... , y ha finalizado el de de 2.0... y se desarrolló en [*si ha habido varias localizaciones para el trabajo de campo, indicar la fecha para cada una de ellas*]

11. Idioma

La auditoría se realizó en idioma/s

12. Documentación revisada

Para la correcta ejecución de la auditoría se revisó la siguiente documentación:

- Política de seguridad (versión)
- Análisis de riesgos (versión)
- Declaración de aplicabilidad (versión) (que incluya el nivel de cada medida de seguridad del ENS aplicable)
-

13. Resultado de la auditoría

[Indicar:

- *Categoría del sistema, con detalle del nivel de seguridad en cada una de las dimensiones de seguridad.*
- *El grado de confianza en las revisiones de la Dirección y auditorías internad del auditado (si las hubiera).*
- *Los hallazgos identificados, tanto de conformidad como de no conformidad, incluyendo observaciones (Datos, hechos y observaciones)*
- *Los detalles de las no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la certificación.*
- *comentarios sobre la conformidad del sistema de gestión de la seguridad del auditado con los requisitos de la certificación, con una redacción clara de las no conformidades que hubieran podido evidenciarse, así como cualquier comparación útil con los resultados de auditorías de seguridad previas.*
- *Riesgos que provocan las no conformidades encontradas.*
- *La conclusión o dictamen de la auditoría sobre si el sistema de información auditado debe ser certificado o no, con información que soporte esa conclusión.*

14. Comentarios al informe por los participantes

[Indicar los comentarios que los participantes hayan podido realizar a raíz de la presentación de los resultados de las revisiones y pruebas, antes de la emisión del informe de auditoría]

15. Conclusiones y dictamen

[Indicar el grado de cumplimiento del ENS] (Favorable/ Favorable con no conformidades o Desfavorable

Anexo I

[Detalles y resultados de las pruebas que permiten llegar a las conclusiones del informe, agrupándolos por los apartados del mismo]

Anexo II

[Contestación al informe por parte del Responsable de Seguridad o acciones que se tomarán para solucionar las deficiencias, si las hubiera]

ANEXO III. TABLA DE VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS

Descargar hoja Excel adjunta a esta guía CCN-STIC-808.