GUÍA DE SEGURIDAD
(CCN-STIC-808)

VERIFICACIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS EN EL ENS

19 DE OCTUBRE 2010

BORRADOR

Edita:



© Editor y Centro Criptológico Nacional, 2010
NIPO: 076-08-238-1

Tirada: 1000 ejemplares
Fecha de Edición: octubre de 2010
Andrés Méndez Barco y Javier Almendro Sagristá han elaborado el presente documento.
El Ministerio de Política Territorial y Administración Pública ha financiado el desarrollo del presente documento y sus anexos.

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

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

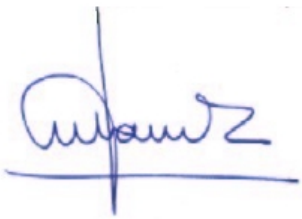
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

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

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

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

Octubre de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

BORRADOR

ÍNDICE

1. INTRODUCCIÓN Y MARCO DE REFERENCIA 4
2. OBJETO 4
3. ALCANCE 4
4. CÓMO UTILIZAR ESTA GUÍA 4
5. VERIFICACIÓN CUMPLIMIENTO "ANEXO II. MEDIDAS DE SEGURIDAD" 6
5.1. MARCO ORGANIZATIVO 7
5.2. MARCO OPERACIONAL 13
5.3. MEDIDAS DE PROTECCIÓN 48
6. ANEXO I. DEFINICIÓN DE TÉRMINOS 87
7. ANEXO II. PLANTILLA DE INFORME DE AUDITORÍA 88

BORRADOR

1. INTRODUCCIÓN Y MARCO DE REFERENCIA

1. El Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), en su artículo 34 (Auditoría de la seguridad) y en su Anexo III (Auditoría de la seguridad), establece la obligatoriedad de la realización de una auditoría de seguridad para los sistemas de categoría media y alta de forma ordinaria cada dos años, o de forma extraordinaria cada vez que se produzcan modificaciones sustanciales en el sistema de información.
2. La presente guía viene a complementar a la guía "CCN-STIC-802 Esquema Nacional de Seguridad – Guía de auditoría".

2. OBJETO

3. 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.

BORRADOR

3. ALCANCE

4. Esta guía es de aplicación a cualquier entidad pública española que deba cumplir con los preceptos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007 de 22 de junio), de la que emana el Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), con independencia de su naturaleza o dimensión y cuyos sistemas se hayan clasificado como de nivel medio o alto.

4. CÓMO UTILIZAR ESTA GUÍA

5. 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.
6. 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:
    a. ☑ si lo cumple.
    b. ☒ si no lo cumple.
7. Con objeto de 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.

8. Igualmente, con objeto de cumplir el apartado 5 del artículo 34 del RD 3/2010 en el que se indica que "El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto", se sugiere el uso del número de casillas marcadas como ☑ a la hora de valorar el grado de cumplimiento, considerándose que una medida de seguridad tendrá el siguiente grado de cumplimiento:
    a. Completo (100%): Si todos los requisitos de la medida de seguridad están satisfechos.
    b. Alto (50%-99%): Si sólo la mitad de los requisitos de la medida de seguridad están satisfechos.
    c. Bajo (1%-49%): Si menos de la mitad de los requisitos de la medida de seguridad están satisfechos.
    d. Nulo (0%): Si ninguno de los requisitos de la medida de seguridad están satisfechos.
9. 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", apartado "3.4 Programa de auditoría"), por lo que deberá marcar "No" si la ha omitido. Aquellas medidas que deben auditarse siempre no permiten marcar "No".
10. 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 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.

BORRADOR

5. VERIFICACIÓN CUMPLIMIENTO "ANEXO II. MEDIDAS DE SEGURIDAD"

11. Este apartado se divide en aquellos grupos que componen las medidas de seguridad, es decir, marco organizativo, marco operacional y medidas de protección.
12. 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.
13. 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.

BORRADOR

5.1. MARCO ORGANIZATIVO

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
org	***MARCO ORGANIZATIVO***			
org.1	*Política de seguridad*			
	Básica - D, A, I, C, T	☐ 1.- ¿Dispone de una política de seguridad escrita? *Evidencia: La política de seguridad está impresa o guardada en formato electrónico.* Respecto a dicha política de seguridad: ☐ 1.1.- ¿Ha sido aprobada por el órgano superior competente (de acuerdo a lo establecido en el artículo 11 del RD 3/2010)? *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).* ☐ 1.2.- ¿Precisa los objetivos y misión de la organización? *Evidencia: Dentro de la política se indica cuáles son los objetivos (p.ej: reducir el número de quejas en un 10% con respecto al año anterior) y la misión (p.ej: prestar servicios de calidad en materia de gestión educativa a los ciudadanos) de la organización.* ☐ 1.3.- ¿Precisa el marco legal y regulatorio en el que se desarrollarán las actividades? *Evidencia: Dentro de la política se indican las leyes que le son de aplicación (LO 15/1999, RD 1720/2007, L 11/2007, RD 3/2010, etc.) así como las distintas regulaciones que pudieran existir (ámbito europeo, local, etc.).* ☐ 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? *Evidencia: Dentro de la política se indican los roles de seguridad (responsable de la información, responsable del servicio, responsable de la seguridad ó*	Aplica: ☐ Sí Lo audito: ☐ Sí	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		STIC, responsable del sistema ó 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.). ☐ 1.5.- ¿Precisa la estructura del comité/s para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización? *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.).* ☐ 1.6.- ¿Precisa las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso? *Evidencia: Dentro de la política se indica cuál es el procedimiento para la clasificación de los documentos, quién debe generarla y aprobarla, qué personas pueden acceder a ella, etc.* ☐ 1.7.- En aquello en lo que se corresponda con el Documento de Seguridad exigido por el R.D. 1720/2007 ¿hace referencia y es coherente con el mismo? *Evidencia: Roles de los responsables, identificación de ficheros/activos, plan de auditoría, etc.* ☐ 1.8.- ¿Ha sido difundida, así como cualquier actualización de la misma, entre el personal afectado? *Evidencia: Colocar la política en el tablón de anuncios accesible por el personal afectado, en la intranet, envío mediante circular escrita o por e-mail, etc. Si hay varias versiones, constatar que se ha avisado de la existencia de nuevas versiones, así como de lo que ha cambiado.* Consultar guías: ***CCN-STIC-001*** *Seguridad de las TIC en la Administración* ***CCN-STIC-201*** *Organización y Gestión para la Seguridad de las TIC* ***CCN-STIC-203*** *Estructura y Contenido de los Procedimientos Operativos de Seguridad (POS)* ***CCN-STIC-400*** *Manual de Seguridad de las TIC*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-402 *Organización y Gestión para la Seguridad de los Sistemas TIC* ***CCN-STIC-801*** *ENS Responsables y Funciones*		
org.2	*Normativa de seguridad*			
	Básica - D, A, I, C, T	☐ 1.- ¿Dispone de uno o varios documentos que constituyan la normativa de seguridad escrita? *Evidencia: La normativa de seguridad está impresa o guardada en formato electrónico, la ha elaborado el responsable STIC y está aprobada por el Comité STIC. Además, se indica que es de obligado cumplimiento y existe un procedimiento de revisión y firma regular.* Respecto a dicha normativa de seguridad: ☐ 1.1.- ¿Precisa el uso correcto de equipos, servicios e instalaciones? *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* ☐ 1.2.- ¿Precisa lo que se considera uso indebido? *Evidencia: Existen normativas que indican lo que se considera un uso indebido de los equipos (p.ej: utilizar el ordenador para fines personales), las instalaciones (p.ej: comer en la sala de servidores), la información (p.ej: enviar datos confidenciales mediante correo electrónico sin cifrar), etc.* ☐ 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)? *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).* ☐ 1.4.- ¿Ha sido difundida, así como cualquier actualización de la misma, entre el personal afectado? *Evidencia: Colocar la normativa accesible por el personal afectado, en la intranet, envío mediante circular escrita o por e-mail, etc. Si hay varias versiones, constatar que se ha avisado de la existencia de nuevas versiones, así como de lo que ha cambiado.* Consultar guías:	Aplica: ☐ Sí Lo audito: ☐ Sí	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-402 *Organización y Gestión para la Seguridad de los Sistemas TIC* ***Criterios de seguridad*** *Capítulos 3 y 17*		
org.3	*Procedimientos de seguridad*			
	Básica - D, A, I, C, T	☐ 1.- ¿Dispone de uno o varios documentos que constituyan los procedimientos de seguridad escritos? *Evidencia: Los procedimientos de seguridad están impresos 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 aproximadamente el 80% de las actividades rutinarias (p.ej: sobre la modificación de reglas en el firewall, las tareas de backup, el alta de usuarios, identificación y cobertura de nuevas necesidades, etc.).* Respecto a dichos procedimientos de seguridad: ☐ 1.1.- ¿Precisan cómo llevar a cabo las tareas habituales? *Evidencia: Cada procedimiento debe cubrir, entre otros, en qué condiciones se aplica, qué se debe hacer, qué registros quedan de las actividades, y cómo reportar deficiencias en el procedimiento.* ☐ 1.2.- ¿Precisan quién debe hacer cada tarea? *Evidencia: Se asigna a cada tarea a un rol (responsable STIC, administrador, operador, etc.) y una frecuencia.* ☐ 1.3.- ¿Precisan cómo identificar y reportar comportamientos anómalos? *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).* Consultar guías: ***CCN-STIC-203*** *Estructura y contenido de los procedimientos operativos de seguridad (POS)* ***Criterios de seguridad*** *Capítulo 3*	Aplica: ☐ Sí Lo audito: ☐ Sí	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
org.4	*Proceso de autorización*			
	Básica - D, A, I, C, T	☐ 1.- ¿Existe un proceso formal para las autorizaciones respecto a los sistemas de información? *Evidencia: Cada proceso de autorización debe haber quedado reflejado en la normativa y cada solicitud debe contener: Descripción del elemento o*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		actuación (componente) para la que se solicita la autorización, de las actividades para las que se requiere el nuevo componente, 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. *A continuación se exponen los elementos sobre los cuales debe existir un proceso de autorización, que debe contener* Respecto a dicho proceso de autorización: ☐ 1.1.- ¿Cubre la utilización de instalaciones, tanto habituales como alternativas (p.ej: acceso al CPD, etc.)? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.2.- ¿Cubre la entrada de equipos en producción, en particular, equipos que involucren criptografía? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.3.- ¿Cubre la entrada de aplicaciones en producción (p.ej: actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.)? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.4.- ¿Cubre el establecimiento de enlaces de comunicaciones con otros sistemas? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.5.- ¿Cubre la utilización de medios de comunicación (tanto habituales como alternativos)? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.6.- ¿Cubre la utilización de soportes de información (p.ej: cintas de backup, DVD, memorias USB, etc.)? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 1.7.- ¿Cubre la utilización de equipos móviles (ordenadores portátiles, PDA, etc.)? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* ☐ 1.8.- ¿Ha sido difundido, así como cualquier actualización de los mismos, entre el personal afectado? *Evidencia: Existe evidencia documental de que estos recursos han sido autorizados antes de su entrada en explotación.* Consultar guías: ***CCN-STIC-002*** *Coordinación criptológica* ***CCN-STIC-302*** *Interconexión de sistemas de las tecnologías de la información y las comunicaciones que manejan información nacional clasificada en la administración* ***Criterios de seguridad*** *Capítulo 13*		

BORRADOR

5.2. MARCO OPERACIONAL

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
op	***MARCO OPERACIONAL***			
op.pl	*PLANIFICACIÓN*			
op.pl.1	*Análisis de riesgos*			
	Básica - D, A, I, C, T	☐ 1.- ¿Dispone de un análisis de riesgos, al menos, informal? *Evidencia: Dispone de un documento aprobado por la Dirección en el que se ha realizado una exposición textual en lenguaje natural del análisis de riesgos. Existe un procedimiento para la revisión y aprobación regular del análisis de riesgos.* Respecto a dicho análisis de riesgos: ☐ 1.1.- ¿Identifica los activos más valiosos del sistema? *Evidencia: En el documento se identifican los servicios que presta la organización en referencia al cumplimiento de la Ley 11/2007 (p.ej: servicio 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.).* ☐ 1.2.- ¿Identifica las amenazas más probables? *Evidencia: En el documento se identifican las amenazas más probables (p.ej: incendio, robo, virus informático, ataque informático, etc.).* ☐ 1.3.- ¿Identifica las salvaguardas que protegen de dichas amenazas? *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.).* ☐ 1.4.- ¿Identifica los principales riesgos residuales? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 5*	Aplica: ☐ Sí Lo audito: ☐ Sí	Registros: ☐ Documento: ☐ Registro: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Media - D, A, I, C, T	☐ 2.- ¿Dispone de un análisis de riesgos, al menos, semi-formal? *Evidencia: Dispone de un documento aprobado por la Dirección 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. Existe un procedimiento para la revisión y aprobación regular del análisis de riesgos.* Respecto a dicho análisis de riesgos: ☐ 2.1.- ¿Identifica y valora cualitativamente los activos más valiosos del sistema? *Evidencia: En el documento se identifican los servicios que presta la organización en referencia al cumplimiento de la Ley 11/2007 (p.ej: servicio 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).* ☐ 2.2.- ¿Identifica y cuantifica las amenazas más probables? *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).* ☐ 2.3.- ¿Identifica y valora las salvaguardas que protegen de dichas amenazas (p.ej: extintor en todos los pasillos, antivirus en todos los servidores, puerta con cerradura sólo en el CPD, etc.)? *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.).* ☐ 2.4.- ¿Identifica y valora el riesgo residual? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 5* ***CCN-STIC-803*** *ENS Valoración de los sistemas* ***MAGERIT v2***	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Registro: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Alta - D, A, I, C, T	☐ 3.- ¿Dispone de un análisis de riesgos formal? *Evidencia: Dispone de un documento aprobado por la Dirección 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. Existe un procedimiento para la revisión y aprobación regular del análisis de riesgos. Utiliza una herramienta reconocida de análisis de riesgos (p.ej: PILAR, CRAMM, EBIOS, etc.).* Respecto a dicho análisis de riesgos: ☐ 3.1.- ¿Identifica y valora cualitativamente los activos más valiosos del sistema? *Evidencia: En el documento se identifican los servicios que presta la organización en referencia al cumplimiento de la Ley 11/2007 (p.ej: servicio 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).* ☐ 3.2.- ¿Identifica y cuantifica las amenazas posibles? *Evidencia: En el documento se identifican las amenazas más probables, su frecuencia y degradación (p.ej: incendio con baja probabilidad y degradación total, robo con baja probabilidad y degradación total, virus con alta probabilidad y degradación parcial, etc.).* ☐ 3.3.- ¿Identifica las vulnerabilidades habilitantes de dichas amenazas? *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.).* ☐ 3.4.- ¿Identifica y valora las salvaguardas adecuadas? *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.* ☐ 3.5.- ¿Identifica y valora el riesgo residual? *Evidencia: En el documento se identifica el nivel de riesgo al que están expuestos los servicios (bajo, medio o alto).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: ***Criterios de seguridad*** *Capítulo 5* ***CCN-STIC-803*** *ENS Valoración de los sistemas* ***MAGERIT v2*** ***CCN-STIC-410*** *Análisis de riesgos en sistemas de la Administración* ***CCN-STIC-470x*** *Manual de usuario de PILAR*		
op.pl.2	*Arquitectura de seguridad*			
	Básica - D, A, I, C, T	☐ 1.- ¿Dispone de documentación de las instalaciones? *Evidencia: Dispone de un documento que detalla las instalaciones (p.ej: número de instalaciones, su ubicación, etc.). Existe un procedimiento para su revisión (bien explícitamente o implícitamente en los documentos de gestión de cambios).* ☐ 1.1.- ¿Precisa las áreas? *Evidencia: El documento detalla las áreas existentes (p.ej: CPD, zona de acceso público, zona de carga y descarga, zona de operadores, etc.).* ☐ 1.2.- ¿Precisa los puntos de acceso? *Evidencia: El documento detalla los puntos de acceso (p.ej: puerta principal, salida de emergencia, etc.).* ☐ 2.- ¿Dispone de documentación del sistema? *Evidencia: Dispone de un inventario de los sistemas de información. Existe un procedimiento para su revisión (bien explícitamente o implícitamente en los documentos de gestión de cambios).* ☐ 2.1.- ¿Precisa los equipos? *Evidencia: Dicho inventario describe los activos del sistema (p.ej: servidor de correo, robot de backup, etc.).* ☐ 2.2.- ¿Precisa las redes internas y conexiones al exterior? *Evidencia: Dicho inventario describe las redes existentes (p.ej: red local con direccionamiento 192.168.0.0/24, DMZ con direccionamiento 172.16.0.0/24, etc.) y los elementos de conexión al exterior (p.ej: la red local está separada de Internet mediante un firewall, etc.).* ☐ 2.3.- ¿Precisa los puntos de acceso al sistema? *Evidencia: Dicho inventario describe los puntos de acceso al sistema (p.ej: puestos de trabajo, consolas de administración, web de la intranet, etc.).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

PROHIBIDO

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 3.- ¿Dispone y tiene documentación de líneas de defensa? *Evidencia: Dicho inventario describe los sistemas de seguridad de que dispone (p.ej: firewalls, antivirus, antispam, antiphishing, etc.). Existe un procedimiento para su revisión (bien explícitamente o implícitamente en los documentos de gestión de cambios).* ☐ 3.1.- ¿Precisa los puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet? *Evidencia: Dicho inventario 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.).* ☐ 3.2.- ¿Precisa los cortafuegos, DMZ, etc.? *Evidencia: Dicho inventario 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.).* ☐ 3.3.- ¿Precisa la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa? *Evidencia: Se utilizan tecnologías de seguridad diferentes (p.ej: el antivirus del firewall es diferente del antivirus del servidor de correo, el sistema operativo del router es diferente del sistema operativo del firewall, etc.).* ☐ 4.- ¿Dispone de documentación del sistema de identificación y autenticación de usuarios? *Evidencia: Dispone de un documento que detalla los sistemas de identificación y autenticación de usuarios para cada sistema o servicio. Existe un procedimiento para su revisión (bien explícitamente o implícitamente en los documentos de gestión de cambios).* ☐ 4.1.- ¿Precisa el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga? *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 DNIe, el acceso a la consola de administrador del servidor es mediante usuario y contraseña, etc.).* ☐ 4.2.- ¿Precisa de ficheros o directorios para autenticar al usuario y		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		determinar sus derechos de acceso (p.ej: /etc/passwd en Linux, Active Directory en Windows, etc.)? *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.).* ☐ 5.- ¿Dispone y tiene documentación de los controles técnicos internos? *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.).* ☐ 5.1.- ¿Precisa la validación de datos de entrada, salida y datos intermedios? *Evidencia: En dicho documento se detalla cómo se controlan los datos una vez en los sistemas (p.ej: validación de rangos en los datos, bloqueo de caracteres no autorizados, etc.).* ☐ 6.- ¿Dispone de documentación del sistema de gestión con actualización y aprobación periódica? *Evidencia: Dispone de un documento que detalla cómo se gestionan dichos elementos (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.).* Consultar guías: ***Criterios de seguridad*** *Capítulos 8, 9, 13 y 14* ***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*		
	Media - D, A, I, C, T	☐ 7.- ¿Está esta documentación aprobada por la Dirección? *Evidencia: Los documentos han sido aprobados por la Dirección.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
op.pl.3	*Adquisición de nuevos componentes*			
	Básica - D, A, I, C, T	☐ 1.- ¿Existe un proceso formal para planificar la adquisición de nuevos componentes del sistema? *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.).* Respecto a dicho proceso de adquisición: ☐ 1.1.- ¿Atiende las conclusiones del análisis de riesgos [op.pl.1]? *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.* ☐ 1.2.- ¿Es acorde con la arquitectura de seguridad [op.pl.2]? *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).* ☐ 1.3.- ¿Contempla las necesidades técnicas, de formación y de financiación de forma conjunta? *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 al cargo del componente dispone de la formación necesaria para su uso o se le proporcionará, y que ha recibido el consentimiento del departamento económico para su adquisición.* Consultar guías: ***Criterios de seguridad*** *Capítulo 4* ***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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D, A, I, C, T	☐ 2.- ¿Existe documentación semi-formal del plan de seguridad? *Evidencia: Está documentado el análisis de riesgos en lenguaje semi-formal.*	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
			Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	☐ 3.- ¿El plan de seguridad está aprobado por la Dirección? *Evidencia: El análisis de riesgos está tiene la firma o el reconocimiento formal de la Dirección.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.pl.4	*Dimensionamiento / gestión de capacidades*			
	Media - D	☐ 1.- ¿Antes de la puesta en explotación, se han estudiado las necesidades de dimensionamiento? *Evidencia: Dispone de un procedimiento documentado para el 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 satisfagan los requisitos establecidos. Existen evidencias documentales de cada estudio, en el que se refleja quién lo realizó.* Respecto a dicho estudio del dimensionamiento: ☐ 1.1.- ¿Cubre las necesidades de procesamiento? *Evidencia: Dicho estudio cubre las necesidades de procesamiento (p.ej: la CPU y memoria del dispositivo soportarán el número concurrente de sesiones estimadas).* ☐ 1.2.- ¿Cubre las necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse? *Evidencia: Dicho estudio cubre 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).* ☐ 1.3.- ¿Cubre las necesidades de comunicación? *Evidencia: Dicho estudio cubre las necesidades de comunicación (p.ej: el ancho de banda disponible soporta el volumen de datos a transmitir en cada*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		momento, o que el dispositivo soporta el acceso desde otra ubicación). ☐ 1.4.- ¿Cubre las necesidades de personal: cantidad y cualificación profesional? *Evidencia: Dicho estudio cubre las necesidades de personal necesario para la gestión del mismo (p.ej: existe personal con dedicación disponible 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).* ☐ 1.5.- ¿Cubre las necesidades de instalaciones y medios auxiliares? *Evidencia: Dicho estudio cubre 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).* Consultar guías: ***Criterios de seguridad*** *Capítulo 12*		
	Alta - D	☐ 1.6.- ¿El estudio está aprobado por la Dirección? *Evidencia: El estudio está tiene la firma o el reconocimiento formal de la Dirección.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.pl.5	*Componentes certificados*			
	Alta - D, A, I, C, T	☐ 1.- ¿Se utilizan preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales? *Evidencia: Dispone de un procedimiento documentado 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:* *- 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,*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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 directos que se ejecuten con información incorrecta pero sin manipular el normal funcionamiento del producto según su diseño.* *- Garantizar, al menos documentalmente, que el fabricante del producto dispone de procedimientos definidos para el tratamiento de futuras vulnerabilidades que se detecten en el producto.* *Existen evidencias de que los componentes han pasado dicha evaluación.* ☐ 2.- ¿Y están certificados por entidades independientes de reconocida solvencia? *Evidencia: Las certificaciones de los componentes han sido emitidas por entidades independientes de reconocida solvencia (p.ej: la entidad certificadora cumple la ISO/IEC 17025). Respecto a los componentes de cifra y generación de firma electrónica han sido certificados criptológicamente, en términos de su fortaleza algorítmica.* Consultar guías: ***Criterios de seguridad*** *Capítulos 9, 10, 11, 12, 13, 14 y 15* ***CCN-STIC-103*** *Catálogo de productos certificados* ***Common Criteria***		
op.acc	*CONTROL DE ACCESO*			
op.acc.1	*Identificación*			
	Baja - A, T	☐ 1.- ¿Cada entidad (usuario o proceso) que accede al sistema tiene asignado un identificador singular? *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: administracion, direccion, sistemas, becario, etc.).* Respecto a dicho identificador: ☐ 1.1.- ¿Se puede saber a quién corresponde? *Evidencia: Existe una relación de los identificadores con sus usuarios (p.ej: el identificador "webmaster" es de Jorge Pérez, pertenece al grupo "web" y*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		tiene por lo tanto permisos de lectura y escritura en la carpeta \web y de lectura en la carpeta \ftp). ☐ 1.2.- ¿Se puede saber qué derechos tiene? *Evidencia: 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).* ☐ 1.3.- ¿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? *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.* ☐ 1.4.- ¿El identificador se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas? *Evidencia: Dispone de un procedimiento documentado que identifica el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad (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).* Consultar guías: ***Criterios de seguridad*** *Capítulos 9 y 13* ***CCN-STIC-501A*** *Configuración segura Windows XP Professional SP2 (miembro de dominio)* ***CCN-STIC-503A*** *Configuración segura Windows Server 2003 (controlador de dominio)* ***CCN-STIC-509*** *Seguridad en servidores de ficheros Windows Server 2003 (servidor independiente/miembro de dominio)* ***CCN-STIC-517A*** *Configuración segura Windows Vista Enterprise (miembro de dominio)* ***CCN-STIC-521A*** *Configuración segura Windows Server 2008 R2* ***CCN-STIC-602*** *Configuración segura HP-UX 11i* ***CCN-STIC-610*** *Configuración segura RedHat Linux 7*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-611 *Configuración segura SUSE Linux Enterprise Server 9* ***CCN-STIC-625*** *Guía de securización de Solaris 10 con Oracle 10g*		
op.acc.2	*Requisitos de acceso*			
	Baja - A, I, C, T	☐ 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)? *Evidencia: Dispone de un procedimiento documentado que especifique que los sistemas, previos a su puesta en explotación o ya en producción, deben contar con un mecanismo de control de acceso. Para acceder a cualquier recurso es necesario estar identificado 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).* Respecto a dicha protección: ☐ 1.1.- ¿Incluye la protección frente al acceso a los componentes del sistema y a sus ficheros o registros de configuración? *Evidencia: El acceso a los ficheros de configuración del sistema sólo está autorizado al personal técnico.* ☐ 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? *Evidencia: La política y normativa de seguridad del sistema especifica 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.* Consultar guías: ***Criterios de seguridad*** *Capítulos 9 y 13* ***CCN-STIC-501A*** *Configuración segura Windows XP Professional SP2 (miembro de dominio)* ***CCN-STIC-503A*** *Configuración segura Windows Server 2003 (controlador de dominio)* ***CCN-STIC-509*** *Seguridad en servidores de ficheros Windows Server 2003 (servidor independiente/miembro de dominio)* ***CCN-STIC-517A*** *Configuración segura Windows Vista Enterprise (miembro de dominio)*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-521A *Configuración segura Windows Server 2008 R2* ***CCN-STIC-602*** *Configuración segura HP-UX 11i* ***CCN-STIC-610*** *Configuración segura RedHat Linux 7* ***CCN-STIC-611*** *Configuración segura SUSE Linux Enterprise Server 9* ***CCN-STIC-625*** *Guía de securización de Solaris 10 con Oracle 10g*		
op.acc.3	*Segregación de funciones y tareas*			
	Media - A, I, C, T	☐ 1.- ¿Existe segregación de funciones y tareas? *Evidencia: Dispone de un esquema de funciones y tareas en el que se contemplan las que son incompatibles en una misma persona. Dispone de un procedimiento documentado ligado a la gestión de recursos humanos que contempla que no se le puedan asignar tareas incompatibles a una misma persona.* Respecto a dicha segregación de funciones y tareas: ☐ 1.1.- ¿Contempla la incompatibilidad de tareas de desarrollo con las de operación? *Evidencia: En el esquema de funciones aparecen "desarrollo" y "operación", y están marcadas como incompatibles entre sí.* ☐ 1.2.- ¿Contempla la incompatibilidad de tareas de configuración y mantenimiento del sistema con las de de operación? *Evidencia: En el esquema de funciones aparecen "configuración y mantenimiento del sistema" y "operación", y están marcadas como incompatibles entre sí.* ☐ 1.3.- ¿Contempla la incompatibilidad de tareas de auditoría o supervisión con las de cualquier otra función relacionada con el sistema? *Evidencia: En el esquema de funciones aparece "auditoría o supervisión del sistema" y está marcada como incompatibles con todas las demás.* Consultar guías: ***Criterios de seguridad*** *Capítulo 20* ***CCN-STIC-801*** *ENS Responsables y funciones*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.acc.4	*Proceso de gestión de derechos de acceso*			
	Media - A, I, C, T	☐ 1.- ¿Se limitan los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones? *Evidencia: La política y normativa de seguridad especifican que a cada*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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). Dispone de un procedimiento documentado que especifica la frecuencia con la que se reasegura periódicamente el reconocimiento de la necesidad de acceso y de conocer, extinguiéndose cuando no se demuestre positivamente que la necesidad perdura. ☐ 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? *Evidencia: 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. Dispone de un procedimiento documentado que especifica que la modificación de privilegios vendrá precedida de una solicitud del responsable del recurso al que va a concedérsele acceso.* Consultar guías: ***Criterios de seguridad*** *Capítulos 6 y 13* ***CCN-STIC-801*** *ENS Responsables y funciones*		Observaciones auditoría:
	Alta - A, I, C, T	☐ 3.- ¿Se acredita por escrito la necesidad de acceso o de conocer? *Evidencia: Dispone de un procedimiento documentado que especifica que la modificación de privilegios vendrá precedida de una solicitud por escrito del responsable del recurso (información o proceso) al que va a concedérsele acceso.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.acc.5	*Mecanismo de autenticación*			
	Baja - A, I, C, T	☐ 1.- ¿Se encuentra identificado el mecanismo de autenticación en cada recurso? *Evidencia: Existe un listado de recursos que requieren autenticación y su mecanismo de autenticación correspondiente (p.ej: la intranet requiere autenticación mediante usuario y contraseña, el correo electrónico requiere*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		autenticación mediante usuario y contraseña). Respecto a dicho autenticador: ☐ 1.1.- Si utilizan contraseñas ¿cumplen las reglas básicas de calidad? *Evidencia: Dispone de una política o normativa documentada que especifica que deben utilizar contraseñas de más de 5 caracteres, que contengan caracteres alfabéticos y numéricos, que no repitan caracteres consecutivamente, 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* ☐ 1.2.- ¿Se activa una vez que esté bajo el control efectivo del usuario? *Evidencia: La cuenta del usuario no se habilita hasta que éste haya confirmado la recepción del autenticador.* ☐ 1.3.- ¿Están los autenticadores bajo el control exclusivo del usuario? *Evidencia: El autenticador sólo lo tiene el usuario. 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).* ☐ 1.4.- ¿Ha confirmado el usuario que ha recibido el identificador, 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? *Evidencia: Existe un registro de cada usuario confirmando la recepción del identificador y en el mismo se le informa de esos aspectos.* ☐ 1.5.- ¿Se cambian los autenticadores con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)? *Evidencia: Dispone de una política o normativa de seguridad documentada que especifica la periodicidad en el cambio de los autenticadores.* ☐ 1.6.- ¿Se retiran y deshabilitan los autenticadores cuando la entidad (persona, equipo o proceso) que autentican terminan su relación con el sistema? *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.*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: ***Criterios de seguridad*** *Capítulos 9 y 13*		
	Media - A, I, C, T	☐ 2.- ¿Se utilizan claves concertadas? *Evidencia: Constatar que ha sido analizado el empleo de este tipo de clave y que su uso está motivado.* ☐ 3.- Si utilizan contraseñas ¿cumplen las políticas rigurosas de calidad y renovación? *Evidencia: Dispone de una política o normativa documentada que aplica el recurso, por lo que obliga a utilizar contraseñas de más de 5 caracteres, 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 los autenticadores. El mecanismo de gestión de autenticadores obliga a utilizar contraseñas de más de 5 caracteres, 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 3 caracteres, además de que obliga a modificar la contraseña con la periodicidad estipulada).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - A, I, C, T	☐ 4.- ¿Se suspenden los autenticadores tras un periodo definido de no utilización? *Evidencia: Dispone de una política o normativa documentada para la revisión de autenticadores que no se estén utilizando, igualmente ésta indica el periodo máximo de inactividad de un autenticador antes de ser suspendido.* ☐ 5.- ¿Se utilizan claves concertadas o contraseñas? *Evidencia: No está permitido el uso de claves concertadas ni contraseñas. Se deben utilizar dispositivos físicos (tokens) o biometría.* ☐ 6.- ¿Se utilizan dispositivos físicos (tokens)? *Evidencia: Dispone de un procedimiento documentado para la adquisición de componentes que empleen algoritmos acreditados por el Centro Criptológico Nacional y, preferentemente, certificados.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
op.acc.6	*Acceso local (local logon)*			
	Baja - A, I, C, T	☐ 1.- ¿Se previene la revelación de información del sistema? *Evidencia: Los diálogos de acceso (al puesto local dentro de la propia instalación de la organización, 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").* ☐ 2.- ¿Se limita el número de intentos fallidos de acceso? *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).* ☐ 3.- ¿Se registran los accesos con éxito y los fallidos? *Evidencia: El sistema de registro almacena tanto los accesos con éxito como los fallidos.* ☐ 4.- ¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener el acceso? *Evidencia: Una vez habiendo accedido con éxito al sistema, éste muestra un aviso con las obligaciones del usuario.* Consultar guías: ***Criterios de seguridad*** *Capítulo 9* ***CCN-STIC-501A*** *Configuración segura Windows XP Professional SP2 (miembro de dominio)* ***CCN-STIC-503A*** *Configuración segura Windows Server 2003 (controlador de dominio)* ***CCN-STIC-509*** *Seguridad en servidores de ficheros Windows Server 2003 (servidor independiente/miembro de dominio)* ***CCN-STIC-517A*** *Configuración segura Windows Vista Enterprise (miembro de dominio)* ***CCN-STIC-521A*** *Configuración segura Windows Server 2008 R2*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-602 *Configuración segura HP-UX 11i* ***CCN-STIC-610*** *Configuración segura RedHat Linux 7* ***CCN-STIC-611*** *Configuración segura SUSE Linux Enterprise Server 9* ***CCN-STIC-625*** *Guía de securización de Solaris 10 con Oracle 10g*		
	Media - A, I, C, T	☐ 5.- ¿Informa el sistema al usuario del último acceso con su identidad con éxito? *Evidencia: Una vez habiendo accedido con éxito al sistema, éste muestra la fecha y hora del último acceso con éxito de ese usuario.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - A, I, C, T	☐ 6.- ¿Se limita el horario, fechas y lugar desde donde se accede? *Evidencia: Dispone de una política o normativa documentada que indica el horario, fechas y lugar desde donde está autorizado el acceso. Existen mecanismos para aplicar dicha política o normativa.* ☐ 7.- ¿Se han establecido puntos en los que el sistema requerirá una renovación de la autenticación del usuario? *Evidencia: Dispone de una política o normativa documentada 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 el usuario y autenticador).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.acc.7	*Acceso remoto (remote login)*			
	Baja - A, I, C, T	☐ 1.- ¿Se garantiza la seguridad del sistema cuando acceden remotamente usuarios u otras entidades? *Evidencia: Cumple los requisitos de las medidas [op.acc.6], [mp.com.2] y [mp.com.3].* Consultar guías: ***Criterios de seguridad*** *Capítulo 13*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Media - A, I, C, T	☐ 2.- ¿Está documentado lo que puede hacerse remotamente? *Evidencia: Dispone de una política o normativa documentada que regula las actividades que pueden realizarse remotamente.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp	*EXPLOTACIÓN*			
op.exp.1	*Inventario de activos*			
	Baja - D, A, I, C, T	☐ 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 naturaleza (p.ej: router Cisco 2128, servidor Dell PowerEdge R420, etc.).* Respecto a dicho inventario: ☐ 1.1.- ¿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).* ☐ 1.2.- ¿Se mantiene actualizado? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 6*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D, A, I, C, T	☐ 1.3.- ¿Se retiene en el inventario los componentes desmantelados? *Evidencia: Están identificados en el inventario los elementos que se encuentran desmantelados, así como su fecha de desmantelación.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp.2	*Configuración de seguridad*			

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Baja - D, A, I, C, T	☐ 1.- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación? *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: recomendaciones de securización del CCN). Dispone de un procedimiento documentado que indica la frecuencia con la que se revisan dichos perfiles, tanto periódico como a raíz de la publicación de vulnerabilidades en los sistemas.* Respecto a dicho procedimiento de bastionado: ☐ 1.1.- ¿Indica que se retiren las cuentas y contraseñas estándar? *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.).* ☐ 1.2.- ¿Indica que el sistema proporcione la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad? *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.* ☐ 2.- En caso de existir situaciones que puedan poner en riesgo la seguridad ¿indica el sistema esa posibilidad al usuario, y tiene éste que dar su consentimiento expreso asumiendo el riesgo? *Evidencia: 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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: ***CCN-STIC-501A*** *Configuración segura Windows XP Professional SP2 (miembro de dominio)* ***CCN-STIC-503A*** *Configuración segura Windows Server 2003 (controlador de dominio)* ***CCN-STIC-509*** *Seguridad en servidores de ficheros Windows Server 2003 (servidor independiente/miembro de dominio)* ***CCN-STIC-517A*** *Configuración segura Windows Vista Enterprise (miembro de dominio)* ***CCN-STIC-521A*** *Configuración segura Windows Server 2008 R2* ***CCN-STIC-602*** *Configuración segura HP-UX 11i* ***CCN-STIC-610*** *Configuración segura RedHat Linux 7* ***CCN-STIC-611*** *Configuración segura SUSE Linux Enterprise Server 9* ***CCN-STIC-625*** *Guía de securización de Solaris 10 con Oracle 10g*		
	Media - D, A, I, C, T	☐ 1.3.- ¿Dispone de un procedimiento de revisión de la configuración? *Evidencia: Dispone de un procedimiento documentado que indica la frecuencia con la que se revisan los perfiles, tanto periódico como a raíz de la publicación de vulnerabilidades en los sistemas.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp.3	*Gestión de la configuración*			
	Media - D, A, I, C, T	☐ 1.- ¿Se gestiona de forma continua la configuración? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulos 16 y 17*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp.4	*Mantenimiento*			

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Baja - D, A, I, C, T	☐ 1.- ¿Dispone de un plan de mantenimiento del equipamiento físico y lógico? *Evidencia: Dispone de un procedimiento documentado que indica la frecuencia y componentes a revisar. Solicitar evidencias de la ejecución del plan.* Respecto a dicho plan de mantenimiento: ☐ 1.1.- ¿Atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas? *Evidencia: Dispone de las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. El procedimiento refleja dichas especificaciones.* ☐ 1.2.- ¿Efectúa un seguimiento continuo de los anuncios de defectos? *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.* ☐ 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? *Evidencia: Dispone de un procedimiento documentado que indica quién y con qué frecuencia monitorizar esos anuncios, así 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.* Consultar guías: ***Criterios de seguridad** Capítulos 12, 16 y 17*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp.5	*Gestión de cambios*			
	Media - D, A, I, C, T	☐ 1.- ¿Dispone de un control continuo de cambios realizados en el sistema? *Evidencia: Dispone de un procedimiento documentado que indica la frecuencia y 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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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). Respecto a dicho control de cambios: ☐ 1.1.- ¿Analiza todos los cambios anunciados por el fabricante o proveedor para determinar su conveniencia para ser incorporados o no? *Evidencia: Dispone de evidencias del análisis de todos los cambios anunciados, así como del motivo de su aplicación o no.* ☐ 1.2.- ¿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? *Evidencia: Dicho procedimiento contempla la realización de pruebas previas a la puesta en producción del cambio. Consultar el último cambio realizado, el resultado de las pruebas y el sistema en el que se realizaron dichas pruebas.* ☐ 1.3.- ¿Se planifican los cambios para reducir el impacto sobre la prestación de los servicios afectados? *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 estima oportuno.* ☐ 1.4.- ¿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? *Evidencia: Dicho procedimiento contempla la actualización previa al cambio del análisis de riesgos (que contempla la situación tras el cambio) y, en caso de que el riesgo resultante sea alto, requerirá la aprobación explícita del cambio por parte del propietario.* Consultar guías: ***Criterios de seguridad*** *Capítulos 12, 16 y 17*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
op.exp.6	*Protección frente a código dañino*			
	Baja - D,A, I, C, T	☐ 1.- ¿Dispone de mecanismos de prevención y reacción frente a código dañino? *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 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.* Respecto a dichos mecanismos frente a código dañino: ☐ 1.1.- ¿Siguen un mantenimiento conforme a las recomendaciones del fabricante? *Evidencia: Las opciones de configuración 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.* Consultar guías: ***Criterios de seguridad** Capítulo 9*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.exp.7	*Gestión de incidencias*			
	Media - D, A, I, C, T	☐ 1.- ¿Dispone de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema? *Evidencia: Dispone de un procedimiento documentado para la gestión de incidencias. Consultar incidencias de este tipo y, si no existe ninguna 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 ninguna incidencia (p.ej: porque no se han producido incidentes de seguridad, o porque el personal desconoce el procedimiento y por lo tanto no las reporta, etc.).* Respecto a dicho procedimiento: ☐ 1.1.- ¿Incluye el reporte de incidentes reales o sospechados, detallando el escalado de la notificación? *Evidencia: Dicho procedimiento contempla el reporte tanto de incidencias reales como sucesos sospechosos (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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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 incidencias. ☐ 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)? *Evidencia: Dicho procedimiento contempla la toma de medidas urgentes en base a un procedimiento de valoración de la urgencia. 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, etc.* ☐ 1.3.- ¿Incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente? *Evidencia: Dicho procedimiento contempla la asignación de recursos para investigar las causas del incidente, analizar las consecuencias y resolver el incidente.* ☐ 1.4.- ¿Incluye el aviso a las partes interesadas (internas y externas)? *Evidencia: Dicho procedimiento contempla el aviso a las partes 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 que pudieran causar problemas similares en otras organizaciones, el procedimiento contempla la notificación de los mismos al CERT.* ☐ 1.5.- ¿Incluye medidas de prevención de la repetición del incidente? *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 ligado al de "[op.exp.3] Gestión de la configuración", "[op.exp.5] Gestión de cambios" y "[op.exp.2] Configuración de seguridad".* ☐ 1.6.- ¿Incluye en los procedimientos de usuario la identificación y forma de tratar el incidente? *Evidencia: Dispone de un procedimiento documentado para la gestión de incidencias orientado al usuario final, de forma que este sepa identificar y*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		resolver los incidentes más comunes. ☐ 1.7.- ¿Incluye el actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias? *Evidencia: El procedimiento de gestión de incidencias contempla su revisión periódica o a raíz de la identificación de posibles mejoras en el mismo.* ☐ 1.8.- En caso de afectar el incidente a ficheros con datos de carácter personal ¿contempla su gestión además lo dispuesto en la LO 15/1999? *Evidencia: El procedimiento documentado para la gestión de incidencias está alineado o integrado con el de gestión de incidencias de LOPD.* Consultar guías: ***Criterios de seguridad*** *Capítulos 17 y 18* ***CCN-STIC-403*** *Gestión de incidentes de seguridad*		
op.exp.8	*Registro de la actividad de los usuarios*			
	Media - T	☐ 1.- ¿Dispone de mecanismos que garanticen la corrección de la hora a la que se realiza el registro? *Evidencia: 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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - T	☐ 2.- ¿Se registran todas las actividades de los usuarios en el sistema? *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 herramientas para analizar los registros en busca de actividades fuera de lo normal.* Respecto a dichos registros: ☐ 2.1.- ¿Indican quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario? *Evidencia: Consultar si los mecanismos de registro 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 "tramites"). 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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 2.2.- ¿Incluye la actividad de los operadores y administradores del sistema? *Evidencia: 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.* ☐ 2.3.- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados? *Evidencia: Consultar si los mecanismos de registro almacenan ambos.* ☐ 2.4.- ¿La determinación de las actividades a registrar y su nivel de detalle se determina en base al análisis de riesgos del sistema? *Evidencia: La política o normativa los establece en base al resultado del análisis de riesgos.* Consultar guías: ***Criterios de seguridad** Capítulo 20* ***CCN-STIC-434** Herramientas para el análisis de ficheros de log*		
op.exp.9	*Registro de la gestión de incidencias*			
	Media - D, A, I, C, T	☐ 1.- ¿Se registran todas las actuaciones relacionadas con la gestión de incidencias ([op.exp.7])? *Evidencia: Dispone de un procedimiento documentado para la gestión de incidencias que incluye mantener un registro de todas las actuaciones relacionadas con la gestión de las mismas.* Respecto a dicho registro de las incidencias: ☐ 1.1.- ¿Se registran el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente? *Evidencia: El procedimiento de gestión de incidencias ([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".* ☐ 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? *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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		frente a una demanda judicial tras un incidente. ☐ 2.- ¿Se revisa la determinación de los eventos auditables en base al análisis de las incidencias? *Evidencia: Dispone de un procedimiento documentado para el análisis de las incidencias que alimente la determinación de qué eventos deben ser auditados.* Consultar guías: ***Criterios de seguridad** Capítulo 18*		
op.exp.10	*Protección de los registros de actividad*			
	Alta - T	☐ 1.- ¿Se encuentran protegidos los registros del sistema? *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.* Respecto a dichos registros: ☐ 1.1.- ¿Está determinado el periodo de retención de los mismos? *Evidencia: Dispone de un procedimiento documentado para la declaración formal, por parte del propietario del activo del cual se recogen los registros, del periodo de retención de los mismos. 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).* ☐ 1.2.- ¿La fecha y hora de los mismos está asegurada? *Evidencia: Dispone de mecanismos para garantizar la fecha y hora de su generación conforme a [mp.info.5].* ☐ 1.3.- ¿Se encuentran protegidos frente a su modificación o eliminación por personal no autorizado? *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.* ☐ 1.4.- ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos? *Evidencia: Dispone de una política o normativa de seguridad que determina*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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. Consultar guías: ***Criterios de seguridad** Capítulo 20*		
op.exp.11	*Protección de claves criptográficas*			
	Baja - D, A, I, C, T	☐ 1.- ¿Se protegen las claves criptográficas durante todo su ciclo de vida? *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).* ☐ 2.- ¿Se utilizan medios de generación aislados de los medios de explotación? *Evidencia: Dispone de una política o normativa documentada que especifica que los medios de generación deben estar aislados de los medios de explotación. Consultar dónde se generan.* ☐ 3.- ¿Las claves retiradas de operación que deban ser archivadas, lo son en medios aislados de los de explotación? *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. Consultar si se archivan en contenedores físicos seguros (p.ej: en una caja fuerte) o en contenedores criptográficos.* Consultar guías: ***Criterios de seguridad** Capítulo 10*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D, A, I, C, T	☐ 4.- ¿Se utilizan medios de generación y custodia en explotación evaluados o dispositivos criptográficos certificados? *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. Consultar la evaluación o certificación de los medios de generación.* ☐ 5.- ¿Los medios de generación y custodia en explotación emplean algoritmos acreditados por el CCN? *Evidencia: Dispone de una política o normativa documentada que especifica*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		que los medios de generación deben emplear algoritmos acreditados por el CCN. Consultar la acreditación de los algoritmos. ☐ 6.- ¿Los medios de custodia en explotación están protegidos? *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.*		
	Alta - D, A, I, C, T	☐ 7.- ¿Existe un registro que indique las actuaciones realizadas sobre cada clave en el sistema a lo largo de su ciclo de vida? *Evidencia: Dispone de un registro que indica las actuaciones realizadas sobre cada clave en el sistema a lo largo de su ciclo de vida.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.ext	*SERVICIOS EXTERNOS*			
op.ext.1	*Contratación y acuerdos de nivel de servicio*			
	Media - A, I, C, T	☐ 1.- ¿Se han analizado los riesgos de la contratación de servicios externos? *Evidencia: El análisis de riesgos identifica los riesgos asociados al proveedor externo.* Previamente a la utilización de recursos externos se ha establecido: ☐ 2.1.- ¿Las características del servicio prestado? *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.* ☐ 2.2.- ¿Lo que se considera calidad mínima y las consecuencias de su incumplimiento? *Evidencia: Dicho procedimiento requiere también el detalle de lo que se considera calidad mínima y las consecuencias para el proveedor de su incumplimiento.* ☐ 2.3.- ¿Las responsabilidades de las partes? *Evidencia: Dicho procedimiento requiere también el establecimiento de las funciones o roles, obligaciones y responsabilidades de cada parte.* Consultar guías:	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Criterios de seguridad *Capítulos 7 y 13*		
op.ext.2	*Gestión diaria*			
	Media - A, I, C, T	☐ 1.- ¿Dispone de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio? *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. Consultar los resultados de las mediciones.* ☐ 2.- ¿Dispone de un procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado? *Evidencia: Dicho procedimiento contempla un protocolo de actuación en caso de incumplimiento o degradación en la calidad acordada en [op.ext.1].* ☐ 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? *Evidencia: Dispone de un procedimiento documentado que define el mecanismo y los procedimientos de coordinación para 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.).* ☐ 4.- ¿Se han establecido el mecanismo y los procedimientos de coordinación en caso de incidencias y desastres? *Evidencia: El procedimiento de gestión de incidencias sobre el servicio externo estará relacionado con el definido en [op.exp.7].*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.ext.9	*Medios alternativos*			
	Alta - D	☐ 1.- ¿Dispone de un plan para reemplazar el servicio por medios alternativos en caso de indisponibilidad del servicio contratado? *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]).* ☐ 2.- ¿El servicio alternativo ofrece las mismas garantías de seguridad que	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		el servicio habitual? *Evidencia: Las características del servicio alternativo incluyen las mismas garantías de seguridad que el servicio habitual.*		
op.cont	*CONTINUIDAD DEL SERVICIO*			
op.cont.1	*Análisis del impacto*			
	Media - D	☐ 1.- ¿Se ha realizado un análisis de impacto que determine? *Evidencia: Dispone de un procedimiento documentado para el análisis de impacto de una contingencia en la continuidad del servicio, este contempla su revisión periódica o actualización tras cambios en los sistemas (ligado a [op.exp.3], [op.exp.4] y [op.exp.5]) y su aprobación por la Dirección. Consultar el último análisis de impacto así como el hecho que haya motivado su posible revisión o actualización.* Respecto a dicho análisis de impacto: ☐ 1.1.- ¿Identifica los requisitos de disponibilidad de cada servicio? *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.* ☐ 1.2.- ¿Identifica los elementos que son críticos para la prestación de cada servicio? *Evidencia: Dicho análisis de impacto identifica los elementos que son críticos para la prestación de cada servicio, bien sean propios o proporcionados por externos.* Consultar guías: ***Criterios de seguridad** Capítulo 19* ***CCN-STIC-470C** Manual de usuario de PILAR*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☑ Muestreo: Observaciones auditoría:
op.cont.2	*Plan de continuidad*			
	Alta - D	☐ 1.- ¿Dispone de un plan de continuidad? *Evidencia: Dispone de un plan de continuidad que establece las acciones a ejecutar en caso de interrupción de los servicios 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.* Respecto a dicho plan: ☐ 1.1.- ¿Identifica funciones, responsabilidades y actividades a realizar?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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. 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. ☐ 1.2.- ¿Existe una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios? *Evidencia: Dicho plan identifica los medios alternativos que 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]).* ☐ 1.3.- ¿Están los medios alternativos planificados y materializados en acuerdos o contratos con los proveedores correspondientes? *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.* ☐ 1.4.- ¿Han recibido las personas afectadas por el plan la formación específica relativa a su papel en el mismo? *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.* ☐ 1.5.- ¿Es parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad? *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.*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: ***Criterios de seguridad*** *Capítulo 19*		
op.cont.3	*Pruebas periódicas*			
	Alta - D	☐ 1.- ¿Se realizan pruebas periódicas para localizar y corregir, en su caso, los errores o deficiencias que puedan existir en el plan de continuidad? *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 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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 19*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.mon	*MONITORIZACIÓN DEL SISTEMA*			
op.mon.1	*Detección de intrusión*			
	Alta - A, I, C, T	☐ 1.- ¿Dispone de herramientas de detección o prevención de intrusión? *Evidencia: Dispone de una herramienta de detección o prevención de intrusión que se encuentra operativa. 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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 14* ***CCN-STIC-434*** *Herramientas de análisis de logs* ***CCN-STIC-953*** *Recomendaciones empleo herramienta Snort*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
op.mon.2	*Sistema de métricas*			
	Alta - A, I, C, T	☐ 1.- ¿Dispone de un conjunto de indicadores que midan el desempeño real del sistema en materia de seguridad? *Evidencia: Dispone de un procedimiento documentado para la asignación de la responsabilidad en la definición de indicadores y la frecuencia en la adición o eliminación de dichos indicadores. Para cada indicador se contempla el objetivo que se pretende medir, el responsable del indicador, el origen de la información, el procedimiento de recogida y tratamiento de los datos, la frecuencia de recogida de datos y de presentación de resultados y los criterios de valoración del indicador a efectos de reaccionar y tomar decisiones.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Respecto a dichos indicadores: ☐ 1.1.- ¿Miden el grado de implantación de las medidas de seguridad? *Evidencia: Existe un conjunto de indicadores aprobados por la Dirección 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.* ☐ 1.2.- ¿Miden la eficacia y eficiencia de las medidas de seguridad? *Evidencia: Existe un conjunto de indicadores aprobados por la Dirección para medir el la eficacia y eficiencia de las medidas de seguridad. Consultar los valores, su frecuencia de actualización y las medidas tomadas a cabo a raíz de su análisis.* ☐ 1.3.- ¿Miden el impacto de los incidentes de seguridad? *Evidencia: Existe un conjunto de indicadores aprobados por la Dirección para medir el impacto de los incidentes de seguridad. Consultar los valores, su frecuencia de actualización y las medidas tomadas a cabo a raíz de su análisis.*		

BORRADOR

5.3. MEDIDAS DE PROTECCIÓN

Aptdo.	Categoría - Dimensiones	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 - D, A, I, C, T	☐ 1.- ¿El equipamiento ha sido instalado en áreas separadas específicas para su función? *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.* Respecto a dichas áreas separadas: ☐ 1.2.- ¿Se controlan los accesos? *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 la persona que accede pone su nombre y firma en un listado de entradas, etc.).* Consultar guías: ***Criterios de seguridad*** *Capítulo 8*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.2	*Identificación de las personas*			
	Baja - D,A, I, C, T	☐ 1.- ¿El control de acceso a los locales donde hay equipamiento que forme parte del sistema de información se encuentra gestionado? *Evidencia: Dispone de una política o normativa documentada que establece una segregación de las funciones de la gestión del control de acceso a las salas separadas: autorización, ejecución y registro. Dichas funciones deben*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		recaer en, al menos, dos personas diferentes. Dispone de un listado de personas autorizadas para acceder a las salas separadas. Respecto a dicho control de acceso: ☐ 1.1.- ¿Se identifican a todas las personas que accedan a estos locales? *Evidencia: Dispone de un procedimiento documentado que especifica que cada persona que accede debe ser identificada.* ☐ 1.2.- ¿Se registran las entradas y salidas de personas? *Evidencia: Dicho procedimiento, que cumple los requisitos de la LOPD, especifica que para cada persona debe quedar registrada inequívocamente junto con su fecha y hora de entrada y salida, así como la persona que realiza el registro. Consultar el registro de accesos.* Consultar guías: ***Criterios de seguridad** Capítulo 8*		Observaciones auditoría:
	Media - D, A, I, C, T	☐ 1.3.- ¿Cuál es el periodo de retención de los registros de acceso? *Evidencia: Dicho procedimiento contempla la retención de los datos registrados durante el periodo aprobado por la Dirección, de acuerdo a la LOPD. Consultar los registros del comienzo del periodo de retención.* ☐ 1.4.- ¿Disponen de un mecanismo de identificación de las personas? *Evidencia: Dicho procedimiento establece que todas las personas porten una identificación visible. Observar si las personas que acceden a estos locales están identificadas visiblemente.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	☐ 2.- ¿Se encuentran segregadas totalmente las funciones de la gestión de acceso a los locales? *Evidencia: Dichas funciones recaen en tres personas diferentes.* ☐ 3.- ¿Se encuentran acompañados en todo momento los visitantes? *Evidencia: Dicho procedimiento contempla el acompañamiento en todo momento de los visitantes salvo autorización expresa de la persona responsable de la visita.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.3	*Acondicionamiento de los locales*			
	Baja - D, A, I, C, T	☐ 1.- ¿Los locales donde se ubican los sistemas de información y sus componentes disponen de las adecuadas condiciones de temperatura y humedad? *Evidencia: Dispone de una política o normativa documentada que especifica que el local debe contar con las adecuadas condiciones de temperatura y*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		humedad. Dispone de un procedimiento documentado para el control de que la temperatura y humedad se encuentren en los márgenes especificados por los fabricantes de los equipos. Consultar si hay aire acondicionado, termómetro e higrómetro en el CPD y si se encuentran en los valores recomendados. Respecto a dichos locales: ☐ 1.1.- ¿Cuentan con protección frente a las amenazas identificadas en el análisis de riesgos? *Evidencia: Dicha política o normativa contempla la protección del local 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]), prohibiendo la existencia de material innecesario en el 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 atractor de otras amenazas. Consultar las medidas existentes (p.ej: si el análisis de riesgos ha identificado como amenaza un incendio, se debe disponer de salvaguardas para ello como extintores, sensores de humo, etc.).* ☐ 1.2.- ¿Cuentan con protección del cableado frente a incidentes fortuitos o deliberados? *Evidencia: Dicha política o normativa 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).* Consultar guías: ***Criterios de seguridad** Capítulo 8*		Observaciones auditoría:
	Media - D, A, I, C, T	☐ 2.- ¿Cuenta con un plano del cableado? *Evidencia: Dispone de un procedimiento documentado para la elaboración y actualización de un plano del cableado que incluye el etiquetado de los cables. Consultar el plano.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	☐ 3.- ¿Existe equipamiento redundante en caso de fallo de los equipos principales de acondicionamiento?	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dispone de equipamiento redundante en caso de fallo de los equipos principales de acondicionamiento. ☐ 4.- ¿Se encuentra actualizado el etiquetado de los cables? *Evidencia: Dispone de un procedimiento documentado para la revisión y actualización del etiquetado de los cables. Consultar las etiquetas.*	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
mp.if.4	*Energía eléctrica*			
	Baja - D	☐ 1.- ¿Se garantiza el suministro de potencia eléctrica? *Evidencia: Dispone de una política o normativa documentada que especifica que el local debe contar con la potencia eléctrica necesaria.* ☐ 2.- ¿Se garantiza el correcto funcionamiento de las luces de emergencia? *Evidencia: Dispone de una política o normativa documentada que especifica el local debe contar con luces de emergencia. Dispone de un procedimiento documentado para la revisión del correcto funcionamiento de las luces de emergencia.* Consultar guías: ***Criterios de seguridad** Capítulos 8 y 12*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D	☐ 3.- ¿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? *Evidencia: Dispone de una política o normativa documentada que especifica el local debe contar con un sistema de alimentación ininterrumpida (compuesto por SAI 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. Ver el SAI. Consultar los registros de las pruebas que se hayan llevado a cabo para constatar que el SAI soporta el tiempo necesario para la terminación ordenada.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - D	☐ 4.- ¿Existe un contrato con un proveedor alternativo? *Evidencia: Dispone de una política o normativa documentada que indica la necesidad de disponer de una doble acometida eléctrica con otro proveedor. Consultar el contrato con el segundo proveedor.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.5	*Protección frente a incendios*			

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Baja - D	☐ 1.- ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incendios fortuitos o deliberados? *Evidencia: Dispone de una política o normativa documentada que especifica que se deben proteger los locales 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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 8*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.6	*Protección frente a inundaciones*			
	Media - D	☐ 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? *Evidencia: Dispone de una política o normativa documentada que especifica que se deben proteger los locales 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 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.).* Consultar guías: ***Criterios de seguridad*** *Capítulo 8*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.7	*Registro de entrada y salida de equipamiento*			
	Baja - A, I, C, T	☐ 1.- ¿Se lleva un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento? *Evidencia: Dispone de una política o normativa documentada que establece una segregación de las funciones de la gestión del control de entrada y salida de equipamiento a las salas separadas: autorización, ejecución y registro. Dichas funciones deben recaer en, al menos, dos personas diferentes. Dispone de un procedimiento documentado que 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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registro. Consultar el registro de entrada y salida de equipamiento. Consultar guías: ***Criterios de seguridad*** *Capítulo 8*		
	Media - A, I, C, T	☐ 2.- ¿Cuál es el periodo de retención de los registros de movimiento de equipamiento? *Evidencia: Dicho procedimiento contempla la retención de los datos registrados durante el periodo aprobado por la Dirección. Consultar los registros del comienzo del periodo de retención.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - A, I, C, T	☐ 3.- ¿Se encuentran segregadas totalmente las funciones de la gestión de movimiento de equipamiento? *Evidencia: Dichas funciones recaen en tres personas diferentes.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.if.9	*Instalaciones alternativas*			
	Alta - D	☐ 1.- ¿Está garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles? *Evidencia: Dispone de una política o normativa documentada que garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles. 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] Plan de continuidad").* Consultar guías: ***Criterios de seguridad*** *Capítulo 8*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.per	*GESTIÓN DEL PERSONAL*			
mp.per.1	*Caracterización del puesto de trabajo*			
	Media - D, A, I, C, T	☐ 1.- ¿Se ha caracterizado cada puesto de trabajo? *Evidencia: Dispone de una política o normativa documentada que contiene*	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		la caracterización de cada puesto de trabajo en materia de seguridad. Respecto a dicha caracterización: ☐ 1.1.- ¿Define las responsabilidades relacionadas con cada puesto de trabajo? *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.* ☐ 1.2.- ¿Define los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad? *Evidencia: Dicha política o normativa define los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad* ☐ 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? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 7*	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
mp.per.2	*Deberes y obligaciones*			
	Baja - D, A, I, C, T	☐ 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? *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 responsabilidades) firmados.* Respecto a dicha información de deberes y responsabilidades: ☐ 1.1.- ¿Se especifican las medidas disciplinarias a que haya lugar?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dicho documento informa de las medidas disciplinarias a que haya lugar. ☐ 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? *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.* ☐ 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? *Evidencia: Dicho documento informa de que las obligaciones de confidencialidad 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.* ☐ 2.- ¿Se han establecido, en el caso de personal contratado a través de un tercero, los deberes y obligaciones del personal? *Evidencia: Dispone de una normativa documentada que especifica los deberes y obligaciones del personal contratado a través de un tercero.* Respecto del personal contratado a través de un tercero: ☐ 2.1.- ¿Se han establecido los deberes y obligaciones de cada parte? *Evidencia: Dispone de una normativa documentada o contrato que incluye los deberes y obligaciones de cada parte.* ☐ 2.2.- ¿Se ha establecido el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones? *Evidencia: Dispone de un procedimiento documentado que define la resolución de incidentes relacionados con el incumplimiento de las obligaciones.* Consultar guías: ***Criterios de seguridad*** *Capítulo 7*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Media - C	☐ 3.- ¿Dispone del acuerdo de confidencialidad escrito y firmado? *Evidencia: Dispone, por cada persona, de su acuerdo de confidencialidad firmado.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.per.3	*Concienciación*			
	Baja - D, A, I, C, T	☐ 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? *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.* Respecto a dicha concienciación: ☐ 1.1.- ¿Forma parte del contenido la normativa de seguridad relativa al buen uso de los sistemas? *Evidencia: El contenido del plan de concienciación incluye la normativa de seguridad relativa al buen uso de los sistemas.* ☐ 1.2.- ¿Forma parte del contenido la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado? *Evidencia: El contenido del plan de concienciación incluye la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.* ☐ 1.3.- ¿Forma parte del contenido el procedimiento de reporte de incidencias de seguridad, sean reales o falsas alarmas? *Evidencia: El contenido del plan de concienciación incluye el procedimiento de reporte de incidencias de seguridad, sean reales o falsas alarmas.* Consultar guías: ***Criterios de seguridad** Capítulos 7 y 18*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D, A, I, C, T	☐ 1.4.- ¿Se encuentra ese plan financiado? *Evidencia: El responsable de la definición del plan de concienciación cuenta*	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		con la financiación necesaria para que esta actividad se lleve a cabo regularmente.	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	☐ 1.5.- ¿Existe constancia de que cada persona ha recibido y seguido el plan de concienciación? *Evidencia: Dispone de un registro que deje constancia de que cada persona ha recibido y seguido el plan de concienciación.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.per.4	*Formación*			
	Baja - A, I, C, T	☐ 1.- ¿Se forma regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones? *Evidencia: Dispone de un plan de formación en el que se identifican 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.* Respecto a dicha formación: ☐ 1.1.- ¿Cubre la configuración de sistemas? *Evidencia: Dicho plan tiene contenidos formativos relativos a la configuración de sistemas.* ☐ 1.2.- ¿Cubre la detección y reacción a incidentes? *Evidencia: Dicho plan tiene contenidos formativos relativos a la detección y reacción a incidentes.* ☐ 1.3.- ¿Cubre la gestión de la información en cualquier soporte en el que se encuentre? *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.* Consultar guías: ***Criterios de seguridad** Capítulos 7, 8 y 17*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Media - A, I, C, T	☐ 1.4.- ¿Existe constancia de la ejecución del plan formativo? *Evidencia: Dispone de registros de la recepción de la formación por parte del personal que estaba planificado.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.per.9	*Personal alternativo*			
	Alta - D	☐ 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? *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.* Respecto a dicho personal alternativo: ☐ 1.1.- ¿Está sometido a las mismas garantías de seguridad que el personal habitual? *Evidencia: El personal alternativo está sometido a las mismas garantías de seguridad que el personal habitual.* Consultar guías: ***Criterios de seguridad** Capítulo 9*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.eq	*PROTECCIÓN DE LOS EQUIPOS*			
mp.eq.1	*Puesto de trabajo despejado*			
	Baja - D, A, I, C, T	☐ 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? *Evidencia: Dispone de una política o normativa documentada que indica que los puestos de trabajo deben permanecer despejados, sin más material*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Dispone de un procedimiento disciplinario documentado asociado a su incumplimiento. Observar si se cumple. Consultar guías: ***Criterios de seguridad*** *Capítulos 7, 13 y 16*		Observaciones auditoría:
	Media - D, A, I, C, T	☐ 2.- ¿Se guarda este material de nivel medio en lugar cerrado cuando no se está utilizando? *Evidencia: Dicha política o normativa indica que el material de nivel medio se guardará en lugar cerrado cuando no se esté utilizando. Observar si los usuarios disponen de lugares donde guardar bajo llave este material.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.eq.2	*Bloqueo de puesto de trabajo*			
	Media - A	☐ 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? *Evidencia: Dispone de una política o normativa documentada relacionada 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]). Pasado un cierto tiempo, superior al anterior, se cancelan las sesiones abiertas con acceso remoto.* Consultar guías: ***Criterios de seguridad*** *Capítulo 13*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - A	☐ 2.- ¿Pasado un cierto tiempo, superior al anterior, se cancelan las sesiones abiertas desde dicho puesto de trabajo? *Evidencia: Pasado un cierto tiempo, superior al anterior, se cancelan las sesiones abiertas desde dicho puesto de trabajo.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.eq.3	*Protección de equipos portátiles*			

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Baja - D, A, I, C, T	☐ 1.- ¿Son protegidos adecuadamente los equipos que abandonen las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo? *Evidencia: Dispone de un procedimiento documentado que especifica las medidas de seguridad que deben cumplir los equipos que abandonen las instalaciones de la organización. Dicho procedimiento especifica la aplicación de lo previsto en [mp.si.5] al desmantelarlo. Los equipos portátiles deben cumplir lo establecido en [op.acc.5].* Respecto a los equipos portátiles: ☐ 1.1.- ¿Se lleva un inventario de los mismos junto con una identificación de la persona responsable del mismo? *Evidencia: Dispone de un procedimiento documentado de inventario de equipos portátiles que recoge la identificación de la persona responsable del mismo. Consultar dicho inventario.* ☐ 1.2.- ¿Se lleva un control regular de que está positivamente bajo su control? *Evidencia: Dicho procedimiento recoge la responsabilidad de revisar con la frecuencia definida la posesión de cada equipo portátil por la persona identificada en el inventario.* ☐ 1.3.- ¿Se ha establecido un canal de comunicación para informar, al servicio de gestión de incidencias, de pérdidas o sustracciones? *Evidencia: Dispone de un procedimiento documentado para la comunicación, al servicio de gestión de incidencias, de pérdidas o sustracciones, y el personal responsable de los equipos portátiles lo conoce.* ☐ 1.4.- ¿Se ha establecido un sistema de protección perimetral que minimice la visibilidad exterior y minimice las opciones de acceso al interior? *Evidencia: Dispone de un procedimiento documentado para protección de las conexiones de red (p.ej: un firewall personal).* ☐ 1.5.- ¿Se evita, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización? *Evidencia: Dispone de política o normativa documentada que prohíbe 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.* Consultar guías:	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Criterios de seguridad *Capítulo 13*		
	Alta - D, A, I, C, T	☐ 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? *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.* ☐ 1.7.- ¿Se protege la información de nivel alto almacenada en el disco mediante cifrado? *Evidencia: Dispone de medios criptográficos (relacionados con [mp.si.2] para la protección de la información almacenada.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.eq.9	*Medios alternativos*			
	Media - D	☐ 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos de tratamiento de la información en caso de indisponibilidad de los medios habituales? *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.* Respecto a dichos medios alternativos: ☐ 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales? *Evidencia: Los medios alternativos está sometidos a las mismas garantías de seguridad que los habituales.* ☐ 1.2.- ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento? *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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Consultar guías: ***Criterios de seguridad*** *Capítulos 8 y 12*		
mp.com	*PROTECCIÓN DE LAS COMUNICACIONES*			
mp.com.1	*Perímetro seguro*			
	Baja - D, A, I, C, T	☐ 1.- ¿Dispone de cortafuegos que separe la red interna del exterior? *Evidencia: Dispone de una política o normativa documentada que especifica que la red interna está separada del exterior mediante un cortafuegos. 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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 14* ***CCN-STIC-408*** *Seguridad perimetral (cortafuegos)* ***CCN-STIC-419*** *Configuración segura con IPtables* ***CCN-STIC-507*** *Guía de seguridad para Microsoft ISA Server* ***CCN-STIC-641*** *Seguridad en equipos de comunicaciones routers Cisco*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	Respecto a dicho cortafuegos: ☐ 1.1.- ¿Consta de dos o más equipos de diferente fabricante dispuestos en cascada? *Evidencia: Dicha política o normativa indica que se cuenta con dos o más equipos de diferente fabricante dispuestos en cascada. Ver los firewalls y el esquema de red.* ☐ 1.2.- ¿Consta de sistemas redundantes? *Evidencia: Dicha política o normativa indica que los firewalls deben ser redundantes. Ver los firewalls.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.com.2	*Protección de la confidencialidad*			
	Media - C	☐ 1.- ¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad? *Evidencia: Dispone de una política o normativa documentada que indica que 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]. Dispone de un inventario de conexiones que discurren por redes fuera del propio dominio de seguridad. Consultar el mecanismo VPN utilizado.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Respecto a esas VPN: ☐ 1.1.- ¿Emplean algoritmos acreditados por el CCN? *Evidencia: Los algoritmos criptográficos han sido acreditados por el CCN.* Consultar guías: ***Criterios de seguridad*** *Capítulos 10 y 14* ***CCN-STIC-416*** *Seguridad de redes privadas virtuales*		
	Alta - C	☐ 1.2.- ¿Se emplean preferentemente dispositivos hardware en el establecimiento y utilización de la VPN? *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 utilización de dispositivos hardware se encuentra debidamente acreditado y aprobado por el responsable.* ☐ 1.3.- ¿Se emplean preferentemente productos certificados? *Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). En caso de utilización de productos no certificados se encuentra debidamente acreditado y aprobado por el responsable.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.com.3	*Protección de la autenticidad y de la integridad*			
	Baja - A, I	☐ 1.- ¿Se asegura la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna? *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]).* ☐ 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? *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 si se emplea una VPN.* Consultar guías: ***Criterios de seguridad*** *Capítulo 14* ***CCN-STIC-416*** *Seguridad de redes privadas virtuales*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - A, I	☐ 3.- ¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad?	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dispone de una política o normativa documentada que indica que 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]. Dispone de un inventario de conexiones que discurren por redes fuera del propio dominio de seguridad. Consultar el mecanismo VPN utilizado. Respecto a esas VPN: ☐ 3.1.- ¿Emplean algoritmos acreditados por el CCN? *Evidencia: Los algoritmos criptográficos han sido acreditados por el CCN.*	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
	Alta - A, I	☐ 3.2.- ¿Se emplean preferentemente dispositivos hardware en el establecimiento y utilización de la VPN? *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 utilización de dispositivos hardware se encuentra debidamente acreditado y aprobado por el responsable.* ☐ 3.3.- ¿Se emplean preferentemente productos certificados? *Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). En caso de utilización de productos no certificados se encuentra debidamente acreditado y aprobado por el responsable.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.com.4	*Segregación de redes*			
	Alta - A, I, C, T	☐ 1.- ¿Se encuentra la red segmentada? *Evidencia: Dispone de una política o normativa documentada que especifica que la red se encuentra 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.* Respecto a dichos segmentos: ☐ 1.1.- ¿Existe control de entrada de los usuarios que llegan a cada segmento? *Evidencia: Dispone de control de entrada de los usuarios que llegan a cada segmento.* ☐ 1.2.- ¿Existe control de salida de la información disponible en cada segmento?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dispone de control de salida de la información disponible en cada segmento. ☐ 1.3.- ¿Está el punto de interconexión particularmente asegurado, mantenido y monitorizado? *Evidencia: Dispone de un procedimiento documentado para la securización, mantenimiento y monitorización del punto de interconexión entre segmentos.* Consultar guías: ***Criterios de seguridad*** *Capítulo 14* ***CCN-STIC-408*** *Seguridad perimetral (cortafuegos)* ***CCN-STIC-419*** *Configuración segura con IPtables* ***CCN-STIC-641*** *Seguridad en equipos de comunicaciones routers Cisco*		
mp.com.9	*Medios alternativos*			
	Alta - A, I, C, T	☐ 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos de comunicación en caso de indisponibilidad de los medios habituales? *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.* Respecto a dichos medios alternativos: ☐ 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales? *Evidencia: Los medios alternativos está sometidos a las mismas garantías de seguridad que los habituales.* ☐ 1.2.- ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento? *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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.si	*PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN*			
mp.si.1	*Etiquetado*			

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	Baja - C	☐ 1.- ¿Se encuentran etiquetados los soportes de información? *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. Consultar si los soportes tienen el etiquetado correspondiente.* Respecto a dicho etiquetado: ☐ 1.1.- ¿Revela el contenido? *Evidencia: Dicho procedimiento especifica que el etiquetado no debe revelar el contenido.* ☐ 1.2.- ¿Indica el nivel de seguridad de la información contenida de mayor calificación? *Evidencia: Dicho procedimiento especifica que el etiquetado debe indicar el nivel de seguridad de la información contenida de mayor calificación, pero de forma que no sea comprensible para alguien ajeno al sistema.* ☐ 1.3.- ¿Pueden los usuarios entender el significado de las etiquetas, bien mediante simple inspección, bien mediante recurriendo a un repositorio que lo explique? *Evidencia: Dicho procedimiento especifica cómo etiquetar los soportes y cómo leer la etiqueta. Esta información forma parte del plan de formación [mp.per.4], con lo que conocen y aplican además los procedimientos asociados a cada nivel de información.* Consultar guías: ***Criterios de seguridad*** *Capítulos 6 y 16*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.si.2	*Criptografía*			
	Media - I, C	☐ 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? *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]).* Consultar guías: ***Criterios de seguridad*** *Capítulos 10, 13 y 16* ***CCN-STIC-955*** *Recomendaciones empleo GnuPG v1.4.7*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta -	Respecto a dichos mecanismos criptográficos:	Aplica:	Registros:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
	I, C	☐ 1.1.- ¿Emplean algoritmos acreditados por el CCN? *Evidencia: Los algoritmos criptográficos han sido acreditados por el CCN.* ☐ 1.2.- ¿Se emplean preferentemente productos certificados? *Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). En caso de utilización de productos no certificados se encuentra debidamente acreditado y aprobado por el responsable.*	☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.si.3	*Custodia*			
	Baja - D, A, I, C, T	☐ 1.- ¿Se aplica la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización? *Evidencia: Dispone de un procedimiento documentado para el control de los soportes de información. Dispone de un inventario de todos los soportes de información en uso, indicando su etiqueta, contenido actual, ubicación física y quién es el responsable del mismo. Consultar el inventario.* Respecto a dicho control: ☐ 1.1.- ¿Garantiza el control de acceso con medidas físicas, lógicas o ambas? *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.* ☐ 1.2.- ¿Garantiza que se respeten las exigencias de mantenimiento del fabricante, en especial en lo referente a temperatura, humedad y otros agresores medioambientales? *Evidencia: Dicho procedimiento identifica las exigencias de mantenimiento del fabricante y las aplica (relacionado con [mp.if.3]).* Consultar guías: ***Criterios de seguridad** Capítulo 16*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - D, A, I, C, T	☐ 1.3.- ¿Conserva la historia de cada dispositivo? *Evidencia: Dicho procedimiento establece las actividades para mantener la historia de cada dispositivo, desde su primer uso hasta la terminación de su vida útil y/o destrucción del mismo.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
mp.si.4	*Transporte*			
	Baja - D, A, I, C, T	☐ 1.- ¿Dispone de un registro de salida que identifica al transportista que recibe el soporte para su traslado? *Evidencia: Dispone de un registro de transportistas autorizados. Dispone de un procedimiento documentado que registra cada salida de un soporte de las instalaciones de la organización. Dicho registro almacena tanto la etiqueta como el transportista encargado de su traslado. Consultar los registros.* ☐ 2.- ¿Dispone de un registro de entrada que identifica al transportista que lo entrega? *Evidencia: Dispone de un procedimiento documentado que registra cada llegada de un soporte a las instalaciones de la organización. Dicho registro almacena tanto la etiqueta como el transportista encargado de su traslado. Consultar los registros.* ☐ 3.- ¿Dispone de un procedimiento rutinario que coteja las salidas con las llegadas y levanta las alarmas pertinentes cuando se detecte algún incidente? *Evidencia: Dispone de un procedimiento documentado que coteja los registros las salidas con las llegadas y levanta las alarmas pertinentes cuando se detecte algún incidente. Consultar resultados de los análisis.* ☐ 4.- ¿Utiliza medios de protección criptográfica correspondientes al nivel de calificación de la información contenida de mayor nivel? *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.* Respecto a dicha protección criptográfica: ☐ 4.1.- ¿Gestiona las claves de forma segura? *Evidencia: Las claves se gestionan conforme a lo especificado en [op.exp.11].* Consultar guías: ***Criterios de seguridad** Capítulo 16*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.si.5	*Borrado y destrucción*			
	Media - C	☐ 1.- ¿Los soportes, sean o no electrónicos, que vayan a ser reutilizados para otra información o liberados a otra organización, son borrados de	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		forma segura? *Evidencia: Dispone de un procedimiento documentado que especifica el método de borrado seguro de los soportes (discos de equipos portátiles en línea con [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.).* ☐ 2.- ¿Se destruyen de forma segura los soportes cuando la naturaleza del soporte no permita un borrado seguro? *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 para constatar cuáles han sido eliminados.* ☐ 3.- ¿Se destruyen de forma segura los soportes según el tipo de la información contenida? *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.* ☐ 4.- ¿Se emplean preferentemente productos certificados? *Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). En caso de utilización de productos no certificados se encuentra debidamente acreditado y aprobado por el responsable.* Consultar guías: ***Criterios de seguridad*** *Capítulo 9* ***CCN-STIC-400*** *Manual de seguridad de las TIC* ***CCN-STIC-403*** *Herramientas de seguridad* ***CCN-STIC-404*** *Control de soportes informáticos*	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
mp.sw	*PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS*			
mp.sw.1	*Desarrollo de aplicaciones*			
	Media - D, A, I, C, T	☐ 1.- ¿Se desarrollan aplicaciones sobre un sistema diferente y separado del de producción? *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*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		servidores se utilizan para desarrollo. ☐ 2.- ¿Existen herramientas o datos de desarrollo en el entorno de producción? *Evidencia: Dicha política o normativa establece que en el entorno de producción no pueden existir herramientas o datos de desarrollo.* ☐ 3.- ¿Aplica una metodología de desarrollo reconocida? *Evidencia: Dispone de una política o normativa documentada que indica el uso de una metodología de desarrollo conocida (p.ej: METRICA).* Respecto a dicha metodología de desarrollo: ☐ 3.1.- ¿Toma en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida? *Evidencia: Dicha metodología de desarrollo toma en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.* ☐ 3.2.- ¿Trata específicamente los datos usados en pruebas? *Evidencia: Dicha metodología de desarrollo trata específicamente los datos usados en pruebas.* ☐ 3.3.- ¿Permite la inspección del código fuente? *Evidencia: Dicha metodología de desarrollo permite la inspección del código fuente.* ☐ 4.- ¿Los mecanismos de identificación y autenticación son parte integral del diseño del sistema? *Evidencia: Dispone de una política o normativa documentada respecto al diseño de un sistema que contempla los mecanismos de identificación y autenticación.* ☐ 4.1.- ¿Y los mecanismos de protección de la información tratada? *Evidencia: Dicha política o normativa respecto al diseño contempla los mecanismos de protección de la información tratada.* ☐ 4.2.- ¿Y la generación y tratamiento de pistas de auditoría? *Evidencia: Dicha política o normativa respecto al diseño contempla la generación y tratamiento de pistas de auditoría. Consultar el diseño de un desarrollo.*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 5.- ¿Se realizan las pruebas anteriores a la implantación o modificación de los sistemas de información con datos reales? *Evidencia: Dispone de una política o normativa documentada que indica que las pruebas se realizan con datos ficticios, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente.* Consultar guías: ***Criterios de seguridad*** *Capítulo 17* ***METRICA v3*** ***CCN-STIC-205*** *Actividades seguridad ciclo vida CIS*		
	Alta - D, A, I, C, T	☐ 6.- ¿Aplica un procedimiento de inspección de código? *Evidencia: Dispone de un procedimiento documentado para la inspección del código desarrollado. Consultar un informe de inspección de código.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.sw.2	*Aceptación y puesta en servicio*			
	Baja - D, A, I, C, T	☐ 1.- ¿Dispone de un plan de pruebas antes de pasar a producción para comprobar el correcto funcionamiento de la aplicación? *Evidencia: Dispone de un procedimiento documentado para la elaboración y ejecución de un plan de pruebas de una aplicación.* Respecto a dichas pruebas: ☐ 1.1.- ¿Comprueba que se cumplen los criterios de aceptación en materia de seguridad? *Evidencia: Dicho plan contempla pruebas de aceptación en materia de seguridad.* ☐ 1.2.- ¿Comprueba que no se deteriora la seguridad de otros componentes del servicio? *Evidencia: Dicho plan contempla pruebas para constatar que no se deteriora la seguridad de otros componentes del servicio.* ☐ 1.3.- ¿Se realizan en un entorno aislado? *Evidencia: Dicho plan contempla que las pruebas se realizan en un entorno aislado (pre-producción).* ☐ 1.4.- ¿Utilizan datos reales?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dicho plan contempla que las no utilizan datos reales, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente. Consultar guías: ***METRICA v3***		
	Media - D, A, I, C, T	☐ 2.- ¿Previamente a la entrada en servicio, se le realiza un análisis de vulnerabilidades? *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.* ☐ 2.1.- ¿Y se le realiza una prueba de penetración? *Evidencia: Dicho plan contempla la ejecución de una prueba de penetración.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Alta - D, A, I, C, T	☐ 2.2.- ¿Y un análisis de coherencia en la integración en los procesos? *Evidencia: Dicho plan contempla la ejecución de un análisis de coherencia en la integración en los procesos.* ☐ 2.3.- ¿Y se considera la oportunidad de realizar una auditoría de código fuente? *Evidencia: Dicho plan contempla la oportunidad de realizar una auditoría de código fuente.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.info	*PROTECCIÓN DE LA INFORMACIÓN*			
mp.info.1	*Datos de carácter personal*			
	Baja - D, A, I, C, T	☐ 1.- ¿Se ha identificado si el sistema trata datos de carácter personal? *Evidencia: Dispone de un procedimiento documentado para identificar si el sistema trata datos de carácter personal.* ☐ 2.- En caso de tratar datos de carácter personal ¿se aplica la normativa vigente? *Evidencia: Se ha publicado la inscripción de ficheros con datos de carácter personal en un boletín oficial, se han inscrito en la Agencia Española de Protección de Datos, dispone del Documento de Seguridad y se aplican las medidas en él descritas (derivadas del nivel correspondiente indicado en el R.D. 1720/2007).* Consultar guías: ***Criterios de seguridad*** *Capítulos en los que se hace referencia a la LOPD* ***Ley Orgánica 15/1999****, de 13 de diciembre, de Protección de Datos de Carácter Personal*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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*		
mp.info.2	*Calificación de la información*			
	Baja - C	☐ 1.- ¿Se califica la información conforme a lo establecido legalmente sobre la naturaleza de la misma? *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 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 re-calificaciones posteriores. Consultar si la información impresa o disponible en las aplicaciones recogen su calificación.* ☐ 2.- ¿Establece la política de seguridad quién es el responsable de cada información manejada por el sistema? *Evidencia: Dispone de una política de seguridad documentada que especifica quién es el responsable de cada información manejada por el sistema.* ☐ 3.- ¿Recoge la política de seguridad, directa o indirectamente, los criterios que en la organización determinan el nivel de seguridad requerido? *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.* ☐ 4.- ¿El responsable de cada información sigue los criterios determinados en la política de seguridad para asignar a cada información el nivel de seguridad requerido y es responsable de su documentación y aprobación formal? *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.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 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? *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.* Consultar guías: ***Criterios de seguridad** Capítulo 6*		
	Media - C	☐ 6.- ¿Existen procedimientos que describan en detalle la forma en que se ha de etiquetar y tratar la información? *Evidencia: Dispone de un procedimiento documentado que describe la forma en que se ha de etiquetar y tratar la información, en función del nivel de seguridad que se requiere.* Respecto a dicho tratamiento de la información: ☐ 6.1.- ¿Contempla su control de acceso? *Evidencia: Cumple [op.acc].* ☐ 6.2.- ¿Contempla su almacenamiento? *Evidencia: Cumple [mp.si.3] y [mp.si.2].* ☐ 6.3.- ¿Contempla la realización de copias? *Evidencia: Cumple [mp.info.9].* ☐ 6.4.- ¿Contempla el etiquetado de soportes? *Evidencia: Cumple [mp.si.1].* ☐ 6.5.- ¿Contempla su transmisión telemática? *Evidencia: Cumple [mp.com].* ☐ 6.6.- ¿Y contempla cualquier otra actividad relacionada con dicha información? *Evidencia: Consultar qué otra actividad relacionada con la información realiza la organización, y si esta se realiza conforme a una política, normativa y procedimientos documentados, aprobados y revisados.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.info.3	*Cifrado*			
	Alta - C	☐ 1.- ¿Se cifra la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión?	Aplica: ☐ Sí ☐ No	Registros: ☐ Documento:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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, TrueCrypt, VPN IPSec, etc.) y la información está, efectivamente, cifrada. ☐ 2.- ¿Permanece sólo en claro la información con un nivel alto en confidencialidad mientras se está haciendo uso de ella? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulos 10 y 13* ***CCN-STIC-955*** *Recomendaciones empleo GnuPG v1.4.7*	Lo audito: ☐ Sí ☐ No	☐ Muestreo: Observaciones auditoría:
mp.info.4	*Firma electrónica*			
	Baja - A, I	☐ 1.- ¿Dispone de una Política de Firma Electrónica aprobada por el órgano superior competente que corresponda? *Evidencia: Dispone de una Política de Firma Electrónica aprobada por el órgano superior competente que corresponda, y se cumple [op.exp.11].* ☐ 2.- ¿Se firman electrónicamente los documentos que requieren capacidad probatoria según la ley de procedimiento administrativo? *Evidencia: Dispone de un procedimiento documentado para identificar los documentos que requieren capacidad probatoria según la ley de procedimiento administrativo. Estos documentos se firman electrónicamente.* Consultar guías: ***Criterios de seguridad*** *Capítulo 15* ***CCN-STIC-405*** *Algoritmos y parámetros de firma electrónica*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
	Media - A, I	☐ 3.- ¿Se emplean algoritmos acreditados por el CCN? *Evidencia: Los algoritmos criptográficos han sido acreditados por el CCN.* ☐ 4.- ¿Se emplean preferentemente certificados reconocidos?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados reconocidos. En caso de utilización de certificados no reconocidos se encuentra debidamente acreditado y aprobado por el responsable. ☐ 5.- ¿Se emplean preferentemente dispositivos seguros de firma? *Evidencia: Dispone de una política o normativa documentada que indica el uso de dispositivos seguros de firma. En caso de utilización de dispositivos no considerados seguros de firma se encuentra debidamente acreditado y aprobado por el responsable.* ☐ 6.- ¿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? *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.* Respecto a la verificación y validación de la firma electrónica: ☐ 6.1.- ¿Se adjunta a la firma, o se referencia, el certificado? *Evidencia: Dispone de un procedimiento documentado que contempla adjuntar o referenciar en la firma el certificado.* ☐ 6.2.- ¿Se adjunta a la firma, o se referencia, los datos de verificación y validación? *Evidencia: Dicho procedimiento contempla adjuntar o referenciar en la firma los datos de verificación y validación.* ☐ 6.3.- ¿Se protegen la firma, el certificado y los datos de verificación y validación con un sello de tiempo? *Evidencia: Dicho procedimiento contempla acompañar la firma, el certificado y los datos de verificación y validación con un sello de tiempo.* ☐ 6.4.- ¿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?		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		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. ☐ 6.5.- ¿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? *Evidencia: Dicho procedimiento contempla el certificado, los datos de verificación y validación, y el sello de tiempo.*		
	Alta - A, I	☐ 7.- ¿Se emplean preferentemente certificados reconocidos? *Evidencia: Dispone de una política o normativa documentada que indica el uso de certificados reconocidos. En caso de utilización de certificados no reconocidos se encuentra debidamente acreditado y aprobado por el responsable.* ☐ 8.- ¿Se emplean dispositivos seguros de creación de firma? *Evidencia: Dispone de una política o normativa documentada que indica el uso de dispositivos seguros de creación de firma.* ☐ 9.- ¿Se emplean preferentemente productos certificados? *Evidencia: Dispone de una política o normativa documentada que indica el uso de productos certificados (en relación con [op.pl.5]). En caso de utilización de productos no certificados se encuentra debidamente acreditado y aprobado por el responsable.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.info.5	*Sellos de tiempo*			
	Alta - T	☐ 1.- ¿Se aplican sellos de tiempo (fechado electrónico) a aquella información que sea susceptible de ser utilizada como evidencia en el futuro? *Evidencia: Dispone de un procedimiento documentado para identificar y establecer el tiempo de retención de la información 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.* ☐ 2.- ¿Los datos pertinentes para la verificación posterior de la fecha son	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad? *Evidencia: Dispone de un procedimiento documentado para el tratamiento de los datos pertinentes para la verificación posterior de la fecha son con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.* ☐ 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? *Evidencia: Dispone de un procedimiento documentado para el 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.* Consultar guías: ***Criterios de seguridad*** *Capítulos 11 y 15*		
mp.info.6	*Limpieza de documentos*			
	Baja - C	☐ 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? *Evidencia: Dispone de un procedimiento documentado que identifica el destino del documento y, si va a ser transferidos a otro dominio de seguridad o publicado electrónicamente, indica cómo limpiar el documento. Dispone de herramientas evaluadas para limpiar los documentos.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.info.9	*Copias de seguridad (backup)*			
	Media - D	☐ 1.- ¿Realizan copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada? *Evidencia: Dispone de un procedimiento documentado por el que el responsable de la información determina la frecuencia con la que deben realizarse las copias y el periodo de retención durante el que mantenerlas.*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Dispone de un procedimiento documentado para la realización y eliminación de los backups. Dispone de un plan para realizar regularmente el backup. 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 los backups. Respecto a dichas copias de seguridad: ☐ 1.1.- ¿Abarcan la información de trabajo de la organización? *Evidencia: Dicho procedimiento contempla que todos los responsables de la información de la organización determinen su necesidad de copias de seguridad.* ☐ 1.2.- ¿Abarcan las aplicaciones en explotación, incluyendo los sistemas operativos? *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], [op.exp.4] y [op.exp.5].* ☐ 1.3.- ¿Abarcan los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga? *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], [op.exp.2], [op.exp.3], [op.exp.4] y [op.exp.5].* ☐ 1.4.- ¿Abarcan las claves utilizadas para preservar la confidencialidad de la información? *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] y [mp.info.3].* ☐ 1.5.- ¿Disfrutan de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad? *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 trazabilidad, tanto en su acceso, almacenamiento como transporte. Este procedimiento está ligado a [op.acc], [op.exp.9] y [op.exp.10] y, en caso de utilizar cifrado, con [op.exp.11].*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 1.6.- ¿Existe un proceso de autorización para la recuperación de información de las copias de seguridad? *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.* ☐ 1.7.- ¿Se verifica regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad? *Evidencia: Dispone de un procedimiento documentado para la realización de pruebas de restauración del backup, que mantienen los requisitos de seguridad establecidos para la información original restaurada. Dispone de un plan de pruebas de respaldo que cubre, a lo largo del tiempo, todos los ámbitos de los que se realizan backups.* ☐ 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? *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.* Consultar guías: ***Criterios de seguridad*** *Capítulo 16*		
mp.s	*PROTECCIÓN DE LOS SERVICIOS*			
mp.s.1	*Protección del correo electrónico (e-mail)*			
	Baja - D, A, I, C, T	☐ 1.- ¿La información que se distribuye por medio de correo electrónico se protege, tanto en el cuerpo de los mensajes como en los anexos? *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 se protege, tanto en el cuerpo de los mensajes*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		como en los anexos (relacionado con [mp.info.6]). ☐ 2.- ¿Se protege la información de encaminamiento de mensajes y establecimiento de conexiones? *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).* ☐ 3.- ¿Se protege a la organización frente a problemas que se materializan por medio del correo electrónico, como del correo no solicitado (spam)? *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).* Respecto a la protección frente a problemas por el e-mail: ☐ 3.1.- ¿Se protege frente a programas dañinos (virus, gusanos, troyanos, espías u otros de naturaleza análoga)? *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).* Respecto a la protección frente a problemas por el e-mail: ☐ 3.2.- ¿Se protege frente a código móvil de tipo “applet”? *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).* ☐ 4.- ¿Se han establecido normas de uso del correo electrónico? *Evidencia: Dispone de una normativa documentada que especifica el uso correcto y autorizado del correo electrónico.*		Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Respecto a dicha norma de uso del e-mail: ☐ 4.1.- ¿Contempla limitaciones al uso como soporte de comunicaciones privadas? *Evidencia: Dicha normativa especifica las limitaciones al uso como soporte de comunicaciones privadas.* ☐ 4.2.- ¿Se llevan a cabo actividades de concienciación y formación relativas al uso del correo electrónico? *Evidencia: Dispone de plan de formación y concienciación que cubre el uso del correo electrónico (relacionado con [mp.per.3] y [mp.per.4]).* ☐ 5.- ¿Se protege la disponibilidad del correo electrónico? *Evidencia: Se ha estudiado la disponibilidad requerida del servicio de correo electrónico y se han establecido las medidas pertinentes de protección de los equipos, aplicaciones y líneas de comunicación que lo soportan.* Consultar guías: ***CCN-STIC-502*** *Navegador y correo electrónico* ***CCN-STIC-502B*** *Navegador y correo electrónico en Windows Vista* ***CCN-STIC-506*** *Seguridad en servidores Microsoft Exchange Server 2003* ***CCN-STIC-519A*** *Navegador y correo electrónico en Windows XP* ***CCN-STIC-681*** *Configuración segura de servidores de correo Postfix* ***CCN-STIC-682*** *Configuración segura de Sendmail*		
mp.s.2	*Protección de servicios y aplicaciones web*			
	Baja - D, A, I, C, T	☐ 1.- ¿Se encuentran protegidos los subsistemas dedicados a la publicación de información frente a las amenazas que les son propias? *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.* ☐ 2.- Cuando la información tenga algún tipo de control de acceso ¿se garantiza la imposibilidad de acceder a la información obviando la autenticación? *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).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Respecto a dicho control de acceso: ☐ 2.1.- ¿Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado? *Evidencia: Dispone de una política o normativa documentada 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).* ☐ 2.2.- ¿Se previenen ataques de manipulación de URL? *Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir ataques de manipulación de URL. El sistema aplica dicha política (p.ej: no es posible acceder a páginas que requieren haber visitado antes otras páginas en el proceso).* ☐ 2.3.- ¿Se previenen ataques de manipulación de las cookies de los usuarios? *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).* ☐ 2.4.- ¿Se previenen ataques de inyección de código? *Evidencia: Dicha política o normativa especifica el uso de 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.).* ☐ 3.- ¿Se previenen intentos de escalado de privilegios? *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.).* ☐ 4.- ¿Se previenen ataques de “cross site scripting”? *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.).*		

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		☐ 5.- ¿Se previenen ataques de manipulación de "proxys" o "cachés"? *Evidencia: Dicha política o normativa especifica el uso de mecanismos para impedir ataques de manipulación de "proxys" 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).* ☐ 6.- ¿Se limpian los documentos publicados? *Evidencia: Dispone de un procedimiento documentado para autorizar la publicación sólo de los documentos que han sido limpiados conforme a lo establecido en [mp.info.6]. Consultar algunos documentos publicados.* ☐ 7.- ¿Se realizan auditorías de seguridad y pruebas de penetración? *Evidencia: Se cumple [mp.sw.2].* Consultar guías: ***CCN-STIC-504*** *Configuración segura de Internet Information Services 6.0* ***CCN-STIC-671*** *Configuración segura de servidores web Apache* ***CCN-STIC-672*** *Guía de seguridad de Tomcat*		
mp.s.8	*Protección frente a la denegación de servicio*			
	Media - D	☐ 1.- ¿Se ha planificado y dotado al sistema de capacidad suficiente para atender a la carga prevista con holgura? *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]) y es suficiente.* ☐ 2.- ¿Se han desplegado tecnologías para prevenir los ataques conocidos de denegación de servicio (Denial of Service)? *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).* Consultar guías: ***CCN-STIC-412*** *Requisitos de seguridad de entornos y aplicaciones web* ***CCN-STIC-434*** *Herramientas para el análisis de ficheros de log* ***CCN-STIC-503A*** *Configuración segura Windows Server 2003 (controlador de dominio)* ***CCN-STIC-503B*** *Configuración segura Windows Server 2003 (servidor independiente)* ***CCN-STIC-641*** *Seguridad en equipos de comunicaciones routers Cisco*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		CCN-STIC-642 *Seguridad en equipos de comunicaciones switches Enterasys* ***CCN-STIC-671*** *Configuración segura de servidores web Apache* ***CCN-STIC-953*** *Recomendaciones empleo herramienta Snort*		
	Alta - D	☐ 3.- ¿Se ha establecido un sistema de detección de ataques de denegación de servicio? *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.).* ☐ 4.- ¿Se ha establecido un procedimiento de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones? *Evidencia: Dispone de un procedimiento documentado que indica el procedimiento de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.* ☐ 5.- ¿Se impide el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros? *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.).*	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:
mp.s.9	*Medios alternativos*			
	Alta - D	☐ 1.- ¿Está garantizada la existencia y disponibilidad de medios alternativos para prestar los servicios en caso de indisponibilidad de los medios habituales? *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.* Respecto a dichos medios alternativos: ☐ 1.1.- ¿Están sometidos a las mismas garantías de seguridad que los habituales?	Aplica: ☐ Sí ☐ No Lo audito: ☐ Sí ☐ No	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

BORRADOR

Aptdo.	Categoría - Dimensiones	Requisito	Aplicabilidad - Auditado	Comentarios
		Evidencia: Los medios alternativos está sometidos a las mismas garantías de seguridad que los habituales. ☐ 1.2.- ¿Se ha establecido un tiempo máximo para que los medios alternativos entren en funcionamiento? *Evidencia: Dicho procedimiento identifica el tiempo máximo para que los medios 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.*		

Firma: _____	Verificación del cumplimiento de las medidas del ENS
Auditor: _____	Fecha y hora de inicio: _____/_____/_____._____:_____ Fecha y hora de fin: _____/_____/_____._____:_____

BORRADOR

6. ANEXO I. DEFINICIÓN DE TÉRMINOS

Término	Descripción
CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
Firewall	Cortafuegos
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

BORRADOR

7. ANEXO II. PLANTILLA DE INFORME DE AUDITORÍA

14. Esta plantilla está diseñada para ser utilizada para la redacción del informe de auditoría del ENS requerido para los sistemas de categoría media y alta, no 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 dentro de lo previsto en el Artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y específicamente 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 en el ámbito de la Administración Electrónica.

BORRADOR

Cargo	Nombre completo	Firma	Fecha
Auditor Jefe			…../…../……..
Responsable de 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 3/2710 en los Capítulos II y III y en los Anexos I y II.

4. Alcance

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

[*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 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
- 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
- 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*]
- ……

8. Equipo auditor

El equipo auditor ha estado compuesto por:

- Auditor jefe: ……
- Auditor: ……..…… [*repetir por cuantos auditores haya habido*]

BORRADOR

- Experto: ……..…… [*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 …….)
- ……

BORRADOR

13. Resultado de la auditoría

[*Indicar:*

- *Datos, hechos y observaciones*
- *Deficiencias identificadas*
- *Riesgos que provocan las deficiencias*
- *Sugerencias (medidas correctoras o complementarias)*]

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

[*Indicar el grado de cumplimiento del ENS*]

Anexo I

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

Anexo II

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

BORRADOR