GPF-OCEX 5330 Revisión de los Controles Generales de Tecnologías de la Información

Anexo 4 Programa de auditoría (Fichas de revisión)

INSTRUCCIONES

Introducción

En esta GPF-OCEX 5330 aborda la revisión de los CGTI, procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.
No será posible concluir sobre la razonabilidad de las cuentas examinadas ni emitir una opinión de seguridad razonable sin haber revisado los CGTI salvo que se incurra en un riesgo global de auditoría muy elevado, no asumible desde un punto de vista técnico

Esta guía GPF-OCEX 5330, que incluye el subconjunto de controles de ciberseguridad considerados básicos (GPF-OCEX 5313), se ha realizado tomando como marco de refencia las medidas de control especificadas por el Esquema Nacional de Seguridad (ENS), pero considerando una taxonomía propia de controles generales de TI.

Finalidad

La finalidad de este programa de trabajo es ayudar a realizar y documentar la revisión de los controles generales de TI.

Alcance de la revisión

Dada la naturaleza del objeto material a revisar, los sistemas de información de un ente público, y su gran amplitud y diversidad hoy día, es necesario concretar qué sistemas se van a ser analizados y qué controles generales de TI son relevantes para la auditoría a realizar. En la planificación de cada trabajo de revisión de los controles generales de TI se completará la pestaña B de este fichero, donde se definirá el alcance concreto del trabajo de acuerdo con los objetivos fijados.

A la hora de seleccionar los sistemas a revisar podrán adoptarse distintos enfoques, dependiendo, fundamentalmente, de si la revisión de los controles generales de TI está enmarcada en el ámbito de una auditoría financiera, de un proceso en concreto o de una auditoría operativa o, por el contrario, se trata de una auditoría horizontal de controles generales de TI.

En el apartado 6 de la GPF-OCEX 5330 se señalan los criterios generales a seguir para determinar el alcance y los controles a analizar.

Para los distintos procesos de gestión seleccionados, la revisión debe incluir los controles adecuados en base al alcance descrito en la memoria de planificación de la auditoría, tipicamente controles relacionados con:

- la aplicación informática de gestión
- la base de datos subyacente
- los sistemas operativos instalados en cada uno de los sistemas que integren la aplicación de gestión (ej. servidor web, servidor de aplicación, servidor de base de datos)

Y para la muestra de los sistemas de información no específicos de un determinado proceso de gestión, sino que forman parte de la infraestructura TI general, que da servicio a todos los procesos de gestión de una entidad, se considerarán los siguientes tipos de elementos:

- controlador de dominio
- software de virtualización
- equipos de usuario
- elementos de la red de comunicaciones (ej. router, switches, punto de acceso a red wifi, etc.)
- elementos de seguridad (ej: firewall, IPS, proxy de correo, proxy de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Descripción de la estructura del Anexo 4 de la GPF-OCEX 5330

Este documento se estructura de la siguiente forma:

* **Pestaña "A) Instrucciones":** *Orientación sobre la estructura del presente programa y de cómo registrar los resultados de la revisión.*
* **Pestaña "B) Entorno y alcance"**:
El objetivo de esta es:
  * Recoger, a alto nivel, una descripción breve de los sistemas de información existentes en la Entidad (entorno tecnológico).
  * Los sistemas de información sobre los que se ha focalizado la revisión (alcance).

* **Pestañas de controles**: Hay una pestaña por cada uno de los controles incluidos en el programa de trabajo.
En cada una de estas pestañas se encuentra la siguiente información:
  * XY: Categoría y número del control junto con su descripción y el objetivo de control.
  * Subcontrol: Código y descripción del objetivo del subcontrol.
  * ENS: Código de la medida de seguridad del ENS equivalente. En caso de que no exista, se indica "No".
  * Descripción del control implantado en la Entidad: Donde se deberá describir las características específicas de cómo la entidad ha diseñado e implementado el subcontrol.
  * Pruebas a realizar y posibles evidencias a obtener: Descripción de la prueba a realizar y de las posibles evidencias a obtener.
  * Resultado de la Auditoría del ENS: Resultado de la evaluación del subcontrol según la auditoría del ENS (en caso de que la entidad disponga de ésta y de que el subcontrol cuente con una medida de seguridad equivalente en el ENS).
  * Resultado de la revisión: Columna a completar con el resultado de las pruebas realizadas y las evidencias analizadas.
  * Valoración del subcontrol: Valoración de la efectividad de cada subcontrol, de acuerdo a los criterios establecidos en la GPF-OCEX 5330 "Revisión de los controles generales de la TI en un entorno de administración electrónica".
  * Recomendación: Columna a completar en los casos en los que el subcontrol no sea efectivo y se considere oportuno realizar una recomendación.
  * Riesgo: Nivel de riesgo derivado de las deficiencias asociadas al subcontrol bajo análisis.
  * Coste de implementación de la recomendación: Estimación del coste.
  * Al final de cada una de las pestañas se incluye un campo para registrar la "Valoración global del control": Valoración de la madurez de cada control según se especifica en GPF-OCEX 5330.

* **Pestaña "D) Modelo de madurez":** Contiene los diferentes niveles considerados en el Modelo de Madurez para la evaluación global de los controles junto con una descripción de los mismos.

* **Pestaña "E) Valores Predefinidos":** Recoge los valores predefinidos para:
  * Concluir sobre el resultado de la evaluación de un subcontrol.
  * Valorar el Riesgo derivado de las deficiencias en los controles.
  * Cuantificar el Coste de implementación de las recomendaciones.

Descripción del trabajo a realizar

La revisión se realizará de la siguiente forma:

* En primer lugar, se completará la ficha o pestaña "B) Entorno tecnológico y alcance", describiendo brevemente los sistemas de información existentes en la Entidad e identificando el alcance de la revisisón.

* A continuación se rellenarán las fichas o pestañas de controles del Anexo 4.

Se cumplimentarán las pestañas de controles que recogen los resultados del trabajo realizado. En caso de revisiones cuyo alcance sea muy amplio, se puede optar por rellenar un fichero Excel para cada una de las aplicaciones/entornos incluidos en el alcance del trabajo.

* NOTA: Hay ciertos subcontroles que el ENS los exige para sistemas de categoría media y/o alta. La categoría de los sistemas se puede consultar en el documento "Declaración de Aplicabilidad" que haya realizado la entidad, que es una de las evidencias solicitadas para la evaluación del control CBCS8. En caso de que la entidad no esté adaptada al ENS y no disponga de dicha categorización, se considerará, como mínimo, los controles exigidos para nivel medio.

Criterios para la revisión de cada uno de los subcontroles que integran cada control:

a) Si la entidad SÍ dispone del informe de auditoría del ENS vigente (el ENS establece que las auditorías ordinarias deben realizarse, como mínimo, cada dos años) y el subcontrol tiene medida de seguridad equivalente en el ENS, entonces el cumplimiento será el reflejado en dicho informe, SIN QUE SE DEBA REALIZAR TRABAJO ADICIONAL, salvo que en la planificación se decida otra cosa, y se registrará en la columna "Resultado de Auditoría del ENS" (en estos casos, no habrá que completar la columna "Resultado de la revisión").

b) Si la entidad SÍ dispone del informe de auditoría del ENS pero el subcontrol NO tiene medida de seguridad equivalente en el ENS, se realizará una revisión ad-hoc de acuerdo a las pruebas indicadas en la columna "Pruebas a realizar y posibles evidencias a obtener". El resultado se documentará en la columna "Resultado de la revisión". En estos casos, la columna "Resultado según Auditoría ENS" aparece sombreada.

c) El procedimiento anterior también aplica en el caso de subcontroles que sí tienen medida de seguridad equivalente en el ENS pero para las que se ha incluido en el programa de trabajo la obligatoriedad de realizar pruebas complementarias. Éstas están identificadas como "Prueba complementaria para evaluar este control".

d) Si la entidad NO dispone del informe de auditoría del ENS, se realizará la evaluación ad-hoc de todos los subcontroles y se reflejará el resultado en la columna "Resultado de la revisión".

Criterios para la revisión de cada subcontrol (cuando no se parte del resultado del informe de auditoría del ENS):

* Descripción del control implantado en la Entidad: En primer lugar, se obtendrá conocimiento sobre cómo la Entidad ha implementado el subcontrol bajo análisis y éste se registrará en la columna destinada a tal efecto.

* Como se ha explicado anteriormente, el resultado de las pruebas realizadas se debe registrar en la columna "Resultado de la revisión".

* Asimismo, se debe evaluar y registrar por separado los resultados de los diferentes niveles (capa de aplicación, de base de datos y de sistema operativo), cuando el tipo de control lo exija (por ejemplo, los controles de acceso).

* Para documentar los resultados se han definido los siguientes apartados, que son los mismos que los utilizados en la guía "CCN-STIC-808 Anexo III Verificación del cumplimiento del ENS".

* **Documento:** Donde se indicará si la entidad dispone del procedimiento formalizado y si éste se considera adecuado.
* **Muestreo:** Donde se indicarán las pruebas realizadas para comprobar que el procedimiento está implantado y funcionando.
* **Observaciones:** En este apartado, se documentará cualquier aspecto adicional relacionado con las pruebas realizadas.

Cómo valorar los resultados del trabajo

Criterios para la evaluación de cada subcontrol:

* En función de los resultados de las pruebas realizadas, o bien de la información proporcionada en el informe de auditoría del ENS, se realizará la evaluación del subcontrol.

* La evaluación del subcontrol se registrará en la columna "Evaluación del subcontrol", estando los valores predefinidos. Estos pueden ser:
  - Control efectivo.
  - Control bastante efectivo.
  - Control poco efectivo.
  - Control no efectivo o no implantado.

Criterios para la valoración del riesgo:

* Se realizará una evaluación del riesgo asociado a los incumplimientos.

* Ésta se registrará en la columna "Riesgo", estando los valores predefinidos. Estos pueden ser:
  - Alto.
  - Medio.
  - Bajo.

Criterios para la evaluación global de cada control básico de ciberseguridad:

* En función de la eficacia de los distintos subcontroles, se realizará la evaluación del nivel de madurez de cada control.

* Ésta se registrará al final de cada ficha del Anexo 3 o pestaña de la hoja Excel, en el campo "Evaluación global del control CBCS x", estando los valores predefinidos. Estos pueden ser:
  - Inexistente.
  - Inicial / ad hoc.
  - Repetible, pero intuitivo.
  - Proceso definido.
  - Gestionado y medible.
  - Optimizado.

Descripción del entorno tecnológico y alcance

1. Descripción del entorno tecnológico

Describir brevemente el entorno tecnológico de la Entidad.
(Si se dispone de documentación relativa al mapa de red, la ubicación de los principales elementos de seguridad y sistemas de TI dentro de la red, etc. adjuntar en este punto).

2. Alcance

2.1.- Proceso/s de gestión seleccionado/s:

Proceso	Arquitectura
* Proceso 1	* Aplicación: *SAP* * SW Gestor de Base de Datos: *Oracle* * Sistema operativo: *RHEL 7*
* Proceso 2	* Aplicación: * SW Gestor de Base de Datos: * Sistema operativo:
* Proceso N	* Aplicación: * SW Gestor de Base de Datos: * Sistema operativo:

2.2.- Resto de elementos y componentes del entorno de TI:

Tipología	Elemento seleccionado
Controlador de dominio	*ejemplo.es*
Software de virtualización	*VMWare*
Equipos de usuario	*A0987654321 (Epinar) y B0987654321 (Asalom)*
Un elemento de la red de comunicaciones (ej. router, switches, punto de acceso a red wifi, etc.)	*rou01 (router de Internet)*
Un elemento de seguridad (ej: firewall, IPS, proxy de correo, proxy de navegación, etc.)	*Ironport01*

2.3.- Relación entre controles y elementos en los que se ha probado

Control	Elementos										
	Aplicación 1			Aplicación N			Controlador de dominio	Software de virtualización	Equipos de usuario	Elemento comunicaciones	Elemento seguridad
	Aplic.	BBDD	SO	Aplic.	BBDD	SO					
A1 - CBCS 8 Cumplimiento de Legalidad											
A2 Estrategia de Seguridad											
A3 Organización y Personal de TI											
A4 Marco Normativo y Procedimental de Seguridad											
B1 Adquisición de Aplicaciones y Sistemas											
B2 Desarrollo de Aplicaciones											
B3 Gestión de Cambios											
C1 - CBCS 1 Inventario y control de dispositivos físicos											
C1 - CBCS 2 Inventario y control de software autorizado											
C2 - CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades											
C3 - CBCS 5 Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores											
C4 - CBCS 6 Registro de la actividad de los usuarios (Mantenimiento, monitorización y análisis de los LOG de auditoría)											
C5 Servicios Externos											
C6 Protección Frente a Malware											

C7 Protección de Instalaciones e Infraestructuras											
C8 Gestión de Incidentes											
C9 Monitorización											
D1 - CBCS 4 Uso controlado de privilegios administrativos											
D2 Mecanismos de Identificación y Autenticación											
D3 Gestión de Derechos de Acceso											
D4 Gestión de Usuarios											
D5 Protección de Redes y Comunicaciones											
E1 - CBCS 7 Copia de seguridad de datos y sistemas											
E2 Plan de Continuidad											
E3 Alta Disponibilidad											

GPF-OCEX 5330 Revisión de los Controles Generales de Tecnologías de la Información

Anexo 4 Programa de auditoría (Fichas de revisión)

Resultado de la valoración global de los Controles Generales de Tecnologías de la Información

		Valoración global del control
A. Marco Organizativo	**A1 - CBCS 8 Cumplimiento de Legalidad**	0 - Inexistente.
	A2 Estrategia de Seguridad	0 - Inexistente.
	A3 Organización y Personal de TI	0 - Inexistente.
	A4 Marco Normativo y Procedimental de Seguridad	0 - Inexistente.
B. Gestión de Cambios en Aplicaciones y Sistemas	**B1 Adquisición de Aplicaciones y Sistemas**	0 - Inexistente.
	B2 Desarrollo de Aplicaciones	0 - Inexistente.
	B3 Gestión de Cambios	0 - Inexistente.
C. Operaciones de los Sistemas de Información	**C1 - CBCS 1 Inventario y control de dispositivos físicos**	0 - Inexistente.
	C1 - CBCS 2 Inventario y control de software autorizado	0 - Inexistente.
	C2 - CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	0 - Inexistente.
	C3 - CBCS 5 Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	0 - Inexistente.
	C4 - CBCS 6 Registro de la actividad de los usuarios (Mantenimiento, monitorización y análisis de los LOG de auditoría)	0 - Inexistente.
	C5 Servicios Externos	0 - Inexistente.
	C6 Protección Frente a Malware	0 - Inexistente.
	C7 Protección de Instalaciones e Infraestructuras	0 - Inexistente.
	C8 Gestión de Incidentes	0 - Inexistente.
	C9 Monitorización	0 - Inexistente.

D. Controles de Acceso a Datos y Programas	**D1 - CBCS 4 Uso controlado de privilegios administrativos**	0 - Inexistente.
	D2 Mecanismos de Identificación y Autenticación	0 - Inexistente.
	D3 Gestión de Derechos de Acceso	0 - Inexistente.
	D4 Gestión de Usuarios	0 - Inexistente.
	D5 Protección de Redes y Comunicaciones	0 - Inexistente.
E. Continuidad del Servicio	**E1 - CBCS 7 Copia de seguridad de datos y sistemas**	0 - Inexistente.
	E2 Plan de Continuidad	0 - Inexistente.
	E3 Alta Disponibilidad	0 - Inexistente.

Valoración general de los Controles Generales de TI	

A1 - CBCS 8 Cumplimiento de Legalidad

Objetivo de control: **La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 8-1: Cumplimiento del ENS La Entidad cumple con los requerimientos establecidos en el ENS.	org.1		***Política de seguridad y responsabilidades respecto al ENS*** 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 genéricos y la misión 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, L39/2015, L40/2015, RD 3/2010, etc.) así como las distintas regulaciones que pudieran existir (ámbito europeo, local, etc.) (Por ejemplo: en un anexo incluir el listado de legislación aplicable). 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 (STIC), responsable del sistema (TIC), administradores, operadores, usuarios, equipo de respuesta ante incidentes, etc.), sus deberes (velar por el cumplimiento de la normativa, estar al tanto de los cambios de la tecnología, realizar el análisis de riesgos, etc.) y el procedimiento para su designación y renovación (cada cuánto se renueva, por qué motivos, quién lo designa, etc.). 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 criterio para la calificación de la documentación, el procedimiento para su calificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse, etc. 1.7.- ¿La política de seguridad incluye una referencia a la legislación aplicable en materia de tratamiento de datos de carácter personal y existe coherencia entre dicha política y la documentación exigida por tal legislación específica? Evidencia: Dentro de la política se incluye referencia a la legislación aplicable en materia de tratamiento de datos de carácter personal y existe coherencia entre dicha política y la documentación que exige la mencionada legislación sobre tratamiento de datos personales. Cuando el sistema auditado tenga por objeto el tratamiento de datos personales se tendrá en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.		☐ Documento: ☐ Muestreo: Observaciones:				
	Art. 27.4		***Declaración de aplicabilidad del ENS*** Tal y como se exige en el punto 2.3 del Anexo II del ENS, verificar que: * La Entidad ha formalizado un documento con la declaración de aplicabilidad, que recoge las medidas de seguridad que son de aplicación en función del nivel y categoría del sistema. * La declaración de aplicabilidad ha sido firmada por el responsable de seguridad.		☐ Documento: ☐ Muestreo: Observaciones:				
	Art.34		***Informe de Auditoría del ENS*** 1.- Verificar que la entidad ha realizado la preceptiva auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta. 1.1.- Comprobar que la periodicidad de realización, es como mínimo, bienal para la auditoría ordinaria. 1.2.- Si se han producido modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas, verificar que se ha realizado con carácter extraordinario la correspondiente auditoría. Evidencia: Solicitar el informe de auditoría. 1.3.- Constatar que los informes de auditoría han sido analizados por el responsable de seguridad y que éste ha presentado sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas. Evidencia: Solicitar posibles convocatorias, orden del día y/o acta de reunión donde se presenten los resultados. 1.4.- Contrastar que la empresa de certificación que ha realizado la auditoría es una empresa acreditada. Evidencia: Consultar el listado actualizado de las empresas certificadas (https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion). 2.- Para los sistemas de categoría Básica, verificar que se ha realizado una autoevaluación (ésta puede ser realizada por el mismo personal que administra el sistema de información, o en quien éste delegue). 2.1.- Comprobar que la periodicidad de realización, es como mínimo, bienal. Evidencia: Solicitar el informe resultado de la autoevaluación (éste debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior). 2.2.- Constatar que los informes de autoevaluación han sido analizados por el responsable de seguridad y que éste ha elevado las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.		☐ Documento: ☐ Muestreo: Observaciones:				
	Art.35		***Informe del estado de la seguridad*** 1.- ¿Cumplimenta la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad regulada por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas? Evidencia: Dispone de acceso a la herramienta INES del portal del CCN y cuenta con una copia del informe individual generado en la última campaña. Dicho informe se encuentra en forma impresa o guardado en formato electrónico.		☐ Documento: ☐ Muestreo: Observaciones:				

A1 - CBCS 8 Cumplimiento de Legalidad

Objetivo de control: **La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
	Art.41		***Publicación del cumplimiento del ENS*** Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad. 1.- Comprobar que la entidad ha determinado la conformidad respecto al ENS de acuerdo a lo establecido en el propio ENS (es decir, para sistemas de categoría Básica --> Mediante autoevaluación o auditoría, y para sistemas de categoría Media y Alta mediante auditoría). Evidencia: Ver resultado del control 8.1-Art.34 2.- Comprobar que le entidad ha publicado en su sede electrónica la declaraciones de conformidad y los distintivos de seguridad correspondientes. Evidencia: Captura de pantalla de la sede electrónica en la que se observen las declaraciones y distintivos.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 8-2: Cumplimiento de la LOPD/RGPD La Entidad cumple con los requerimientos establecidos en la LOPD/RGPD	No		***Delegado de Protección de Datos (DPD) (Art. 37, 38 y 39)*** 1.- Verificar que se ha designado el DPD exigido por el RGPD en su Artículo 37. Evidencia: Documento formalizado del nombramiento del DPD. 2.- Constatar que el responsable o el encargado del tratamiento han publicado los datos de contacto del DPD y los han comunicado a la autoridad de control. Evidencia: Registros correspondientes a la comunicación a la AEPD y a la publicación. 3.- Comprobar que la posición del DPD le permite cumplir sus funciones según lo establecido en el RGPD y que éste rinde cuentas directamente al más alto nivel jerárquico del responsable o encargado. Evidencia: Organigrama en el que se identifique la posición del DPD. Actas u otros registros utilizados para el reporte del DPD al responsable o encargado.		☐ Documento: ☐ Muestreo: Observaciones:				
			Registro de actividades de tratamiento (Artículo 30) 1.- Verificar que la entidad dispone del registro de actividades de tratamiento con la información requerida por el RGPD. Es decir: a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de las categorías de interesados y de las categorías de datos personales; d)las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; e)en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas; f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1. Evidencia: Registro de actividades de tratamiento. *NOTA: La obligación anterior no aplicará a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.*		☐ Documento: ☐ Muestreo: Observaciones:				
			Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (para los de riesgo alto) (Art. 32.2 y 35) 1.- Verificar que la entidad ha realizado un análisis de riesgos de los tratamientos de datos personales bajo su responsabilidad, conforme a los requisitos (75), (76), (77) y (83) del RGPD. Evidencia: Registro de los análisis de riesgo realizados. Consultar https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf 2.- Verificar que la entidad ha realizado una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, conforme a lo establecido en el requisito (84), cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo. La evaluación de impacto debe incluir: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. Evidencia: Documentación de las evaluaciones de impacto.		☐ Documento: ☐ Muestreo: Observaciones:				
			Informe de auditoría de cumplimiento Aclaración: La realización de auditorías NO es un requisito explícito y obligatorio del RGPD. Éste indica que (Art. 32.1) que: *"... el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:* *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento."* 1.- Verificar si la entidad dispone de un informe de auditoría conforme al requisito anterior. En caso contrario, identificar el proceso establecido para dar cumplimiento al requisito anterior. Evidencia: Informe de auditoría o equivalente.		☐ Documento: ☐ Muestreo: Observaciones:				

A1 - CBCS 8 Cumplimiento de Legalidad

Objetivo de control: **La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 8-3: Cumplimiento de la Ley 25/2013, de 27 de diciembre (Impulso de la factura electrónica y creación del registro contable de facturas) La Entidad cumple con los requerimientos establecidos en la Ley 25/2013, de 27 de diciembre.	No		***Informe de auditoría de sistemas anual del Registro Contable de Facturas*** 1.- La entidad dispone de la auditoría de sistemas realizada por las Intervenciones Generales u órganos equivalentes de cada Administración, tal y como se exige en el Art. 12.3. 1.1.- Verificar que la entidad dispone del informe de auditoría y que éste se realiza con periodicidad anual. Evidencia: Solicitar el informe de auditoría y comprobar fechas de realización. 1.2.- Comprobar que el informe se realiza de acuerdo a los requisitos del Art. 12.3 y de las directrices contenidas en la "Guía para las auditorías de los Registros Contables de Facturas" de la IGAE. En particular, constatar que dicho informe incluye: * Un análisis de los tiempos medios de inscripción de facturas en el registro contable de facturas y del número y causas de facturas rechazadas en la fase de anotación en el registro contable. * La revisión de la gestión de la seguridad en aspectos relacionados con la confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad de los datos y servicios de gestión.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 8-4: Cumplimiento del ENI La Entidad cumple con los criterios y recomendaciones	No		***Cumplimiento del ENI*** 1.- Los sistemas se encuentran adecuados a los criterios y recomentaciones establecidos en el Esquema Nacional de Interoperabilidad (Disposición transitoria RD 4/2010). 2.- En defecto del punto anterior, existe el Plan de Adecuación al Esquema Nacional de Interoperabilidad y se encuentra formalmente aprobado .		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control A1 - CBCS 8:	0 - Inexistente.

A2 Estrategia de Seguridad

Objetivo de control: **Disponer de Estrategia y Planificación de TI para el gobierno de la entidad**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
A.2.1: Planificación estratégica de los SI Existencia de planificación estratégica de los SI	NO		1. ¿Existe un Plan Estratégico de los Sistemas de TI? Evidencia 1: Obtener dicho Plan y revisar si se encuentra aprobado y en vigor para el año del ejercicio fiscalizado		☐ Documento: ☐ Muestreo: Observaciones:				
A.2.1: Planificación Anual de Proyectos de SI Existencia de planificación anual de proyectos de SI aprobados para el ejercicio fiscalizado.	NO		1. ¿Existe un Plan Anual de Proyectos de SI? Evidencia 1: Obtener dicho Plan y revisar si se encuentra aprobado y en vigor para el año del ejercicio fiscalizado		☐ Documento: ☐ Muestreo: Observaciones:				
A.2.1: Dotación Presupuestaria para Proyectos de SI Existencia de dotación presupuestaria en el ejercicio para el plan anual de proyectos del ejercicio	NO		1. ¿Existe dotación presupuestaria para los proyectos incluidos en el Plan Anual de Proyectos de SI? Evidencia 1: Obtener los presupuestos de la entidad para el año del ejercicio fiscalizado y revisar que se encuentran las partidas correspondientes a los proyectos incluidos en el Plan Anual de Proyectos de SI		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control A2	0 - Inexistente.

A3 Organización y Personal de TI

Objetivo de control: **Disponer de una organización de la entidad que se encuentre alineada con los objetivos de seguridad de la misma**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
A.3.1: Independencia Funcional Existe independencia funcional del departamente de sistemas respecto del resto de áreas	NO		1. ¿Es el departamento de sistemas de información independiente de otras áreas funcionales? ¿Depende el departamento de sistemas de información directamente de la dirección? Evidencia 1: Obtener el organigrama de la entidad y concluir sobre la independencia funcional del departamento de sistemas		☐ Documento: ☐ Muestreo: Observaciones:				
A.3.2: Segregación de Funciones Se realiza una correcta segregación de funciones en las tareas críticas	op.acc.3		**Nivel MEDIO** 1.- ¿Existe segregación de funciones y tareas? Evidencia: Consultar funciones incompatibles y solicitar el nombre de las personas que tienen asignadas dichas funciones para constatar que no son las mismas personas. 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 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		☐ Documento: ☐ Muestreo: Observaciones:				
A.3.3: Formación y Concienciación Existe un compromiso en la formación y concienciación en seguridad de la información	mp.per.3		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 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 incidentes de seguridad, sean reales o falsas alarmas? Evidencia: El contenido del plan de concienciación incluye el procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.		☐ Documento: ☐ Muestreo: Observaciones:				
	mp.per.4		2.- ¿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 identifica el responsable de su elaboración, las necesidades formativas de cada puesto de trabajo, así como la planificación en la impartición de la formación necesaria y la frecuencia con la que debe actualizar su formación. Respecto a dicha formación: 2.1.- ¿Cubre la configuración de sistemas? Evidencia: Dicho plan tiene contenidos formativos relativos a la configuración de sistemas. 2.2.- ¿Cubre la detección y reacción a incidentes? Evidencia: Dicho plan tiene contenidos formativos relativos a la detección y reacción a incidentes. 2.3.- ¿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. **Aspectos adicionales relacionados con este control:** 3.- ¿Se llevan a cabo efectivamente las acciones de formación planificadas? Evidencia: Seleccionar una muestra de empleados y comprobar los cursos y formación adquirida durante el periodo bajo análisis en las siguientes materias y que estos coincidan con las acciones planificadas: - Concienciación sobre seguridad de la información. - Uso de las aplicaciones críticas.		☐ Documento: ☐ Muestreo: Observaciones:				
A.3.4: Indicadores de Cumplimiento de Objetivos Se utilizan indicadores para valorar el cumplimiento de objetivos por parte de la dirección	NO		1.- ¿Se utilizan indicadores por parte de la dirección para valorar el cumplimiento de objetivos estratégicos de TI? Evidencia: Solicitar la documentación que acredite el uso de indicadores por parte de la dirección.		☐ Documento: ☐ Muestreo: Observaciones:				
A.3.5: Nombramientos y Constitución de Órganos Se han realizado los nombramientos y constituido los organos de gobierno planificados en la Política de Seguridad y requeridos para el cumplimiento de las obligaciones en cuanto a la seguridad de la información	NO		1.- ¿Se han realizado los nombramientos requeridos para asegurar el cumplimiento normativo y organización de la seguridad? Evidencia: Documentación que acredite el nombramiento formal de los distintos roles. 1.- ¿Se han constituido los órganos de gobierno necesarios para asegurar el cumplimiento normativo y organización de la seguridad? Evidencia: Documentación que acredite la constitución de los organos de gobierno de la seguridad requeridos.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control A3	**0 - Inexistente.**

A4 Marco Normativo y Procedimental de Seguridad

Objetivo de control: **Establecer una normativa interna de seguridad de la información y procedimiento asociados**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
A.4.1: Normativa Interna de Seguridad La entidad ha desarrollado una Normativa Interna de Seguridad	org.2		1.- ¿Dispone de uno o varios documentos que constituyan la normativa de seguridad escrita? Evidencia: La normativa de seguridad está impresa y/o guardada en formato electrónico. 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), los servicios (p. ej.: utilizar Internet para descargar contenidos no autorizados o inapropiados), las instalaciones (p. ej.: comer en la sala de servidores), la información (p. ej.: enviar datos confidenciales mediante correo electrónico sin cifrar), etc. 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).		☐ Documento: ☐ Muestreo: Observaciones:				
A.4.2: Procedimientos de Seguridad La entidad ha desarrollado un conjunto de Procedimientos de Seguridad para facilitar el cumplimiento de la Normativa Interna de Seguridad	org.3		1.- ¿Dispone de uno o varios documentos que constituyan los procedimientos de seguridad escritos? Evidencia: Los procedimientos de seguridad están impresos y/o guardados en formato electrónico, los ha elaborado el responsable STIC y están aprobados por el Comité STIC. Además, existe un procedimiento de revisión y firma regular. Deben existir procedimientos para la mayoría de las actividades rutinarias, cuanto más próximo al 100% mejor (p. ej.: sobre el inventariado de activos, la modificación de reglas en el firewall, las tareas de copia de seguridad o backup, el alta de usuarios, etc.). 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, (p. ej.: el procedimiento de inventario de activos podría indicar "Tras la aprobación del cambio -adición, modificación o supresión- de uno o más activos del inventario, la persona encargada y autorizada para dicho cambio -el administrador de sistemas si es un servidor, el técnico de comunicaciones si es un elemento de red, etc.- deberá anotar en el inventario qué tipo de cambio se ha producido, sobre qué activo, la fecha y su nombre –además de actualizar el detalle del activo-. En caso de encontrar algún problema en este procedimiento, reportarlo al responsable STIC detallando, mediante el sistema de notificaciones previamente estipulado, cuál ha sido el problema y, al menos, una propuesta de solución"). 1.2.- ¿Precisan quién debe hacer cada tarea? Evidencia: Se asigna cada tarea a un rol (responsable STIC, administrador, operador, etc.) (p. ej.: el procedimiento de inventario de activos podría indicar "Será el administrador de sistemas quien revise cada 6 meses el inventario de activos, si identifica que no ha cambiado ningún activo desde la última revisión, procederá a comprobar que efectivamente no se ha modificado nada dentro del alcance del inventario para asegurar que no ha habido ningún cambio no autorizado ni reportado"). 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).		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control A4	0 - Inexistente.

B1 Adquisición de Aplicaciones y Sistemas

Objetivo de control: **Disponer de un procedimiento para la compra de aplicaciones y sistemas de forma que se responda efectivamente a las necesidades reales y se tenga en consideración los criterios de seguridad.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
B.1.1: Procedimiento de Adquisición de Aplicaciones y Sistemas Las aplicaciones y los sistemas se compran en base a un procedimiento establecido que tiene en consideración los criterios de seguridad de la entidad	op.pl.3		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.), que incluye la persona responsable de revisar y mantener este procedimiento. Dispone de un documento que indica las medidas de seguridad requeridas para los nuevos componentes adquiridos y su cumplimiento (p. ej.: dispone de un checklist con los requisitos que debe tener el firewall –cifrado IPSec, stateful packet inspection, etc.- y su correspondiente indicación sobre si lo cubre o no -en cuyo caso se argumenta el motivo- junto con el nombre de la persona que ha realizado la verificación y la fecha de la misma). 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 (p. ej.: el checklist indica si el motivo de algún requisito impuesto al firewall proviene del análisis y gestión de riesgos). 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 a 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 (p. ej.: el checklist contempla que cumpla o no -en cuyo caso se argumenta el motivo- las necesidades técnicas enumeradas, las necesidades de formación –si no están cubiertas actualmente indicará la forma de cubrirlas mediante cursos, manuales, etc. aprobados). **Aspectos adicionales relacionados con este control:** 2. ¿Se realizan las compras de aplicaciones y sistemas de acuerdo al procedimiento establecido? Evidencia: Para un determinado numero de aplicaciones o sistemas adquiridos durante el periodo auditado, confirmar que se dispone de un estudio preliminar realizado en base al procedimiento establecido.		☐ Documento: ☐ Muestreo: Observaciones:				
B.1.2: Adquisición de Aplicaciones y Sistemas por Objetivos Estratégicos y de Seguridad Las aplicaciones y los sistemas se compran en base a un procedimiento establecido que tiene en consideración los objetivos estratégicos de la entidad	NO		1.- ¿El proceso formal para planificar la adquisición de nuevos componentes del sistema tiene en consideración los objetivos estratégicos de la entidad? Evidencia: Evaluar si el procedimiento garantiza la alineación con los objetivos estratégicos de la entidad. - Identificación de soluciones automatizadas - Propuestas de adquisición - Comparación de productos - Aprobación 2.- ¿Se realizan las compras de aplicaciones y sistemas considerando la alineación con los objetivos estratégicos de la entidad? Evidencia: Para un determinado numero de aplicaciones o sistemas adquiridos durante el periodo auditado, confirmar que se dispone de un estudio preliminar que incluye la evaluación de la adquisición con los objetivos estratégicos de la entidad.						
B.1.3: Dimensionamiento en la Adquisición de Aplicaciones y Sistemas Las aplicaciones y los sistemas se compran considerando el correcto dimensionamiento para responder efectivamente a los requisitos funcionales de usuario.	op.pl.4		**Nivel MEDIO** 1.- ¿Antes de la puesta en explotación, se han estudiado las necesidades de dimensionamiento? Evidencia: Dispone de un estudio en cualquier formato con dicho análisis, antes de cada adquisición o puesta en explotación, de las necesidades de los medios adicionales o capacidades de los medios existentes, de modo que estos satisfagan los requisitos establecidos. En caso de que no queden satisfechos, se argumenta. Existen evidencias documentales de cada estudio, en el que se refleja quién lo realizó, la fecha y el resultado. Respecto a dicho estudio del dimensionamiento: 1.1.- ¿Cubre las necesidades de procesamiento? Evidencia: Dicho estudio estima 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 estima las necesidades de almacenamiento tanto para su funcionamiento como para el tiempo durante el que la información debe mantenerse (p. ej.:se ha calculado el volumen de datos generado cada día, el número de días que se utilizará el servicio y el tiempo que la información deberá estar accesible –tanto on-line como en un backup-, y el dispositivo lo soporta). 1.3.- ¿Cubre las necesidades de comunicación? Evidencia: Dicho estudio estima las necesidades de comunicación (p. ej.: el ancho de banda disponible soporta el volumen de datos a transmitir en cada momento, o que el dispositivo soporta el acceso desde otra ubicación). 1.4.- ¿Cubre las necesidades de personal: cantidad y cualificación profesional? Evidencia: Dicho estudio estima las necesidades de personal necesario para la gestión del mismo (p. ej.: existe personal con dedicación para la gestión del elemento) de forma adecuada (p. ej.: la gestión del elemento se realizará por personal que domina su interfaz de uso y gestión). 1.5.- ¿Cubre las necesidades de instalaciones y medios auxiliares? Evidencia: Dicho estudio estima las necesidades de las instalaciones (p. ej.: el dispositivo cabe por tamaño en el armario de servidores y además quedan bahías libres donde ubicarlo) y los medios auxiliares (p. ej.: las frigorías existentes de aire acondicionado serán suficientes para seguir enfriando el CPD).		☐ Documento: ☐ Muestreo: Observaciones:				

B.1.4: Adquisición de Aplicaciones y Sistemas Evaluadas desde el punto de vista de la Seguridad Las aplicaciones y los sistemas que lo requieran se compran considerando que hayan sido evaluados conforme a normas europeas o internacionales de seguridad.	op.pl.5		**Nivel ALTO** 1.- ¿Se utilizan sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales? Evidencia: Dispone de un listado de modelos para la adquisición de componentes cuya evaluación se haya realizado conforme a normas europeas o internacionales (p. ej.: cumple la ISO/IEC 15408 -Common Criteria-) o una certificación funcional que contemple: - Diseño, desarrollo, pruebas y revisión del componente con método. - Análisis de vulnerabilidades para ataques de nivel de competencia técnica tan alto como permita la tecnología existente en el campo, o tan alto como permita la normativa de referencia utilizada. - Máximo nivel de confianza que proporcione la normativa utilizada respecto a la prueba de robustez de la seguridad del componente, cuando es utilizado de forma distinta a la especificada por su documentación de uso. - Máximo nivel de confianza que proporcione la normativa utilizada respecto a la resistencia de las funciones de seguridad del producto, que se basen en mecanismos probabilísticos o permutacionales: resistencia a ataques 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 o certificación. 2.- ¿Y están los certificados reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información? Evidencia: Las certificaciones de los componentes son reconocidas por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Respecto a los componentes de cifra y generación de firma electrónica han sido certificados criptológicamente, en términos de su fortaleza algorítmica, y existe evidencia de ello. **Aspectos adicionales relacionados con este control:** 1. ¿Se utilizan sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales? Evidencia: Para cada uno de los componentes del sistema de nivel alto, se confirmará que disponen de evaluación de seguridad conforme a los criterios anteriores		☐ ☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control B1	**0 - Inexistente.**

B2 Desarrollo de Aplicaciones

Objetivo de control: **Disponer de un procedimiento para el desarrollo de aplicaciones y sistemas de forma que se tenga en consideración los criterios de seguridad.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
B.2.1: Metodología de Desarrollo El desarrollo de aplicaciones se realiza de manera metodológica y considera los criterios de seguridad de la entidad	mp.sw.1		**Nivel MEDIO** 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). Existe evidencia documental del uso de la metodología de desarrollo (p. ej.: METRICA establece la elaboración de una serie de documentos, constatar que se han elaborado). 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. 3.4.- ¿Incluye normas de programación segura? Evidencia: Dicha metodología de desarrollo incluye normas de programación segura. 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. 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 o de datos reales disociados o enmascarados, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente. Existe evidencia que en el entorno de desarrollo no existen datos reales, o de lo contrario está aprobado por el responsable.		☐ Documento: ☐ Muestreo: Observaciones:				
B.2.2: Entornos de Desarrollo El desarrollo de aplicaciones se realiza en sistemas o entornos separados de producción	mp.sw.1		**Nivel MEDIO** 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 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. Constatar que no existen herramientas de desarrollo en el entorno de producción (p. ej.: no hay compiladores en los sistemas de producción). Verificar la separación de entornos de desarrollo y operación: Características, requisitos y configuración de estos.		☐ Documento: ☐ Muestreo: Observaciones:				
B.2.3: Aceptación y puesta en servicio La aceptación y puesta en servicio de aplicaciones desarrolladas se realiza de manera metodológica y considera los criterios de seguridad de la entidad	mp.sw.2		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. Existe evidencia documental del plan de pruebas ejecutado y su resultado. 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? Evidencia: Dicho plan contempla que las pruebas se realizan con datos ficticios o datos reales disociados o enmascarados, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente. **Nivel MEDIO** 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. Consultar los resultados y, si estos han identificado alguna		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 1. ¿Se requiere de la aprobación del usuario en las pruebas de testeo previamente al paso a producción? (B.3.6) Evidencia: Los procedimientos de gestión de cambios y puesta en producción de sistemas adquiridos o desarrollados, incluyen la aceptación del usuario final de las pruebas de testeo. Para un número de cambios o puestas en producción de sistemas, verificar la existencia de la aprovación formal por parte del usuario.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control B2	0 - Inexistente.

B3 Gestión de Cambios

Objetivo de control: **Gestionar los cambios de los sistemas y aplicaciones y de sus configuraciones.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
B.3.1: Procedimientos para la gestión de cambios de configuración del sistema Existen procedimientos para la gestión de cambios de configuración del sistema	op.exp.3		**Nivel MEDIO** 1.- ¿Se gestiona de forma continua la configuración? Evidencia: 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		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 2. ¿Se utiliza alguna herramienta para automatizar la gestión de cambios en la configuración de los sistemas? Evidencia: La entidad dispone de herramientas software para la gestión integral de la configuración de los sistemas. 3. ¿Se realiza la gestion continuada de la configuración en las aplicaciones y sistemas significativos? Evidencia: Se dispone de documentación que acredita la gestión continuada de la configuración de todas las aplicaciones y sistemas significativos, incluyendo: -Lista de cambios de configuración en sistemas relevantes del entorno IT desde el principio del periodo de auditoría hasta la fecha de la prueba. Seleccionar una muestra de cambios y comprobar que fueron: + debidamente registrados (se registran todas las solicitudes) + debidamente autorizados + debidamente probados + debidamente aprobados -Documentación generada de los cambios realizados (a nivel de código, manuales de usuario...). -Evidencia suficiente de que el proceso de cambios es monitorizado regularmente (p.e, comité de cambios, revisión de los cambios a producción...)		☐ Documento: ☐ Muestreo: Observaciones:				
B.3.2: Procedimientos para la gestión de cambios de componentes o arquitectura del sistema Existen procedimientos para la gestión de cambios de componentes o arquitectura del sistema	op.exp.5		**Nivel MEDIO** 1.- ¿Dispone de un control continuo de cambios realizados en el sistema? Evidencia: Dispone de un procedimiento documentado que indica los motivos por los que se debe cambiar un componente del sistema e incluye: la aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema tras el cambio, y la retención de una copia del componente previo por un tiempo preestablecido. Consultar si se dispone de copias de seguridad de la versión del software actual y la inmediata anterior de los diferentes componentes. Este procedimiento se encuentra enlazado con el procedimiento de actualización del inventario de activos, de actualización de los procedimientos operativos relacionados con el componente cambiado y de actualización del plan de continuidad del negocio (si aplica). 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. 1.3.- ¿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. Consultar el último cambio realizado y ver si se realizó en la ventana de tiempo estipulada. 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), la persona responsable de dicha actualización y, en caso de que el riesgo resultante sea alto, requerirá la aprobación explícita del cambio por parte del propietario. Consultar el impacto de los cambios en el análisis de riesgos.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 1. ¿Se realiza efectivamente la gestion continuada de los cambios en las aplicaciones y sistemas significativos? Evidencia: Se dispone de documentación que acredita la gestión continuada de los cambios de arquitectura y componentes de todas las aplicaciones y sistemas significativos, incluyendo: -Lista de cambios de arquitectura y componentes en sistemas relevantes del entorno IT desde el principio del periodo de auditoría hasta la fecha de la prueba. Seleccionar una muestra de cambios y comprobar que fueron: + debidamente registrados (se registran todas las solicitudes) + debidamente autorizados + debidamente probados + debidamente aprobados -Documentación generada de los cambios realizados (a nivel de código, manuales de usuario...). -Evidencia suficiente de que el proceso de cambios es monitorizado regularmente (p.e, comité de cambios, revisión de los cambios a producción...)		☐ Documento: ☐ Muestreo: Observaciones:				
B.3.3: Responsables y órganos para la gestión de cambios de aplicaciones o sistemas Se han asignado responsabilidades y constituido organos para la gestión continuada de cambios en aplicaciones y sistemas	NO		1. ¿Se han asignado responsabilidades y constituido organos para la gestión continuada de cambios en aplicaciones y sistemas? Evidencia: Se dispone de documentación que acredita la asignación de responsabilidades relativas a la gestión continuada de los cambios en aplicaciones y sistemas. Se dispone de actas de constitución de organos de gestión de cambios.		☐ Documento: ☐ Muestreo: Observaciones:				

B.3.4: Pruebas de testeo de los cambios en aplicaciones y sistemas Se realizan pruebas de testeo previas a la puesta en producción de los cambios en aplicaciones y sistemas	op.exp.5		**Nivel MEDIO** 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 y el registro de pruebas previas a la puesta en producción del cambio (que, quién, cómo y cuándo). Consultar el último cambio realizado, y hacer muestreo, si se considera.		☐ Documento: ☐ Muestreo: Observaciones:				
B.3.5: Entornos para pruebas separados de producción Se dispone de entornos separados del producción para la realización de pruebas	mp.sw.1		**Nivel MEDIO** 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 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. Constatar que no existen herramientas de desarrollo en el entorno de producción (p. ej.: no hay compiladores en los sistemas de producción). Verificar la separación de entornos de desarrollo y operación: Características, requisitos y configuración de estos.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 3. ¿Se utilizan entornos separados de producción las pruebas de testeo de cambios en configuraciones o componentes del sistema previamente al paso a producción? Evidencia: Para un determinado número de cambios registrados, verificar la documentación y los registros para confirmar las pruebas en entornos separados de producción						
B.3.6: Aprobación del usuario en las pruebas de testeo Se requiere la aprobación del usuario en las pruebas de testeo previamente al paso a producción	NO		1.- ¿Se requiere de la aprobación del usuario en las pruebas de testeo previamente al paso a producción? Evidencia: Los procedimientos de gestión de cambios y puesta en producción de sistemas adquiridos o desarrollados, incluyen la aceptación del usuario final de las pruebas de testeo. Para un número de cambios o puestas en producción de sistemas, verificar la existencia de la aprovación formal por parte del usuario.		☐ Documento: ☐ Muestreo: Observaciones:				
B.3.7: Separación de las tareas para la gestión de cambios de aplicaciones o sistemas Se gestiona la separación de las tareas y el control de los accesos a los distintos entornos utilizado para desarrollo y pruebas de testeo en aplicaciones y sistemas	op.acc.3		1.- ¿Existe segregación de funciones y tareas? Evidencia: Consultar funciones incompatibles y solicitar el nombre de las personas que tienen asignadas dichas funciones para constatar que no son las mismas personas.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 1. ¿Se realiza separación de las tareas y el control de los accesos a los distintos entornos utilizado para pruebas de testeo en aplicaciones y sistemas? Evidencia: Los procedimientos de gestion de cambios de configuración, componentes o arquitectura de aplicaciones y sistemas incluyen la separación formal de tareas y el control de accesos a los distintos entornos. Evidencia: Se comprueba que, tanto orgánicamente como a nivel de accesos lógicos, las siguientes tareas son realizadas por personas diferentes. - Solicitar/aprobar desarrollos de programas o cambios en los programas. - Programar el desarrollo o cambio - Traspaso de programas a/desde producción - Monitorizar el desarrollo de programas y cambios. Obtener una lista de usuarios con acceso a los entornos de desarrollo. Verificar si exite una autorización formal. Obtener listado de los usuarios que están autorizados para transportar los cambios al entorno de producción. Verificar si existen coincidencias con el listado de desarrolladores.		☐ Documento: ☐ Muestreo: Observaciones:				
B.3.8: Registro de cambios y solicitudes Se documentan y registran los cambios y las solicitudes	NO		1. ¿Se realiza la gestión documental y registro de las peticionos y los cambios en las aplicaciones y sistemas significativos? Evidencia: Se dispone de documentación que acredita el reguistro documental de las peticiones y los cambios de configuración, arquitectura y componentes de todas las aplicaciones y sistemas significativos, incluyendo: Lista de cambios de arquitectura y componentes en sistemas relevantes del entorno IT desde el principio del periodo de auditoría hasta la fecha de la prueba. Seleccionar una muestra de cambios y comprobar que fueron: - debidamente registrados (se registran todas las solicitudes) - debidamente autorizados - debidamente probados - debidamente aprobados		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control B3	**0 - Inexistente.**

C1 - CBCS 1 Inventario y control de dispositivos físicos

Objetivo de control: **Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 1.1: Inventario de activos físicos autorizados La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.	op.exp.1		1.- ¿Dispone de un inventario de activos físicos? Evidencia: Dispone de un inventario de los elementos que componen el sistema, en el que se detalla su identificador, fabricante y modelo (p. ej.: "JUPITER" - Cisco 2128, "ORION" - Dell PowerEdge R420, etc.). Respecto a dicho inventario: 1.1.- ¿Identifica la naturaleza de los elementos? Evidencia: Cada elemento del inventario tiene especificado de qué tipo es (p. ej.: el elemento "JUPITER" indica que es un router, el elemento "ORION" indica que es un servidor, etc.). 1.2- ¿El inventario incluye el detalle necesario? El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema de información, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes. - Identificación del activo: fabricante, modelo, número de serie - Configuración del activo: perfil, política, software instalado - Equipamiento de red: MAC, IP asignada (o rango) - Ubicación del activo: ¿dónde está? - Propiedad del activo: persona responsable del mismo. 1.3.- ¿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). 1.4.- ¿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. 1.5.- ¿Se dispone de un procedimiento para la aprobación del uso de nuevo hardware? Evidencia: Dispone de un procedimiento para solicitar la autorización de nuevos elementos HW (quién puede solicitarlo, cómo debe hacerlo, quién debe autorizar, etc.). Aspectos adicionales relacionados con este control: 1.- ¿Cómo se actualiza el inventario? ¿De forma manual o automática? Si es de forma automática, indicar herramienta utilizada. Evidencia 1: En el caso de que la actualización sea manual: Procedimiento de mantenimiento: responsables de realizarlo, frecuencia de actualización, etc. Evidencia 2: En el caso de que la actualización sea automática: Procedimiento de mantenimiento, revisión de la herramienta utilizada. Evidencia 3: Realizar un muestreo de elementos HW y comprobar que el inventario está correctamente actualizado.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 1-2: Control de activos físicos no autorizados La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados.	No		Mantenimiento de la configuración: ¿Cómo se garantiza que no se conectan a la red de la entidad dispositivos o elementos HW no autorizados? Posibles alternativas: - Control reactivo: Se dispone de un procedimiento de revisión periódica de hardware no controlado. El procedimiento indica responsables de su realización, alcance, frecuencia, medidas a adoptar ante la detección de HW no autorizado. Evidencia: Solicitar procedimiento y evidencias de su ejecución. - Control preventivo: La entidad dispone de procedimientos/políticas que describen las medidas de seguridad a implantar para controlar (detectar o restringir) el acceso de dispositivos físicos no autorizados. Dichas medidas pueden variar de una entidad a otra. Posibles alternativas son: * No activar en los paneles de parcheo[1] lo que no sea necesario (ej. si en una toma de red no está previsto que se conecte nadie, no cablearla). * No activar los puertos de switches no utilizados. * Restringir el número de MACs que se pueden conectar a una toma de red. * Aprender la primera MAC que se conecta a una toma de red y restringir la conexión de otras diferentes (en el caso de dispositivos de red CISCO, el comando que se utiliza es *"sticky"*). Evidencia: Obtener procedimiento, guía, etc. donde se describa la implementación de la medida de seguridad, responsables de implementarla, frecuencia de revisión, etc. y obtener evidencia de su eficacia operativa. *(1) El panel de parcheo (patch panel en inglés) es el punto de la red informática donde terminan todos los cables del cableado estructurado. Los puntos de red van desde las cajas de suelo o rosetas ubicadas en los puestos de trabajo hasta el rack o armario de telecomunicaciones, donde se encuentra instalado el panel de parcheo.*		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C1 - CBSC1	0 - Inexistente.

C1 - CBCS 2 Inventario y control de software autorizado

Objetivo de control: **Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 2-1: Inventario de SW autorizado La entidad dispone de un inventario de SW completo, actualizado y detallado.	op.exp.1		1.- ¿Dispone de un inventario de software? Evidencia: Dispone de un inventario de los elementos SW que componen el sistema. * Fabricante, producto, versión y parches aplicados. * Elemento/s HW en los que se encuentra instalado. Respecto a dicho inventario: 1.1.- ¿El inventario incluye el detalle necesario? - Fabricante, producto, versión y parches aplicados. - Elemento/s HW en los que se encuentra instalado. - Propiedad del activo: persona responsable del mismo. 1.2.- ¿Identifica a los responsables de los elementos? Evidencia: Cada elemento del inventario tiene especificado quién es su responsable. 1.3.- ¿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. 1.4.- ¿Se dispone de un procedimiento para la aprobación del uso de nuevo software y existe una relación de SW autorizado? Evidencia: Dispone de un procedimiento para solicitar la autorización de nuevos elementos SW (quién puede solicitarlo, cómo debe hacerlo, quién debe autorizar, etc.) y una relación del SW cuyo uso está autorizado en la entidad. Aspectos adicionales relacionados con este control: 1.- ¿Cómo se actualiza el inventario? ¿De forma manual o automática? Si es de forma automática, indicar herramienta utilizada. Evidencia 1: En el caso de que la actualización sea manual: Procedimiento de mantenimiento: responsables de realizarlo, frecuencia de actualización, etc. Evidencia 2: En el caso de que la actualización sea automática: Procedimiento de mantenimiento, revisión de la herramienta utilizada. Evidencia 3: Realizar un muestreo de software y comprobar que el inventario está correctamente actualizado.	Ver CBCS 1.1	☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 2-2: SW soportado por el fabricante. El SW utilizado por la entidad tiene soporte del fabricante. En caso contrario, se marca en el inventario como fuera de soporte.	op.exp.4		1.- ¿Dispone de un plan de mantenimiento del software? Evidencia: Dispone de un procedimiento documentado que indica los componentes a revisar, responsable de la revisión y evidencias a generar. Solicitar evidencias de la ejecución del 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. *Prueba complementaria para evaluar este control:* 1.- ¿Se controlan las fechas de fin de soporte del SW? Evidencia: Dispone de un procedimiento para la revisión del SW autorizado en la entidad y las fechas dadas por los fabricantes de fin de soporte. Este procedimiento incluye: - Responsable de realizar este control. - Frecuencia de realización (considerar que los procesos de actualización del SW pueden ser complejos y largos (ej. del SW de sistema operativo, de base de datos, etc.) por lo que la frecuencia de realización debe permitir un margen de actuación suficiente. - Relación con el proceso de "Adquisición de nuevos componentes" (op.pl.3), que asegure que una vez detectado la necesidad de actualización del SW, para aquél que requiera la compra de nuevas licencias, éstas son adquiridas en tiempo y forma oportuno. 2.- ¿Existe software fuera de soporte por parte del fabricante? Evidencia: Revisar el inventario de hardware y software y, para una muestra de elementos, comprobar que estos se encuentran dentro del soporte del fabricante.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 2-3: Control de SW no autorizado La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.			1.- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación que garantice la aplicación de la regla de mínima funcionalidad? NOTA: Sólo revisar la existencia del procedimiento y que contemple la instalación únicamente del SW necesario (no revisar resto del procedimiento, ya que se ve en el CBCS 5). Evidencia: Dispone de un procedimiento documentado que indica las actividades a realizar en los sistemas (perfil de seguridad) para su configuración segura previa a su entrada en operación. Dicho procedimiento está avalado por una autoridad reconocida (p. ej.: plantillas de seguridad y recomendaciones de bastionado del CCN). Existe evidencia documental (p. ej.: checklist) de la fortificación realizada a los sistemas, indicando la persona que lo realizó y la fecha y la versión del procedimiento que utilizó. Respecto a dicho procedimiento de bastionado: 1.1.- ¿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.		☐ Documento: ☐ Muestreo: Observaciones:				

C1 - CBCS 2 Inventario y control de software autorizado

Objetivo de control: **Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
	op.exp.2 b)		***Prueba adicional a realizar para evaluar este control:*** 1.- En cuanto al bastionado de equipos, ¿las guías de configuración incluyen el detalle del SW a instalar por tipo de sistema y/o usuario? (ej. SW a instalar en el equipo cliente de un usuario no administrador del área de gestión presupuestaria, SW a instalar en el servidor de BBDD de la aplicación X, etc.). Evidencia: * Existen guías u otros documentos técnicos que indican el detalle del SW a instalar en función del perfil del usuario. Estas guías se utilizan para la instalación y plataformado de los equipos. * Existen maquetas en función del tipo usuario/dispositivo, que se utilizan para plataformar los equipos. 2. Mantenimiento de la configuración: Una vez instalados y configurados los sistemas con el SW necesario, ¿cómo se garantiza que el usuario no pueda instalarse nuevo SW? Posibles alternativas: - Control reactivo: Se dispone de un procedimiento de revisión periódica de software no controlado. El procedimiento indica responsables de su realización, alcance, frecuencia, medidas a adoptar ante la detección de SW no autorizado. Evidencia: Solicitar procedimiento y evidencias de su ejecución. - Control preventivo: Se utilizan herramientas de listas blancas de aplicaciones, librerías, etc... (ej. Applocker). Si éste es el caso revisar si están configuradas en modo auditoría (sólo registra las aplicaciones que se ejecutan) o en modo bloqueo (no permite ejecutar nada que no esté en las listas blancas). NOTA: Si los usuarios son administradores de sus equipos, en la mayoría de los casos, este control NO va a ser efectivo (porque dispondrán de permisos para instalarse lo que deseen). Y, aunque no sean administradores, no es 100% efectivo, porque no te permite el control de todo el tipo de SW (ej. Macros) ni de la no ejecución del SW portable.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C1 - CBSC2	0 - Inexistente.

C2 - CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades

Objetivo de control: **Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 3-1 Identificación de vulnerabilidades Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que éstas son identificadas en tiempo oportuno.	op.exp.4		Publicación de defectos por los fabricantes 1.- ¿Efectúa un seguimiento continuo de los anuncios de defectos realizados por los fabricantes? Evidencia 1: 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, contratación de un servicio directamente con el fabricante para el envío periódico de los defectos publicados y su análisis, suscripción a páginas de la industria donde se publique esta información (CCN-CERT, Hispasec, proveedores de este tipo de noticias, etc.). Dispone de un procedimiento documentado que indica quién y con qué frecuencia monitorizar esos anuncios. Evidencia 2: Obtener evidencias de la ejecución de este procedimiento.		☐ Documento: ☐ Muestreo: Observaciones:				
	mp.sw.2		1.- ¿Previamente a la entrada en servicio de un sistema, se le realiza un análisis de vulnerabilidades? Evidencia 1: Comprobar que el plan de puesta en servicio de un sistema contempla la ejecución de un análisis de vulnerabilidades. Evidencia 2: De un listado de sistemas puestos en servicio durante el periodo de auditoría, solicitar los resultados del escaneo de vulnerabilidades u otras evidencias de su ejecución. 2.- ¿Y se le realiza una prueba de penetración? Evidencia 1: Comprobar que el plan de puesta en servicio de un sistema contempla la ejecución de una prueba de penetración. Evidencia 2: De un listado de sistemas puestos en servicio durante el periodo de auditoría, solicitar los resultados de la prueba de penetración u otras evidencias de su ejecución. 3.- Inspección de código fuente: ¿Se considera la oportunidad de realizar una auditoría de código fuente? Evidencia: Dicho plan contempla la oportunidad de realizar una auditoría de código fuente. Consultar los resultados, o en caso de que no se haya realizado consultar los motivos para ello.		☐ Documento: ☐ Muestreo: Observaciones:				
	No		Prueba complementaria para evaluar este control: Tras la puesta en servicio de un sistema, y a lo largo de toda su vida útil: 1.- ¿Se realizan escaneos de vulnerabilidades periódicos? En caso afirmativo, identificar alcance, frecuencia, responsables. Evidencia 1: Procedimiento de realización de escaneos de vulnerabilidades, que describa los sistemas incluidos en el alcance de dicho procedimiento, responsables de realizarlo y frecuencia. Evidencia 2: Solicitar los informes resultado de los últimos escaneos realizados. Evidencia 3: Identificar la herramienta de escaneo utilizada y si ésta dispone de registros de ejecución revisar que la frecuencia y alcance indicados en el procedimiento concuerdan con estos. 1.3.- Tests de penetración: Evidencia 1: Comprobar que el plan de puesta en servicio de un sistema contempla la ejecución de una prueba de penetración. Evidencia 2: De un listado de sistemas puestos en servicio durante el periodo de auditoría, solicitar los resultados del test de penetración realizado u otras evidencias de su ejecución.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 3-2 Priorización Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al riesgo que suponen para la seguridad del sistema.	op.exp.4c)		¿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 1: Dispone de un 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, nuevas versiones y cualquiera de las actuaciones necesarias para la resolución de defectos de seguridad. Dicho procedimiento contempla el proceso para reportar los cambios que pudieran ser necesarios. ***Aspectos adicionales relacionados con este control:*** Para una relación de las vulnerabilidades identificadas en el apartado anterior, revisar la priorización realizada. Comprobar la coherencia entre la priorización realizada con la criticidad asignada por el fabricante.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 3-3 Resolución de vulnerabilidades Se realiza un seguimiento de la corrección de las vulnerabilidades identificadas, de forma que se garantiza que éstas son resueltas en el tiempo previsto en el procedimiento.	No		1.- ¿Se realiza el seguimiento de la corrección de las vulnerabilidades identificadas que, de acuerdo a la gestión de riesgos se ha decidido resolver? Evidencia 1: Procedimiento de seguimiento y responsables de realizarlo. Solicitar evidencia de la ejecución del plan. Evidencia 2: Si la entidad realiza escaneos periódicos sobre los mismos sistemas, comprobar que las vulnerabilidades identificadas en un informe para las que se ha decidido realizar acciones correctoras, no aparecen en el siguiente escaneo de vulnerabilidades.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 3-4 Parcheo La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los			¿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.		☐ Documento: ☐ Muestreo: Observaciones:				

C2 - CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades

Objetivo de control: **Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
fabricantes en un tiempo razonable.	op.exp.3		***Prueba complementaria para evaluar este control:*** ¿Existe un procedimiento sobre el parcheo de dispositivos? Evidencia 1: Obtener dicho procedimiento y revisar si incluye alcance, frecuencia y método (p.ej. Parcheo automático en equipos cliente y manual en servidores, aplicación de parches de forma acumulada cada x tiempo, etc.). Evidencia 2: Si el parcheo se realiza mediante una herramienta, identificar ésta y, si están disponibles, revisar registros de ejecución. Evidencia 3: En equipos cliente que se actualicen mediante herramienta, comprobar que el sistema fuerza la instalación de parches y actualizaciones, y que el usuario no puede cancelarlas ni posponerlas indefinidamente. Evidencia 4.- Seleccionar una muestra de sistemas y consultar el nivel de parcheo y actualización y su fecha de realización.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C2- CBSC3	0 - Inexistente.

C3 - CBCS 5 Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores

Objetivo de control: **Establecer, implantar y gestionar (seguimiento, reporte y corrección) la configuración de seguridad de los dispositivos móviles, portátiles, servidores y equipos de sobremesa, mediante un proceso de control de cambios y gestión de la configuración riguroso, con el objetivo de prevenir ataques mediante la explotación de servicios y configuraciones vulnerables.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 5-1 Configuración segura La entidad ha definido, documentdo e implantado estándares de configuración segura para todos los sistemas operativos y SW	op.exp.2		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.: plantillas de seguridad y recomendaciones de bastionado del CCN. Existe evidencia documental (p. ej.: checklist) de la fortificación realizada a los sistemas, indicando la persona que lo realizó y la fecha y la versión del procedimiento que utilizó. Respecto a dicho procedimiento de bastionado: 1.0.- Alcance: ¿Qué tipo de dispositivos cubre (servidores, equipos de sobremesa, portátiles, móviles y tabletas, etc.)? 1.0.1.- ¿Contempla diferentes líneas base de configuración (o imágenes de configuración) en función del tipo de dispositivo y funcionalidad (ej. dentro de los servidores, puede ser necesario definir un bastionado diferente para un servidor de la DMZ, un servidor de correo o un servidor de BBDD de la red interna)?. 1.0.2.- Está basado en checklist, guías y recomendaciones de fabricantes y/o organismos de referencia? (Posibles alternativas: guías desarrolladas por el ENS, NIST (https://nvd.nist.gov/ncp/repository), CIS 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.). Solicitar el listado de usuarios para comprobar que no existen cuentas que se han debido retirar según el procedimiento. 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. 1.3.- ¿Detalla los mecanismos a utilizar para mantener el reloj del sistema en hora? --> Este control está también directamente relacionado con el control relativo a asegurar la fecha y hora del sistema en los registros de actividad (ver control 6.2) Evidencia: El procedimiento indica de qué fuentes se tomará la hora del sistema. Preferiblemente considerará más de una fuente. 2.- Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. ¿indica el sistema esa posibilidad al usuario, y tiene éste que dar su consentimiento expreso asumiendo el riesgo? Evidencia: Dispone de un procedimiento documentado para registrar qué situaciones pueden poner en riesgo la seguridad y asegurar que estas requieren el consentimiento expreso del usuario. Si el usuario realiza una acción que puede poner en riesgo la seguridad pero la organización la consiente bajo la responsabilidad del usuario (p. ej.: exportar un listado de datos de carácter personal para un tratamiento específico conocido por la organización, pero que requiere crear un fichero temporal que debe cumplir las mismas medidas de seguridad que el fichero original), el usuario tendrá que aceptar conscientemente esa posibilidad, su responsabilidad y consecuencias (p. ej.: en ese caso debe aparecerle al usuario una ventana de advertencia, que por defecto tendrá marcada la opción de "no continuar", informando de esto al usuario y solicitándole la aceptación de las condiciones). Consultar si quedan registros de estos consentimientos de los usuarios. 3.- ¿La configuración por defecto es segura? Evidencia: Por defecto, la configuración del sistema es segura (p. ej.: en caso de que el usuario no haya especificado una clave para un servicio, ésta no estará vacía, sino que tendrá una clave preconfigurada –que no sea estándar-).		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 5-2: Gestión de la configuración La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.	op.exp.3		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.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba complementaria para evaluar este control: 1.- ¿Cómo garantiza que las configuraciones actuales cumplen con lo anterior, es decir, que no se han realizado cambios en la configuración posteriores a la instalación que perjudiquen la seguridad del sistema? Una posible alternativa es el uso de herramientas de gestión de la configuración y monitorización automática de la configuración (como indica el CIS). Otra alternativa menos robusta pero más sencilla es hacer revisiones periódicas de la configuración.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C3- CBSC5	**0 - Inexistente.**

C4 - CBCS 6 Registro de la actividad de los usuarios (Mantenimiento, monitorización y análisis de los LOG de auditoría)

Objetivo de control: **Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 6-1: Activación de logs de auditoría El log de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ciberataques.	op.exp.8		1.- ¿Se registran todas las actividades de los usuarios en el sistema especialmente activando los registros de actividad en los servidores? Evidencia: Dispone de una política o normativa documentada que indica que se deben registrar todas las actividades de los usuarios en el sistema. Existen mecanismos para aplicar dicha política o normativa y dichos mecanismos están activados. Evidencia 2: Muestreo. Seleccionar una muestra de sistemas y comprobar que los registros de actividad son coherentes con lo definido en la política. Respecto a dichos registros: 1.1.- ¿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 ([op.pl.1]). 1.1.1 .- En base al análisis anterior (u otros criterios si fuera el caso), la política describe qué nivel de detalle se ha de incluir en cada log. Evidencia: Procedimiento para la gestión de registros de auditoría. Comprobar que incluye la información que se registrará. Evidencia 2: Muestreo. Seleccionar una muestra de sistemas y comprobar que los registros de actividad son coherentes con lo definido en la política. 1.2.- ¿Indican quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario? Evidencia: Dicha política o normativa establece qué se debe registrar quién realiza la actividad, cuándo la realiza y sobre qué información. Dispone de un procedimiento documentado relacionado con "[op.exp.2] Configuración de seguridad" en el que se detalla los mecanismos a utilizar para mantener el reloj del sistema en hora. Consultar si los mecanismos de registro almacenan esta información (p. ej.: la lectura por un humano de ese registro podría ser que el usuario user34 el 16-10-2010 a las 14:59:37 modificó la tupla 328 de la base de datos "trámites"). 1.3.- ¿Incluye la actividad de los operadores y administradores del sistema? Evidencia: Dicha política o normativa establece que se debe registrar la actividad de los operadores y administradores del sistema. Consultar si los mecanismos de registro almacenan los accesos a la configuración del sistema de forma que los propios operadores y administradores no puedan modificarlos. 1.4.- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados? Evidencia: Dicha política o normativa establece que se debe registrar tanto las actividades realizadas con éxito como los intentos fracasados. Consultar si los mecanismos de registro almacenan ambos.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 6-2: Almacenamiento de logs: Retención y protección Los logs se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis. Durante dicho periodo, el control de acceso garantiza que no se producen accesos no autorizados.	op.exp.10		**Nivel Alto** 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 del periodo de retención de los mismos, que establece además del periodo de retención de evidencias tras un incidente. El inventario de registros recoge el periodo de retención de los mismos. Dispone de un procedimiento documentado para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen). Consultar si la antigüedad de los registros concuerda con el periodo de retención establecido. 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]. Constatar que la fecha y hora de diversos sistemas, sobre todo de aquellos que generan o almacenan registros de actividad, es la correcta. 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. Consultar la lista de accesos autorizados y constatar que no hay ninguna incompatibilidad conforme a lo establecido en "[op.acc.3] Segregación de funciones y tareas". 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 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. Constatar que las medidas de seguridad aplicadas a las copias de seguridad cumplen lo indicado en dicha política o normativa.		☐ Documento: ☐ Muestreo: Observaciones:				

C4 - CBCS 6 Registro de la actividad de los usuarios (Mantenimiento, monitorización y análisis de los LOG de auditoría)

Objetivo de control: **Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 6-3: Centralización y revisión de logs Los logs de todos los sistemas son revisados periódicamente para detectar anomalías y posibles compromisos de la seguridad del sistema. Se dispone de mecanismos para la centralización de los logs de auditoría, de forma que se facilite la realización de las revisiones anteriores.	op.exp.8		Nivel Medio 1.- ¿Se revisan informalmente los registros de actividad en busca de patrones anormales? Evidencia: Dicha política o normativa establece que se debe revisar periódicamente los registros de actividad para detectar posibles acciones sospechosas o ilícitas. Consultar posibles resultados de estas revisiones informales. Prueba complementaria para evaluar este control: Aunque el objetivo final no es la centralización, esta estrategia facilita enormemente la realización de revisiones periódicas con un coste razonable. Por ello, considerar: 1.- ¿Se centralizan los logs generados en los diferentes sistemas? 1.1.- ¿Cómo? (volcado diario de los logs, reenvío de los logs al sistema central una vez escritos en el sistema original, escritura directa del log del sistema en el equipo centralizador de logs, etc.).		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 6-4: Monitorización y correlación La entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de logs para realizar correlación y análisis de logs.	op.exp.8		**Nivel Alto** 1.- ¿Se dispone de un sistema automático de recolección de registros y correlación de eventos? Evidencia: Dispone de una consola de seguridad centralizada que revise y centralice los registros de actividad automáticamente. Existen herramientas para analizar los registros en busca de actividades fuera de lo normal. Comprobar el resultado del análisis y posibles actividades inusuales.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C4- CBSC6	0 - Inexistente.

C5 Servicios Externos

Objetivo de control: **Gestionar la seguridad y el cumplimiento de los servicios externos**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
C.5.1.- Nivel de Cumplimiento del Servicio Se ha establecido el nivel de clumplimiento de los servicios externos	op.ext.1		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: 1.1.- ¿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. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de las características del servicio. 1.2.- ¿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. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de la calidad mínima exigida (acuerdo de nivel de servicio) y las consecuencias de su incumplimiento y posibles penalizaciones en su caso. 1.3.- ¿Las responsabilidades de las partes? Evidencia: Dicho procedimiento requiere también el establecimiento de las funciones o roles, obligaciones y responsabilidades de cada parte. Existe evidencia documental reconocida por el proveedor (p. ej.: contrato firmado por personal con capacidad de representación legal del proveedor) de las responsabilidades de las partes.		☐ Documento: ☐ Muestreo: Observaciones:				
C.5.2.- Gestión del Nivel de Cumplimiento del Servicio Se gestiona de manera continuada el nivel de cumplimiento de servicios externos	op.ext.2		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. El seguimiento requerido podría estar incluido en el contrato (informes a realizar, revisiones, monitorización...) 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]. Consultar si se ha detectado algún incumplimiento de las obligaciones de servicio y qué actuación se ha llevado a cabo. 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.). Consultar si se está cumpliendo el procedimiento. 4.- ¿Se han establecido el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres? Evidencia: El procedimiento de gestión de incidentes sobre el servicio externo estará relacionado con el definido en [op.exp.7]. Consultar si se está cumpliendo el procedimiento.		☐ Documento: ☐ Muestreo: Observaciones:				
C.5.3.- Requisitos de Seguridad de los Servicios Externos Se planifican y gestionan los requisitos de seguridad de las empresas externas contratadas para la provisión de servicios	NO		1.- ¿Se ha transmitido al proveedor de servicio sus obligaciones sobre la seguridad de los sistemas que proveen servicio a la administración? Evidencia: El contrato debe contener todas las clausulas relativas a los requisitos de seguridad de los sistemas para cumplir el ENS, de acuerdo a su clasificación, a la declaración de aplicabilidad y a lo expuesto en el Anexo II del ENS. Se ha aplicado el procedimiento de selección aprobado o correspondiente a la entidad para la adjudicación del contrato. El contrato contiene clausulas de confidencialidad y propiedad intelectual.		☐ Documento: ☐ Muestreo: Observaciones:				

C.5.4.- Gestión de la Seguridad de los Servicios de Cloud Se gestiona la seguridad de los servicios de Cloud mediante la correcta implantación de medidas de seguridad por parte del proveedor de servicio	NO		1.- ¿Se ha transmitido al proveedor de servicio sus obligaciones adicionales sobre la seguridad de los sistemas que proveen servicios de Cloud a la administración? Evidencia: El contrato debe contener todas clausulas relativas a los requisitos adicionales de seguridad de los servicios prestados mediente Cloud, particularmente los siguientes (CCN-STIC-823): - Los elementos virtualizados y los elementos de virtualización se tratarán igual que los elementos físicos correspondientes a efectos de configuración, mantenimiento, reglas de seguridad y aspectos regulatorios. - Las imágenes de los elementos virtuales se tratarán como datos con los mismos requisitos de seguridad que la información y los servicios manejados por dichos elementos virtuales. - Debe cumplir los requisitos de la norma CCN-STIC 811 relativa a interconexión, en función de la categoría del sistema propio y del otro lado de la interconexión. Nivel BAJO - Los componentes de seguridad del tipo DMZ, cortafuegos o agentes (proxy) no deberán residir en la misma máquina base que los componentes de producción. - El perímetro de la red física que soporte la comunidad cumplirá los requisitos de la guía CCN-STIC-811 relativa a puntos de interconexión. - Se registrarán todas las actuaciones de creación, traslado, activación y destrucción de elementos virtuales. Así mismo se registrará el montaje y la retirada de soportes de información, físicos o virtuales. - Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría MEDIA según el ENS. - Implicaciones (o ejemplos) - La red dedicada a usuarios ENS es una red físicamente diferenciada de otras redes que pueda tener el proveedor. - Si el usuario contrata una interconexión al proveedor, por ejemplo a Internet, el proveedor tendrá una máquina separada que preste los servicios de frontera. Nivel MEDIO - Además de los requisitos para Comunidad BAJA: - No se compartirán equipos base con otras comunidades. - No se compartirá el mismo hipervisor con otras comunidades. - La administración del hipervisor estará separada de la administración de los elementos virtualizados: diferentes interfaces, diferentes cuentas de administrador, y diferentes administradores. - Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría ALTA según el ENS. Nivel ALTO		☐ ☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C5	**0 - Inexistente.**

C6 Protección Frente a Malware

Objetivo de control: **Disponer de una adecuada política de protección contra el malware**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
C.6.1.- Protección Frente a Código Dañino La entidad implementa una adecuada protección frente a código dañino en servidores y puestos de trabajo	op.exp.6		1.- ¿Dispone de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y "malware" en general)? 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: Dispone de las recomendaciones del fabricante. Las opciones de configuración aplicadas son las recomendadas por el fabricante (p. ej.: análisis de ejecución de programas, análisis de correo entrante y saliente, bloqueo automático de código dañino, etc.), así como las referentes a frecuencia de actualización; en caso contrario está documentado el motivo. Comprobar la gestión ante posibles ataques, infecciones, etc… **Aspectos adicionales relacionados con este control:** 2. ¿Actualiza periodicamente la base de datos de firmas? ¿Con qué mecanismo y periodicidad? ¿Qué dispositivos se incluyen en la actualización periódica? Evidencia: Confirmar en el gestor del sistema si lo hubiera, o en equipos finales, la última actulización y la configuración de las actulizaciones automáticas. 3. ¿Tiene instaladas las funcionalidades del producto que proporcionan la protección necesaria? Evidencia: Confirmar en el gestor del sistema si lo hubiera, o en equipos finales, las funcionalidades habilitadas. 4. ¿Cómo protege a aquello equipos que no pueden instalar el software de protección corporativo? Evidencia: Consultar con el responsable la existencia de una lista de equipos que no disponen del software corporativo. Consultar la configuración de seguridad de una muestra de dichos equipos.		**Aplicación** ☐ Documento: ☐ Muestreo: Observaciones:				
C.6.2.- Protección de Correo Electrónico La entidad implementa una adecuada protección frente a código dañino en el servicio de correo electrónico	mp.s.1		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 y se protege, tanto en el cuerpo de los mensajes como en los anexos (relacionado con [mp.info.6] limpieza de documentos). Consultar que los correos electrónicos cumplen con el procedimiento. 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) relacionado con op.exp.6 Protección frente a código dañino? 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 antivirus 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. Constatar que se sigue la normativa. 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] concienciación y [mp.per.4] formación). Consultar los resultados de la ejecución del plan de formación y concienciación.		**Aplicación** ☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C6	0 - Inexistente.

C7 Protección de Instalaciones e Infraestructuras

Objetivo de control: **Gestionar adecuadamente la seguridad física de las instalaciones e infraestructuras**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
C.7.1.- Control de Accesos a Instalaciones Se realiza control de acceso a las instalaciones mediante identificación personal	mp.if.1		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 y constatar que cumplen la política o normativa. 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.). Examinar el acceso a dichas salas y constatar que cumplen la política o normativa.		☐ Documento: ☐ Muestreo: Observaciones:				
	mp.if.2		1.- ¿Se dispone de un mecanismo de control de acceso a los locales donde hay equipamiento que forme parte del sistema de información? Evidencia: Dispone de un mecanismo que establece un control de acceso a los locales especificados 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. Constatar este hecho solicitando acceso a los registros correspondientes. 1.2.- ¿Se registran las entradas y salidas de personas? Evidencia: Dicho procedimiento, que cumple los requisitos de la legislación vigente de tratamiento de datos de carácter personal, especifica que para cada persona debe quedar registrada inequívocamente junto con su fecha y hora de entrada y salida, así como la persona o mecanismo por el que se realiza el registro. Consultar el registro de accesos.		☐ Documento: ☐ Muestreo: Observaciones:				
C.7.2.- Infraestructura en CPD El CPD y centros de cableado disponen de infraestructura física adecuada para el despliegue de instalaciones	NO		1.- ¿Disponen los locales donde se ubican los sistemas de información y sus componentes de las infraestructuras físicas necesarias para su operación de forma segura y efectiva? Evidencia: Comprobar si la sala tiene falso suelo y falso techo. Verificar si las paredes llegan hasta el techo real o hasta las placas del falso techo. Si pasan cables por el interior de falso suelo/techo, constatar si existen detectores. Comprobar que se dispone de canalizaciones adecuadas para cada tipo de cableado, separando cableado electrico de cableado de comunicaciones la distancia adecuada según normativa		☐ Documento: ☐ Muestreo: Observaciones:				
C.7.3.- Acondicionamiento de Locales Los locales se encuentran adecuadamente acondicionados en cuanto a temperatura y	mp.if.3		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 elementos adecuados en el local para mantener las adecuadas condiciones de temperatura y humedad y que se encuentren en los márgenes especificados por los fabricantes de los equipos. Consultar si hay aire acondicionado, termómetro e higrómetro en el CPD, si se monitorizan de forma periódica y si se encuentran en los valores recomendados.		☐ Documento: ☐ Muestreo: Observaciones:				
C.7.4.- Suministro Eléctrico Los locales disponen de un adecuado suministro de energía electrica	mp.if.4		1.- ¿Se dispone de las tomas eléctricas necesarias? Evidencia: El local debe contar con las tomas eléctricas necesarias. Consultar que se cumple (p. ej.: enchufes con toma de tierra, cantidad de enchufes suficiente para no tener que recurrir a multiplicadores en cascada que superen la potencia eléctrica máximas recomendadas, etc.). 2.- ¿Se garantiza el suministro de potencia eléctrica? Evidencia: El local debe contar con la potencia eléctrica necesaria. Dispone de un análisis de la potencia eléctrica necesaria, que se actualiza antes de la adquisición de nuevos componentes. Consultar si el contrato de suministro cubre la potencia eléctrica necesaria. 3.- ¿Se garantiza el correcto funcionamiento de las luces de emergencia? Evidencia: El local debe contar con luces de emergencia y un mecanismo para comprobar el correcto funcionamiento de las luces de emergencia. Constatar que existen luces de emergencia. Existe evidencia documental de la revisión de las luces de emergencia. Nivel MEDIO 4.- ¿Se garantiza el suministro de potencia eléctrica en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información? Evidencia: El local debe contar con un sistema de alimentación ininterrumpida (compuesto por Sistema de Alimentación Ininterrumpida y, en caso de ser necesario, grupo electrógeno) para todo el sistema que garantice el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información. Consultar si el SAI cumple con los requisitos identificados en el análisis de la potencia eléctrica necesaria. Consultar los registros de las pruebas que se hayan llevado a cabo para constatar que el SAI soporta el tiempo necesario para la terminación ordenada. ¿Cada cuánto se realizan las pruebas? ¿Se realiza pruebas de carga o vacío? ¿Cada cuánto se cambian las baterías?		☐ Documento: ☐ Muestreo: Observaciones:				
C.7.5.- Protección Frente a Incendios Los locales disponen de medidas de protección frente a incendios	mp.if.5		1.- ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incendios fortuitos o deliberados? Evidencia: Los locales cuentan con protección frente a incendios conforme a la normativa industrial pertinente (p. ej.: disponer de carteles para evacuación, extintores, materiales no inflamables, etc.). Dispone de la normativa industrial pertinente y se encuentra aplicada.		☐ Documento: ☐ Muestreo: Observaciones:				

			Prueba adicional a realizar para evaluar este control: 2.- ¿Se encuentran los sistemas de detección y extinción de incendios comunicados con una central de alarmas? Evidencia: Confirmar que las alarmas generadas por el sistema anti-incendios son transmitidas y gestionadas. 3.- ¿Se han considerado criterios de protección pasiva frente a incendios en los locales donde se ubican los sistemas de información? ¿Se utiliza cableado libre de halogenos y no propagador de incendios? ¿Dispone el suelo y techo técnicos y la tabiquería de la adecuada protección contra incendios? Evidencia: Se dispone de la documentación técnica de los elementos constructivos del CPD, que disponen de clasificación anti-incendios.						
C.7.6.- Protección Frente a Inundaciones Los locales disponen de medidas de protección frente a inundaciones	mp.if.6		Nivel Medio 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: Los locales se protegen frente a incidentes fortuitos o deliberados causados por el agua (p. ej.: que el CPD no sea recorrido por tuberías de agua, que existan sumideros de agua en el CPD, etc.) conforme al nivel de riesgo identificado. Se ha realizado un estudio de la ubicación física del local para conocer el riesgo real de problemas por causa natural o por el entorno en 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.)		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C7	**0 - Inexistente.**

C8 Gestión de Incidentes

Objetivo de control: **Gestionar los incidentes para reducir su impacto**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
C.8.1.- Detección de Incidentes y Eventos de los Sistemas Se dispone de herramientas para la detección temprana de eventos e incidentes de	NO		1.- ¿Se dispone de herramientas que permitan gestión y detección temprana de incidentes de seguridad en los sistemas? Evidencia: La entidad dispone y explota un SIEM (Sistema de gestión eventos e información de seguridad) o una herramientas de monitorización de eventos en redes y sistemas (analizado en C9) que explota para la detección de incidentes de seguridad. 2. ¿Se disponde de personal asignado al tratamiento de los eventos detectados? Evidencia: La entidad dispone de personal asignado a la monitorización y revisión de eventos detectados y al inicio de los procedimientos de gestión de incidentes.		☐ Documento: ☐ Muestreo: Observaciones:				
C.8.2.- Gestión de Incidentes Se dispone de procedimientos para la gestión de incidentes de seguridad	op.exp.7		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 incidentes. Consultar incidentes de este tipo y, si no existe ninguno y ha pasado mucho tiempo desde que se implantó el procedimiento, consultar si se ha analizado el motivo por el que no se ha detectado ningún incidente (p. ej.: porque no se han producido incidentes de seguridad, o porque el personal desconoce el procedimiento y por lo tanto no los reporta, etc.). Respecto a dicho procedimiento: 1.1.- ¿Incluye el reporte tanto de incidentes, como de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación? Evidencia: Dicho procedimiento contempla el reporte tanto de incidentes como de eventos de seguridad como debilidades (p. ej.: aumento considerable de logs de error, ralentización del servicio, etc.), bien sean internos o provenientes de servicios prestados por terceras partes, así como el detalle del proceso de escalado de la notificación (p. ej.: un usuario final debe comunicar el incidente al centro de soporte, este analiza si es un incidente de seguridad, en cuyo caso lo reporta al técnico responsable de estos incidentes, etc.). Se dispone de sistemas de notificación automatizada de incidentes. Consultar si existen incidentes reportados de estos tipos y si se ha seguido el proceso de escalado de la notificación.		☐ Documento: ☐ Muestreo: Observaciones:				
C.8.3.- Respuesta ante Incidentes Se dispone de procedimientos para la toma de medidas y asignación de recursos durante la gestión de incidentes	op.exp.7		Respecto a dicho procedimiento: 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, y quién debe tomar esas decisiones. Como resultado de dicha valoración se contemplan las medidas a tomar entre las que se encuentran la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y la protección de los registros (según convenga). Consultar si se han tomado este tipo de medidas y si se ha cumplido el procedimiento. 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. Consultar si se han tomado este tipo de medidas y si se ha cumplido el procedimiento.		☐ Documento: ☐ Muestreo: Observaciones:				
C.8.4.- Comunicación de Incidentes Se dispone de procedimientos para recibir notificación de incidentes y reportar incidentes a las partes interesadas	op.exp.7		Respecto a dicho procedimiento: 1.1.- ¿Incluye el reporte tanto de incidentes, como de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación? Evidencia: Dicho procedimiento contempla el reporte tanto de incidentes como de eventos de seguridad como debilidades (p. ej.: aumento considerable de logs de error, ralentización del servicio, etc.), bien sean internos o provenientes de servicios prestados por terceras partes, así como el detalle del proceso de escalado de la notificación (p. ej.: un usuario final debe comunicar el incidente al centro de soporte, este analiza si es un incidente de seguridad, en cuyo caso lo reporta al técnico responsable de estos incidentes, etc.). Se dispone de sistemas de notificación automatizada de incidentes. Consultar si existen incidentes reportados de estos tipos y si se ha seguido el proceso de escalado de la notificación. 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 incidentes orientado al usuario final, de forma que este sepa identificar y resolver los incidentes más comunes. Consultar a un usuario final para constatar que conoce este procedimiento. 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 o tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados o que pudieran causar problemas similares en otras organizaciones, el procedimiento contempla la notificación de los mismos al CERT competente (al CCN-CERT en el caso de organismos del sector público de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categoría de los sistemas en cumplimiento del artículo 36 del ENS). Existe evidencia documental de que se tienen identificadas a las partes interesadas a avisar en caso de incidencia.		☐ Documento: ☐ Muestreo: Observaciones:				
C.8.5.- Prevención de Incidentes y Mejora Continua Se dispone de procedimientos para la mejora continua en la prevención y gestión de	op.exp.7		Respecto a dicho procedimiento: 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". Consultar si como resultado de un incidente se ha determinado que era necesario modificar un procedimiento para que no volviera a ocurrir y efectivamente se ha modificado el mismo. 1.7.- ¿Incluye el actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes? Evidencia: El procedimiento de gestión de incidentes contempla su revisión periódica o a raíz de la identificación de posibles mejoras en el mismo.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C7	0 - Inexistente.

C9 Monitorización

Objetivo de control: **Disponer de herramientas para la monitorización del sistema**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
C.9.1.- Herramienta de monitorización de redes y sistemas La entidad dispone de una herramienta de monitorización de redes	NO		1.- ¿Se dispone de herramientas que permitan la monitorización del estado de redes y sistemas? Evidencia: La entidad dispone y explota una herramienta o conjunto de herramientas que permite: -recibir información de los dispositivos y sistemas - conocer el estado actual de los sistemas - consultar datos históricos sobre el estado de los sistemas Existe personal asignado a la monitorización para la detección de incidentes o existen procedimientos o automatizaciones para el tratamiento de la información y alarmas generadas por el sistema de monitorización.		☐ Documento: ☐ Muestreo: Observaciones:				
C.9.2.- Linea Base de los Sistemas El sistema de monitorización de redes y sistemas permite establecer una línea base de utilización	NO		1.- ¿Proporciona la herramienta información adecuada para establecer una línea base de utilización que puede ser explotada por equipo de TI? Evidencia: La herramienta de monitorización que explota la entidad proporciona información sobra la linea base de funcionamiento, que permite al equipo de TI realizar: - detección de incidentes por comportamiento anómalo - planificación estrategica en base al perfil de utilización de los sistemas		☐ Documento: ☐ Muestreo: Observaciones:				
C.9.3.- Registro de Eventos El sistema de monitorización de redes y sistemas permite registrar, consultar y procesar los eventos detectados	NO		1.- ¿Proporciona la herramienta información sobre los eventos detectados en las redes y sistemas? Evidencia: La herramienta de monitorización que explota la entidad proporciona información sobre los eventos detectados y permite: - revisión de eventos para ejecución de mantenimiento preventivo - correlación eventos para identificar causa raiz - detección de incidentes de seguridad (control C8) - consulta de historicos para análisis forense de incidentes de seguridad Existe personal asinado a la explotación de la información generada por el sistema de monitorización o procedimientos o automatizaciones para el tratamiento de la misma.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control C9	0 - Inexistente.

D1 - CBCS 4 Uso controlado de privilegios administrativos

Objetivo de control: **Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 4-1 Inventario y control de cuentas de administración Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control.	op.acc.4		NOTA: Particularizar la revisión de este control a la gestión de los privilegios de administración. 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 usuario sólo se le proporcionarán los privilegios mínimos para cumplir sus obligaciones. Existe evidencia documental de cuáles son los privilegios que debe tener cada usuario en función de sus obligaciones. Constatar que la información de muestreo está accesible sólo a usuarios cuyos privilegios (obligaciones) coinciden con la anterior evidencia documental. 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: Dispone de evidencia documental en la que se relaciona quién es el responsable de los recursos, y en quién delega la responsabilidad de conceder, alterar o anular el acceso a los recursos (está asignada a personal concreto y no a todos o cualquiera en la organización). 3.- ¿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.: administración, dirección, sistemas, becario, etc.). ***Prueba complementaria para evaluar este control:*** ¿Dispone de un procedimiento que requiera inventariar las cuentas de administración? Evidencia 1: Procedimiento para inventariar las cuentas de administración. Debe contemplar tanto el alta, como la baja de dichas cuentas, sistemas/aplicaciones correspondientes y personal responsable de la cada una de las cuentas de administración. Evidencia 2: Solicitar el inventario de las cuentas de administración. Evidencia 3: Seleccionar una muestra de sistemas/aplicaciones, extraer el listado de usuarios y confirmar que las cuentas de administración son		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 4-2 Cambio de contraseñas por defecto Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema.	op.exp.2		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.: plantillas de seguridad y recomendaciones de bastionado del CCN. Existe evidencia documental (p. ej.: checklist) de la fortificación realizada a los sistemas, indicando la persona que lo realizó y la fecha y la versión del procedimiento que utilizó. Respecto a dicho procedimiento de bastionado: 1.1.- ¿Indica que se retiren las cuentas y contraseñas estándar? Evidencia 1: 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.). Obtener evidencias de la ejecución de este control. Nota: Para obtener evidencia de la ejecución de este control, posibles alternativas son:		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 4-3 Uso dedicado de cuentas de administración Las cuentas de administración sólo se realizan para las tareas que son estrictamente necesarias.	op.acc.1		1.- ¿Cada usuario que accede al sistema tiene asignado distintos identificadores únicos en función de cada uno de los roles que deba desempeñar en el sistema? Evidencia: Dispone de un procedimiento documentado para la creación de nuevos usuarios del sistema que especifica que deben crearse identificadores para cada rol de cada usuario (administración, consulta, invitado, etc.). Nota: Para obtener evidencia de la ejecución de este control, posibles alternativas son: Evidencia 1: Obtener el listado de personas que realiza labores de administración de los distintos sistemas (sistema operativo, base de datos, etc.) e identificar los identificadores de usuario correspondientes. Obtener el listado de usuarios de los sistemas administrados, para comprobar que en dichos sistemas están dados de alta las cuentas creadas para la administración. Evidencia: Existe el riesgo de que la persona sólo utilice la cuenta de administrador, incluso para hacer labores que no sean de administración. Para comprobar si esto es así, analizar la fecha de último acceso de las cuentas "normales" (que no disponen de elevados privilegios) del personal que administra.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 4-4 Mecanismos de autenticación Las cuentas de administración están sujetas a mecanismos de autenticación robustos, que impiden el acceso no	op.acc.5		1.- ¿Se encuentra identificado el mecanismo de autenticación en cada sistema? Evidencia: Dispone de un procedimiento para enumerar, de los sistemas previos a su puesta en explotación o ya en producción, el mecanismo de autenticación para los usuarios administradores (si la política de autenticación es diferente al resto de los usuarios del sistema), y se identifica el responsable de esta tarea. Existe un listado de sistemas que requieren autenticación y su mecanismo de autenticación correspondiente para los usuarios administradores. Respecto a las credenciales utilizadas: 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 al menos una determinada longitud marcada por la política de la entidad, que contengan caracteres alfabéticos y numéricos, que no sean de fácil conjetura (fechas significativas, números de teléfono, matrículas de coche, nombres de familiares o amigos, etc.), ni reutilizar contraseñas de servicios personales. El mecanismo de gestión de credenciales no permite utilizar contraseñas que no cumplan esta política (p. ej.: la política de contraseñas de Windows no permite crear claves que incumplan esta política). Parámetros de robustez a considerar: * Longitud mínima		☐ Documento: ☐ Muestreo: Observaciones:				

D1 - CBCS 4 Uso controlado de privilegios administrativos

Objetivo de control: **Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
autorizado mediante dichas cuentas.			* Vigencia máxima * Vigencia mínima * Uso de mayúsculas, minúsculas, números y caracteres especiales. * Histórico de contraseñas recordadas. Evidencia: Obtener captura/fichero de configuración donde se vean los parámetros anteriores para un subconjunto de los sistemas. 1.2.- ¿Se activa una vez que esté bajo el control efectivo del usuario? Evidencia: Dicha política o normativa establece que la cuenta del usuario no se habilita hasta que éste haya confirmado la recepción de la credencial. 1.3.- ¿Están las credenciales bajo el control exclusivo del usuario? (1) Evidencia: La política establece que las credenciales sólo las tiene el usuario (p. ej.: establece la responsabilidad del usuario de no compartir su credencial). En caso de tratarse de una contraseña, ésta sólo la conoce el usuario (p. ej.: la contraseña se almacena en el sistema de forma cifrada). 1.4.- ¿Ha confirmado el usuario que ha recibido las credenciales, y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida? Evidencia: Existe un registro de cada usuario confirmando la recepción de la credencial y en el mismo se le informa de esos aspectos. 1.5.- ¿Se cambian las credenciales con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)? Evidencia: Dispone de una política de seguridad documentada que especifica la periodicidad en el cambio de las credenciales. Existe evidencia del cambio de las credenciales dentro del periodo establecido en la política (p. ej.: la política de contraseñas de Windows obliga al cambio de credencial pasado el tiempo establecido, existe un histórico en el que se indica cuál fue la fecha del último cambio de la credencial de cada usuario y se encuentra dentro del tiempo establecido, etc.). 1.6.- ¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que autentican termina 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. (1) *Control compensatorio* Cuentas de administración: Estas cuentas pueden no cumplir los requisitos de uso compartido y que no se configure automáticamente el cambio de contraseña. a: Si son de uso compartido, revisar cómo se mantiene la trazabilidad de quién hace qué (por ej. uso de sudo, de la opción "run as", etc.). b: Debe existir un procedimiento para el cambio, de forma manual, de dichas contraseñas periódicamente. Examinar cómo se comunica la nueva contraseña a los administradores. Verificar la fecha de último cambio realizado. c: Debe existir un procedimiento que obligue a realizar el cambio cuando un administrador deja su puesto. Comprobar si se ha dado esta situación durante el periodo fiscalizado y verificar la coherencia de la fecha de cambio de contraseña.					
			Nivel Medio 2.- ¿Se utiliza doble factor de autenticación? Evidencia: Constatar que se emplea doble factor de autenticación: algo que se sabe (contraseñas o claves concertadas); algo que se tiene (certificados software, tokens físicos unipersonales, etc.); y/o algo que se es (elementos biométricos). 3.- Si utilizan contraseñas, ¿cumplen las políticas rigurosas de calidad y renovación? Evidencia 1: Dispone de una política o normativa documentada que aplica el recurso. Evidencia 2.- Comprobar los requisitos de complejidad (ver control anterior). *Controles compensatorios:* Si las contraseñas de administración no permiten el uso de doble factor, considerar mecanismos de control de acceso alternativos (ej. que no se pueda acceder en remoto, uso de máquinas de salto o ciertas estaciones (p.e. las consolas), etc.) 4.- ¿Las credenciales utilizadas han sido obtenidas tras un registro previo? Evidencia: Constatar que las credenciales han sido obtenidas de manera presencial, telemática mediante certificado electrónico cualificado o bien telemática mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.		☐ Documento: ☐ Muestreo: Observaciones:			
			Nivel alto 5.- ¿Se suspenden las credenciales tras un periodo definido de no utilización? Evidencia: Dispone de una política o normativa documentada para la revisión de credenciales que no se estén utilizando, en la que especifica el responsable y la periodicidad, igualmente ésta indica el periodo máximo de inactividad de una credencial antes de ser suspendido. Existe evidencia de la fecha de último uso de las credenciales. Respecto a los tokens:		☐ Documento: ☐ Muestreo: Observaciones:			

D1 - CBCS 4 Uso controlado de privilegios administrativos

Objetivo de control: **Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
			Respecto a los tokens: 6.- ¿El algoritmo está acreditado o certificado? Evidencia: Dispone de un procedimiento documentado para la adquisición de componentes hardware que empleen algoritmos acreditados por el Centro Criptológico Nacional. Existe evidencia documental de los algoritmos utilizados en los tokens, indicando que han sido acreditados por el CCN y si están certificados. 7.- ¿Las credenciales utilizadas han sido obtenidas tras un registro previo? Evidencia: Constatar que las credenciales han sido obtenidas de manera presencial o telemática mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.						
CBCS 4-5 Auditoría y control El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.	op.exp.8		1.- ¿Se registran todas las actividades de los usuarios en el sistema especialmente activando los registros de actividad en los servidores? Evidencia: Dispone de una política o normativa documentada que indica que se deben registrar todas las actividades de los usuarios en el sistema. Existen mecanismos para aplicar dicha política o normativa y dichos mecanismos están activados. Evidencia 2: Muestreo. Seleccionar una muestra de sistemas y comprobar que los registros de actividad son coherentes con lo definido en la política. Respecto a dichos registros: 1.1.- ¿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 ([op.pl.1]). 1.2.- ¿Indican quién realiza la actividad, ¿cuándo la realiza y sobre qué información, sea cual sea el usuario? Evidencia: Dicha política o normativa establece qué se debe registrar, quién realiza la actividad, cuándo la realiza y sobre qué información. Evidencia 2: 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 (preferiblemente disponer de dos o más fuentes). Evidencia 3: Muestreo. Seleccionar una muestra de sistemas y comprobar si los mecanismos de registro almacenan esta información. **1.3.- ¿Incluye la actividad de los operadores y administradores del sistema?** Evidencia: Dicha política o normativa establece que se debe registrar la actividad de los operadores y administradores del sistema. Evidencia 2: Muestreo. Seleccionar una muestra de sistemas y comprobar si los mecanismos de registro almacenan esta información. 1.3 b).- 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. 1.4.- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados? Evidencia: Dicha política o normativa establece que se debe registrar tanto las actividades realizadas con éxito como los intentos fracasados. Evidencia 2: Muestreo. Seleccionar una muestra de sistemas y comprobar si los mecanismos de registro almacenan ambos. **REVISIÓN PERIÓDICA (Nivel medio)** 1.- ¿Se revisan informalmente los registros de actividad en busca de patrones anormales? Evidencia: Dicha política o normativa establece que se debe revisar periódicamente los registros de actividad para detectar posibles acciones sospechosas o ilícitas. Consultar posibles resultados de estas revisiones informales. **ALERTA en TIEMPO REAL (Nivel alto)** 1.- ¿Se dispone de un sistema automático de recolección de registros y correlación de eventos? Evidencia: Dispone de una consola de seguridad centralizada que revise y centralice los registros de actividad automáticamente. Existen herramientas para analizar los registros en busca de actividades fuera de lo normal. Comprobar el resultado del análisis y posibles actividades inusuales.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control D1 - CBCS4	0 - Inexistente.

D2 Mecanismos de Identificación y Autenticación

Objetivo de control: **Disponer de mecanismos que permitan la identificación segura de los usuarios de los sistemas**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
D.2.1.- Procedimiento de Identificación y Autenticación de Usuarios La entidad dispone de un procedimiento de gestión que contempla los mecanismos de identificación y autenticación de	NO		**Prueba adicional a realizar para evaluar este control:** 1.- ¿Dispone la entidad de un procedimiento que contemple los mecanismos para la identificación y autenticación de usuarios? Evidencia: La entidad dispone de un procedimiento que contempla los mecanismo existentes para la identificación de usuarios.		☐ Documento: ☐ Muestreo: Observaciones:				
D.2.2.- Identificación de Usuarios Se utiliza la identificación singular de usuarios para gestionar el acceso a los sistemas	op.acc.1		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.: administración, dirección, sistemas, becario, etc.). Respecto a dicho identificador: 1.1.- ¿Cada usuario que accede al sistema tiene asignado distintos identificadores únicos en función de cada uno de los roles que deba desempeñar en el sistema? Evidencia: Dispone de un procedimiento documentado para la creación de nuevos usuarios del sistema que especifica que deben crearse identificadores para cada rol de cada usuario (administración, consulta, invitado, etc.). 1.2.- ¿Se puede saber a quién corresponde? Evidencia: Dicho procedimiento contempla el mantener un registro de las entidades responsables de cada identificador Existe una relación de los identificadores con sus usuarios (p. ej.: el identificador "webmaster" es de Jorge Pérez, pertenece al grupo "web" y tiene por lo tanto permisos de lectura y escritura en la carpeta \web y de lectura en la carpeta \ftp). 1.3.- ¿Se puede saber qué derechos tiene? Evidencia: Dicho procedimiento contempla el mantener un registro de los derechos de cada entidad. Existe una relación de los identificadores con sus permisos (p. ej.: el identificador "webmaster" pertenece al grupo "web" y tiene por lo tanto permisos de lectura y escritura en la carpeta \web y de lectura en la carpeta \ftp). 1.4.- ¿Se inhabilita el identificador cuando el usuario deja la organización, cesa en la función para la cual se requería la cuenta de usuario o cuando la persona que la autorizó da orden en sentido contrario? 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. 1.5.- ¿El identificador se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas? Evidencia: Dispone de un procedimiento documentado que identifica el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad, procedimiento que indica que debe llevarse a cabo en los sistemas previos a su puesta en explotación o ya en producción, lo que se debe hacer una vez pasado dicho periodo y quién debe hacer cada tarea del procedimiento (p. ej.: cuando un empleado deja la organización, su usuario se bloquea durante el tiempo establecido en la política de retención, y no es hasta pasado ese plazo cuando dicho usuario puede eliminarse del sistema). Existe evidencia documental del periodo necesario para atender a las necesidades de trazabilidad de los registros. Tomando un sistema (el muestreo puede ser mayor según se estime conveniente), se analizará cuál es el periodo de retención establecido y se buscarán identificadores que han sido inhabilitados dentro y fuera del periodo de retención, para constatar que se ha procedido conforme al procedimiento. 2.- ¿El nivel de la dimensión de autenticidad del mecanismo de autenticación de los sistemas de información a los que se accede se corresponde con el nivel de seguridad de los sistemas de identificación electrónica? Evidencia: Existe una correspondencia entre el nivel de autenticidad definido y el nivel de seguridad equivalente de acuerdo al artículo 8 del		☐ Documento: ☐ Muestreo: Observaciones:				

D.2.3.- Auntenticación de Usuarios Se dispone de mecanismos para la autenticación de las identificaciónes	op.acc.5		1.- ¿Se encuentra identificado el mecanismo de autenticación en cada sistema? Evidencia: Dispone de un procedimiento para enumerar, de los sistemas previos a su puesta en explotación o ya en producción, el mecanismo de autenticación, y se identifica el responsable de esta tarea. Existe un listado de sistemas que requieren autenticación y su mecanismo de autenticación correspondiente (p. ej.: la intranet requiere autenticación mediante usuario y contraseña, el correo electrónico requiere autenticación mediante usuario y contraseña). Respecto a las credenciales utilizadas: 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 al menos una determinada longitud marcada por la política de la entidad, que contengan caracteres alfabéticos y numéricos, que no sean de fácil conjetura (fechas significativas, números de teléfono, matrículas de coche, nombres de familiares o amigos, etc.), ni reutilizar contraseñas de servicios personales. El mecanismo de gestión de credenciales no permite utilizar contraseñas que no cumplan esta política (p. ej.: la política de contraseñas de Windows no permite crear claves que incumplan esta política). 1.2.- ¿Se activa una vez que esté bajo el control efectivo del usuario? Evidencia: Dicha política o normativa establece que la cuenta del usuario no se habilita hasta que éste haya confirmado la recepción de la credencial. 1.3.- ¿Están las credenciales bajo el control exclusivo del usuario? Evidencia: Dicha política o normativa establece que las credenciales sólo las tiene el usuario (p. ej.: establece la responsabilidad del usuario de no compartir su credencial). En caso de tratarse de una contraseña, ésta sólo la conoce el usuario (p. ej.: la contraseña se almacena en el sistema de forma cifrada). 1.4.- ¿Ha confirmado el usuario que ha recibido las credenciales, y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida? Evidencia: Existe un registro de cada usuario confirmando la recepción de la credencial y en el mismo se le informa de esos aspectos. 1.5.- ¿Se cambian las credenciales con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)? Evidencia: Dispone de una política de seguridad documentada que especifica la periodicidad en el cambio de las credenciales. Existe evidencia del cambio de las credenciales dentro del periodo establecido en la política (p. ej.: la política de contraseñas de Windows obliga al cambio de credencial pasado el tiempo establecido, existe un histórico en el que se indica cuál fue la fecha del último cambio de la credencial de cada usuario y se encuentra dentro del tiempo establecido, etc.). 1.6.- ¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que autentican termina 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. Nivel Medio 2.- ¿Se utiliza doble factor de autenticación? [illegible]		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control D2	**0 - Inexistente.**

D3 Gestión de Derechos de Acceso

Objetivo de control: **Gestionar y limitar el eso de recursos de los sistemas a los usuarios**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
D.3.1.- Procedimiento de Gestión de Derechos de Acceso La entidad dispone de un procedimiento que contempla la gestión de derechos de acceso a los	NO		1.- ¿Dispone la entidad de un procedimiento que contemple los mecanismos para la gestión de derechos de acceso de los usuarios a los sistemas? Evidencia: La entidad dispone de un procedimento que contempla los procesos implantados para la gestión de los derechos de acceso a los sistemas.		☐ Documento: ☐ Muestreo: Observaciones:				
D.3.2.- Mecanismos de Control de los Accesos Los sistemas cuentan con mecanismos de control de acceso que requieren de la identificación y autenticación de los usuarios	op.acc.2		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: El sistema antes de su puesta en explotación o ya en producción, cuenta con un mecanismo de control de acceso. Para acceder a cualquier recurso es necesario estar identificado 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). 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 especifican quién es el responsable de cada recurso y, por lo tanto, es también responsable de la asignación de autorización y nivel de acceso a cada recurso. Constatar que los derechos de acceso coinciden con los establecidos en la política o normativa. 3.- ¿Incluye el mecanismo la protección frente al acceso a los componentes del sistema y a sus ficheros o registros de configuración? Evidencia: Dispone de evidencia documental (manual de administración, documento desarrollado internamente, etc.) donde se especifica cuáles son los componentes del sistema y sus ficheros o registros de configuración, así como los permisos de usuario que deben establecerse de forma que sólo los usuarios autorizados tengan acceso. Constatar que el acceso a los ficheros de configuración del sistema sólo está autorizado al personal técnico.		☐ Documento: ☐ Muestreo: Observaciones:				
	op.acc.6		1.- ¿Se previene la revelación de información del sistema? Evidencia: Dispone de un mecanismo para que los sistemas antes de entrar en explotación o los ya existentes sean configurados de forma que no revelen información del sistema antes de un acceso autorizado. Los diálogos de acceso (al puesto local dentro de la propia instalación de la organización, 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: Dispone de una política o normativa documentada que especifica que se deben registrar tanto los accesos con éxito como fallidos. Comprobar que el sistema de registro 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: Dispone de una política o normativa documentada que especifica que se debe informar al usuario de sus obligaciones inmediatamente después de obtener el acceso. Una vez habiendo accedido con éxito al sistema, éste muestra un aviso con las obligaciones del usuario. Nivel MEDIO 5.- ¿Informa el sistema al usuario del último acceso con su identidad con éxito? Evidencia: Dispone de un mecanismo que especifica que se debe informar al usuario del último acceso con su identidad con éxito, una vez habiendo obtenido acceso. Una vez habiendo accedido con éxito al sistema, éste muestra la fecha y hora del último acceso con éxito de ese usuario. Nivel ALTO 6.- ¿Se limita el horario, fechas y lugar desde donde se accede? Evidencia: Dispone de un mecanismo que indica el horario, fechas y lugar desde donde está autorizado el acceso. Existen mecanismos para aplicar dicha política o normativa. Comprobar si hay algún registro de acceso con éxito que incumpla 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 un mecanismo que indica los puntos en los que el sistema requerirá una renovación de la autenticación del usuario. Verificar que esto se produce (p. ej.: se reutilizan automáticamente las credenciales de inicio de sesión en el PC para el acceso a la intranet, pero para acceder a la información de la nómina en la intranet vuelve a pedir las credenciales).		☐ Documento: ☐ Muestreo: Observaciones:				
	op.acc.7		1.- ¿Se garantiza la seguridad del sistema cuando acceden remotamente usuarios u otras entidades? Evidencia: Dispone de una política o normativa documentada que especifica que los accesos realizados fuera de las propias instalaciones de la organización, a través de redes de terceros, deben cumplir los requisitos de las medidas [op.acc.6] y [mp.com.3]. Nivel MEDIO 2.- ¿Está documentado lo que puede hacerse remotamente? Evidencia: Dispone de una política o normativa documentada que regula las actividades que pueden realizarse remotamente. 3.- ¿Se han autorizado previamente los accesos remotos? Evidencia: Dispone de una política o normativa documentada que especifica que los accesos remotos deben ser autorizados previamente, indicando la persona que puede autorizar el acceso. Existe evidencia documental de los accesos autorizados, por quién y durante qué periodo.		☐ Documento: ☐ Muestreo: Observaciones:				

D.3.3.- Principio para la Asignación de Derechos de Acceso El derecho al acceso a los recursos del sistema se proporciona exclusivamente en base a los principios de Least Privilege y la necesidad de conocer	op.acc.4		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 usuario sólo se le proporcionarán los privilegios mínimos para cumplir sus obligaciones (p. ej.: un usuario encargado de las altas de nuevos trámites y que no tiene responsabilidad sobre la gestión de dichos trámites no debe ser capaz de acceder a la gestión de los mismos). Existe evidencia documental de cuáles son los privilegios que debe tener cada usuario en función de sus obligaciones. Constatar que la información de muestreo está accesible sólo a usuarios cuyos privilegios (obligaciones) coinciden con la anterior evidencia documental. 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: Dispone de evidencia documental en la que se relaciona quién es el responsable de los recursos, y en quién delega la responsabilidad de conceder, alterar o anular el acceso a los recursos (está asignada a personal concreto y no a todos o cualquiera en la organización).		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control D3	**0 - Inexistente.**

D4 Gestión de Usuarios

Objetivo de control:	Gestionar los usuarios y sus responsabilidades para realizar una correcta provisión de derechos de acceso

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
D.4.1.- Procedimiento de Gestión de Usuarios La entidad dispone de un procedimiento para la gestión de los usuarios de los sistemas	NO		1. ¿Dispone la entidad de un procedimiento para la gestión de los usuarios los sistemas? Evidencia: La entidad dispone de un procedimiento que contempla la gestión de los usuarios de los sistemas y detalla como mínimo la gestión de altas, bajas, tipología de usuarios y procedimientos de control		☐ Documento: ☐ Muestreo: Observaciones:				
D.4.2.- Definición de Puestos de Trabajo Definición de los puestos de trabajo para establecer los requisitos de acceso de los usuarios	mp.per.1		Nivel MEDIO 1.- ¿Se ha caracterizado cada puesto de trabajo? Evidencia: Dispone de una política o normativa documentada que contiene 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. Revisar la relación de personas asignadas a cada tipo de 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 y comprobar que concuerdan.		☐ Documento: ☐ Muestreo: Observaciones:				
D.4.3.- Gestión Continuada de los Derechos de los Usuarios Gestión continuada de los usuarios de los sistemas para verificar la correcta asignación de derechos de acceso de acuerdo a sus responsabilidades	NO		1.- ¿Realiza la entidad la gestión de los usuarios del sistema y sus privilegios de acuerdo a sus obligaciones y responsabilidades? Evidencia: 1.Lista de recursos que incluya las aplicaciones que, si no se protegen, puedan afectar a la precisión de los estados financieros o la tramitación de los procesos críticos de negocio. Se comprueba que el acceso a esos recursos es el apropiado en base a las funciones del puesto de trabajo. 2.Procedimientos para la administración de usuarios (altas, bajas, permisos). Comunicación de usuario y contraseña. 3.Lista de usuarios. Comparar con la relación de trabajadores de la entidad y verificar que las discrepancias son razonables y corresponden a necesidades del funcionamiento de la entidad. 4.Altas de usuarios. Obtener una lista de usuarios añadidos durante el periodo de auditoría y determinar si está completo. Seleccionar una muestra de usuarios y comprobar si se rellenó y autorizó un formulario de solicitud de alta del usuario, si se aprobaron sus permisos de acceso y que los permisos fueron establecidos de forma adecuada según las funciones del usuario 5.Comprobación periódica de usuarios: Si existe un procedimiento de revisión de usuarios activos, comprobar que es adecuado. Si no existe tal procedimiento, obtener una lista de empleados que ya no se encontraban en la organización durante el periodo de auditoría, comprobar que está completo y que se eliminaron sus accesos al sistema. Comprobar si hay usuarios que cambiaron de departamento y que sus permisos se modificaron o desactivaron para adecuarse nuevo puesto de trabajo. 6.Listado actualizado de roles o perfiles en el sistema, así como los usuarios asociados a cada uno de ellos. Escoger una muestra y verificar que la asignación a sus perfiles ha sido autorizada y es la correcta de acuerdo a sus funciones.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control D4	0 - Inexistente.

D5 Protección de Redes y Comunicaciones

Objetivo de control:

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
D.5.1.- Protección por Firewall La entidad dispone de protección por Firewall y se encuentra correctamente configurado y mantenido	mp.com.1		1.- ¿Dispone de cortafuegos que separe la red interna del exterior? Evidencia: Dispone de un perímetro concreto, delimitado y acotado, reflejado en la arquitectura del sistema ([op.pl.2]). Todo el tráfico con el exterior pasa a través del cortafuegos. Sólo se permite el tráfico que ha sido previamente autorizado. Ver el firewall y el esquema de red.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 1.- ¿Ofrece la solución de firewall por arquitectura y tecnología el nivel de seguridad requerido? Evidencia: La solución de firewall implementada ofrece funcionalidades propias del tipo NGFW (Next Generation Firewall) o UTM (Unified Threat Management): -IDS -IPS -DPI (Deep Packet Inspection) -Application Inspection -DLP (Data Leak Prevention) -Inspección de tráfico encriptado 2.- ¿Se mantiene adecuadamente actualizado el firewall en cuanto a firmas y otra información de terceros para el procesado de seguridad? Evidencia: La solución realiza la carga periodica de información por parte del fabricante.		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.2.- Arquitectura de Red La entidad ha implementado un diseño seguro de la arquitectura de red	mp.com.1		Respecto a dicho cortafuegos: 1.1.- ¿El sistema de cortafuegos consta de dos o más equipos de diferente fabricante dispuestos en cascada? Evidencia: Se cuenta con dos o más equipos de diferente fabricante dispuestos en cascada. Ver los firewalls y el esquema de red. 1.2.- ¿Se dispone de sistemas redundantes? Evidencia: Los firewalls deben ser redundantes. Ver la configuración de los firewalls.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: 2.- ¿Se ha realizado un diseño adecuado de la arquitectura de la solución para proporcionar el nivel de seguiridad requerido? Evidencia: Se ha implementado una DMZ mediante el uso de firewalls en cascada.		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.3.- Conexiones Exteriores Seguras Se utilizan conexiones seguras para conexiónes desde el exterior de la entidad	mp.com.2		**Nivel MEDIO** 1.- ¿Se emplean redes privadas virtuales (VPN3) cuando la comunicación discurre por redes fuera del propio dominio de seguridad? Evidencia: Las comunicaciones que discurren por redes fuera del propio dominio de seguridad utilizan VPN con métodos criptográficos que garanticen la confidencialidad de la información transmitida. La protección de la clave de cifrado cumple [op.exp.11]. Consultar el mecanismo VPN utilizado. Consultar el listado de personal con acceso a las VPN (Altas, bajas y modificaciones en su caso) Respecto a esas VPN: 1.1.- ¿Emplean algoritmos acreditados por el CCN? Evidencia: Dispone de un inventario de algoritmos criptográficos empleados. Los algoritmos criptográficos han sido acreditados por el CCN. **Nivel ALTO** 1.2.- ¿Se emplean preferentemente dispositivos hardware en el establecimiento y utilización de la VPN? Evidencia: Uso de dispositivos hardware en el establecimiento y utilización de la VPN. En caso de no utilización de dispositivos hardware debe estar debidamente acreditado y aprobado por el responsable. Consultar si se utilizan dispositivos hardware o, en caso contrario, si está aprobado por el responsable. 1.3.- ¿Se emplean productos certificados? Evidencia: Uso de productos certificados (en relación con [op.pl.5] componentes certificados). Consultar si se utilizan productos certificados.		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.4.- Segmentación de Redes Las redes se encuentran segmentadas	mp.com.4		1.- ¿Se encuentra la red segmentada? Evidencia: Se dispone de un mecanismo para que la red se encuentre segmentada. Dispone de segmentos concretos, delimitados y acotados, reflejados en la arquitectura del sistema ([op.pl.2]), bien sean físicos o lógicos. Sólo se permite el tráfico entre segmentos que ha sido previamente autorizado. Respecto a dichos segmentos: 1.1.- ¿Existe control de entrada de los usuarios que llegan a cada segmento? Evidencia: Se establece el control de entrada de los usuarios que llegan a cada segmento. Dispone de un inventario de los usuarios que llegan a cada segmento. 1.2.- ¿Existe control de salida de la información disponible en cada segmento? Evidencia: Se establece el control de salida de la información en cada segmento. Dispone de control de salida de la información disponible en cada segmento. 1.3.- ¿Está el punto de interconexión particularmente asegurado, mantenido y monitorizado? Evidencia: Esta particularmente asegurado, mantenimiento y monitorización del punto de interconexión entre segmentos como en [mp.com.1]perímetro seguro.		☐ Documento: ☐ Muestreo: Observaciones:				

D.5.5.- Mecanismos de Identificación y Autenticación para Gestión de Red Se usan configuraciónes seguras para gestionar la identificación y autenticación en la gestión de la electrónica de red	NO		1.- ¿Se utilizan configuraciones seguras para la identificación y autenticación de administradores de los sistemas de comunicaciones y electrónica de red? Evidencia: Se han implementado mecanismos de conexión seguros, como SSH, evitando el uso de telnet. Se han implementado mecanismos de encriptación de contraseñas en la configuración de los equipos de comunicaciones. Se han implementado mecanismos de autenticación basados en el uso de sevidores de autenticación, utilizando protocolos de autenticación como RADIUS o TACACS		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.6.- Gestión segura de Logs y Notificaciones Se usan configs seguras para gestionar los logs y notificaciones	NO		1.- ¿Se implementan configuraciones seguras para gestionar los eventos y notificaciones del los sistemas de comunicaciones? Evidencia: Los equipos de comunicaciones y electrónica de red no almacenan únicamente en local la información de eventos genrada, utilizando un repositorio externo para ello. Se utilizan protocolos seguros para la comunicación de eventos y notificaciones, tales como SNMPv3, evitando el uso de protocolos obsoletos como SNMPv1 o SNMPv2.		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.7.- Configuraciones por Defecto y Automáticas No se utilizan configs por defecto o automáticas	NO		1.- ¿Se utiliza en el equipamiento de comunicaciones y electrónica de red configuraciones automática? Evidencia: La electrónica de red NO gestiona automaticamente sus configuraciones mediante el uso de técnicas como: -Configuración dinámica de trunks. Mediante protocolos como DTP (Dynamic Trunking Protocol de CISCO) -Configuración dinámica de vlans. Mediante protocolos como VTP (VLAN Trunking Protocol de CISCO) -Configuración dinámica de Etherchannel. Mediante protocolos como Pgap o LACP. ¿Se utiliza en el equipamiento de comunicaciones y electrónica de red configuraciones por defecto? Evidencia: -La electrónica de red no utiliza para el tráfico de datos la vlan 1, que permanece no tagueada en los trunks. -Los puertos de la electrónica de red no se mantienen habilitados por defecto. -El servidor web embebido en la electrónica de red se encuentra deshabilitado. -La conexión a la electrónica de red mediante protocolo telnet se encuentra deshabilitada. -El servidor FTP embebido en la electrónica de red se encuentra deshabilitado. -La comunity string por defecto de SNMPv1 y v3 se han modificado y se ha dehabilitado el uso de versiones anteriores a SNMPv3. -Se ha modificado el prompt por defecto.		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.8.- Mecanismos contra Ataques en Red de Área Local Se configuran mecanismos de seguridad ante ataques en la Red de Área Local intencionados o involuntarios	NO		1.- ¿Se utilizan mecanismos de seguridad para evitar ataques en la red de área local? Evidencia: La electrónica de red implementa mecanismos para evitar ataques o incidentes de seguridad intencionados o involuntarios. Por ejemplo mediante el uso en electrónica CISCO de configuraciones como: -DHCP snooping -DAI (Dynamic Arp Inspection) -Bpduguard -Rootguard -Sourceguard -Stormcontrol		☐ Documento: ☐ Muestreo: Observaciones:				
D.5.9.- Control de Acceso a los Recursos de Red Se utilizan configuraciones para limitar los accesos a los recursos de la red	NO		1.- ¿Se utilizan mecanismos para limitar el acceso a recursos de la red? Evidencia: -Se aplica la colección de medidas incluidas en CBCS 1-2. -La electrónica de red implementa 802.1X para autenticar el acceso a la red. -La comunicaciones de las actualizaciones de protocolos de routing dinámico como OSPF utiliza mecanismos de autenticación. -La comunicaciones de las actualizaciones de protocolos de alta disponibilidad como HSRP o VRRP utiliza mecanismos de autenticación.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control D5	**0 - Inexistente.**

E1 - CBCS 7 Copia de seguridad de datos y sistemas

Objetivo de control: **Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
CBCS 7-1: Realización de copias de seguridad La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.	mp.info.9		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, el periodo de retención durante el que mantenerlas, realización y eliminación de los backups. Dispone de mecanismos de backup (p. ej.: unidad de cinta, cintas, disco duro para almacenamiento de copias, aplicación de backup, etc.) y de eliminación segura (p. ej.: software de eliminación segura, desmagnetizador, etc.). Consultar que los backups existen y se realizan conforme al procedimiento. 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. Constatar que los backups almacenan esta información. 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] gestión de la configuración, [op.exp.4] Mantenimiento y [op.exp.5] gestión de cambios. Constatar que los backups almacenan esta información. 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 inventario de activos], [op.exp.2] configuración de la seguridad, [op.exp.3] gestión de la configuración, [op.exp.4] Mantenimiento y [op.exp.5] gestión de cambios. Constatar que los backups almacenan esta información. 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]Protección de claves criptológicas y [mp.info.3] cifrado. Constatar que los backups almacenan esta información.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 7-2: Realización de pruebas de recuperación Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.	mp.info.9		1.- ¿Realizan pruebas de recuperación a partir de las copias de respaldo realizadas? ¿Se documenta las pruebas de recuperación realizadas? Evidencia 1: Dispone de un procedimiento documentado en el que se determina la frecuencia con la que deben realizarse las pruebas de recuperación y el alcance de dichas pruebas. Evidencia 2: Comprobar la efectiva realización de dichas pruebas, según la frecuencia y el alcance definidos en el procedimiento.		☐ Documento: ☐ Muestreo: Observaciones:				
CBCS 7-3: Protección de las copias de seguridad Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.	mp.info.9		1.- ¿Las copias de seguridad 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] control de accesos, [op.exp.9] registro de la gestión de incidentes y [op.exp.10]protección de los registros de actividad y, en caso de utilizar cifrado, con [op.exp.11 Protección de claves criptológicas]. Constatar que las medidas de seguridad son las pertinentes. 2.- 2.- ¿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. Consultar las últimas restauraciones de información y constatar que han sido autorizadas por su responsable. NOTA: A la hora de revisar este control, prestar especial atención a las medidas de seguridad aplicadas en el caso de que las copias estén externalizadas y/o se utilicen servicios en la nube. ***Prueba adicional para evaluar este control:*** 1.- ¿Las copias de seguridad están accesibles de forma directa a nivel de red? 2.- ¿Se dispone de una copia de seguridad en offline? ¿Cómo y con qué frecuencia se realiza? En caso contrario, evaluar otras posibles medidas de protección. Evidencia: Procedimiento de realización de copias de seguridad, en el que se detallen los soportes utilizados para almacenar la copia y si se dispone de datos en offline. Verificar la existencia de dichas copias.		☐ Documento: ☐ Muestreo: Observaciones:				

E1 - CBCS 7 Copia de seguridad de datos y sistemas

Objetivo de control: **Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
Valoración global del control E1 - CBCS7					**0 - Inexistente.**				

E2 Plan de Continuidad

Objetivo de control: **Disponer de un Plan de Continuidad o de medidas que permitan el restablecimiento de los servicios**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
E.2.1.- Identificación de Elementos Críticos del Negocio Se ha realizado un Análisis de Impacto en la Actividad (BIA) para identificar los elementos críticos del negocio	op.cont.1		1.- ¿Se ha realizado un análisis de impacto? Evidencia: Dispone de un mecanismo para el análisis de impacto de una contingencia en la continuidad del servicio, este contempla el responsable del mismo, su revisión periódica o actualización tras cambios en los sistemas (ligado a [op.exp.3], [op.exp.4] y [op.exp.5]). En caso de que el mecanismos se refleje en un procedimiento documentado consultar el último análisis de impacto, así como el hecho que haya motivado su 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.		☐ Documento: ☐ Muestreo: Observaciones:				
E.2.2.- Plan de Continuidad de la Actividad Se dispone de un Plan de Continuidad o se han implantado medidas que permitan el restablecimiento de los servicios	op.cont.2		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? Evidencia: Dicho plan define quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y evaluar las consecuencias, quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis y quiénes se encargan de reconstruir el sistema de información (recuperación del desastre), definiendo para cada función las actividades a realizar. Estas funciones no son incompatibles según [op.acc.3], o en caso de serlo está motivado y aprobado por la Dirección. En caso de que las funciones se hayan asignado a roles, existe un documento que permite identificar los roles con las personas nominales. Las personas aceptan formalmente sus obligaciones en el plan. 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]). En caso de que el plan cuente con disponer de medios alternativos, consultar si se dispone de los medios alternativos (p. ej.: servidor de sustitución, switch de sustitución, CPD alternativo, etc.). 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.		☐ Documento: ☐ Muestreo: Observaciones:				
E.2.3.- Pruebas del Plan de Continuidad de la Actividad Se realizan pruebas periodicas de PCN o de las medidas de continuidad implementadas	op.cont.3		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 y, si se han identificado acciones de mejora, que las mismas se hayan ejecutado.		☐ Documento: ☐ Muestreo: Observaciones:				
			Prueba adicional a realizar para evaluar este control: ¿Se establece formalmente la periodicidad y alcance de las pruebas del PCN y se cumple dicho compromiso? Evidencia: -Se estipula formalmente (en el PCN o en la Política de Seguridad) la periodicidad de las pruebas del PCN. -Se estipula formalmente (en el PCN o en la Política de Seguridad) el alcance de las pruebas PCN. -Para el periodo de tiempo auditado, se dispone de documentación que acredita la realización de pruebas de acuerdo a la periodicidad y alcance establecidos y detalla el resultado de las mismas y la relación de posibles soluciones a las incidencias detectadas		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control E2	**0 - Inexistente.**

E3 Alta Disponibilidad

Objetivo de control: **Considerar la alta disponinilidad como requisito de los sistemas criticos**

Subcontrol	ENS	Descripción del control implantado en la Entidad	Pruebas a realizar y posibles evidencias a obtener	Resultado de la Auditoría del ENS	Resultado de la revisión	Valoración del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
E.2.1.- Diseño enfocado a la Alta Disponibilidad Se considera la alta disponibilidad en los criterios de diseño adquisición e implementación de los sistemas críticos	NO		**Prueba adicional a realizar para evaluar este control:** ¿Se establece la alta disponibilidad como criterio en los procesos de diseño, adquisición e implementación de los sistemas? Evidencia: La alta disponibilidad se encuentra contemplada en los procedimientos para la compra y el desarrollo de sistemas. Para el periodo auditado, verificar los estudios previos a la adquisición o desarrollo de los sistemas y verificar que la alta disponibilidad es un criterio de diseño.		☐ Documento: ☐ Muestreo: Observaciones:				
E.2.2.- Ubicaciones Redundantes Se dispone de ubicaciones redundantes para el CPD y locales clave para la provisión de los servicios	mp.if.9		1.- ¿Está garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles? Evidencia: Consultar la existencia de las instalaciones alternativas (p. ej.: contrato con un proveedor de instalaciones alternativas disponibles en el plazo previsto en el "[op.cont.2] Plan de continuidad").		☐ Documento: ☐ Muestreo: Observaciones:				
E.2.3.- Elementos Redundantes de Sistemas Críticos Los sistemas criticos disponen de elementos redundantes para proporcionador el requirido nivel de disponibilidad del servicio	NO		**Prueba adicional a realizar para evaluar este control:** ¿Se dispone de redundancia de elementos y componentes en los sistemas críticos de la entidad de manera que proporcionen un nivel alto de sisponibilidad? Evidencia: -El servicio eléctrico en elementos críticos de los sistemas se encuentra redundado con doble acometida independiente, tales como CPDs o centros de cableado principales. -Los enlaces de comunicaciones que proporcionan servicio a elementos críticos de la red se encuentran redundados y discurren por caminos y canalizaciones independientes. -Los equipos de comunicaciones que realizan tareas críticas en la red se encuentran redundados. -Los equipos de comunicaciones que realizan tareas críticas en la red disponen de doble fuente de alimentación. -Los equipos de comunicaciones que realizan tareas críticas en la red disponen de doble tarjeta supervisora. -Los servidores que realicen tareas críticas o alberguen la ejecución de aplicaciones críticas se encontrarán redundados en localizaciones distintas. -Los servidores que realicen tareas críticas o alberguen la ejecución de aplicaciones críticas dispondrán de doble fuente de alimentación.		☐ Documento: ☐ Muestreo: Observaciones:				

Valoración global del control E3	**0 - Inexistente.**

D) MODELO DE MADUREZ UTILIZADO PARA LA EVALUACIÓN DE LOS CBCS

Resultado de la revisión GLOBAL del control	
Nivel	**Descripción**
0 - Inexistente.	Esta medida no está siendo aplicada en este momento.
1 - Inicial / ad hoc	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. *La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.*
2 - Repetible, pero intuitivo.	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas, sin procedimientos escritos ni actividades formativas. *La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.*
3 - Proceso definido	Los procesos están estandarizados, documentados y comunicados con acciones formativas. *Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.* *Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.*
4 - Gestionado y medible.	La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere. *Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.* *En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.*
5 - Optimizado.	Se siguen buenas prácticas en un ciclo de mejora continua. *El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.* *En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.*

E) VALORES PREDEFINIDOS

Resultado de la evaluación de un subcontrol		Valoración del Riesgo y Cuantificación del Coste	
Nivel	**Descripción**	**Riesgo**	**Coste**
Control efectivo	■Cubre al 100% con el objetivo de control y: • El procedimiento está formalizado (documentado y aprobado) y actualizado. • El resultado de las pruebas realizadas para verificar implementación y eficacia operativa ha sido satisfactorio.	**Alto**	**Alto**
Control bastante efectivo.	■ En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y: • Se sigue un procedimiento, aunque éste puede no estar formalizado o presentar aspectos de mejora (detalle, nivel de actualización, etc.). • Las pruebas realizadas para verificar la implementación son satisfactorias. • Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa pero no son ni significativos ni generalizados.	**Medio**	**Medio**
Control poco efectivo.	■ Cubre de forma muy limitada el objetivo de control y: ■ • Se sigue un procedimiento, aunque éste puede no estar formalizado. • El resultado de las pruebas de implementación y eficacia operativa es satisfactorio. Cubre en líneas generales el objetivo de control pero: • No se sigue un procedimiento claro. • Las pruebas realizadas para verificar implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos aunque no están generalizados).	**Bajo**	**Bajo**
Control no efectivo o no implantado.	■ ■ No cubre el objetivo de control. El diseño cubre el objetivo de control, pero el resultado de la revisión realizada pone de manifiesto que implementación o eficacia operativa del control no son satisfactorias (se han detectado incumplimientos significativos y generalizados).		