GPF-OCEX 5313 Revisión de los Controles Básicos de Ciberseguridad

Anexo 3 Programa de auditoría (Fichas de revisión)

A) INSTRUCCIONES

Introducción

En la "GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa" se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas y, en consecuencia, la atención creciente que los auditores públicos deben conceder a esta materia.
En dicha guía se detallan los diferentes enfoques que los OCEX pueden adoptar a la hora de abordar una auditoría o una revisión de la ciberseguridad.
En esta GPF-OCEX 5313 se profundiza en el enfoque consistente en la revisión de una serie de controles de ciberseguridad considerados básicos. Esta selección se ha realizado tomando como marco de refencia los controles básicos del CIS (Center for Internet Security) y se ha hecho hincapié en la relación existente entre estos y el Esquema Nacional de Seguridad (ENS), puesto que el ENS es de obligado cumplimiento para los entes públicos.

Finalidad

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

Alcance de la revisión *(ver GPF-OCEX 5313, apartado 5)*

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 analizar. Por tanto, en la planificación de cada trabajo de revisión de los controles básicos de ciberseguridad 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 ciberseguridad 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 ciberseguridad.
En el apartado 5 de la GPF-OCEX 5313 se señalan los criterios generales a seguir para determinar el alcance.

Descripción de la estructura del Anexo 3 de la GPF-OCEX 5313

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":*** Describe el entorno tecnológico y la determinación del alcance del trabajo.
El objetivo de ésta es:
    * Recoger, a alto nivel, una descripción breve de los sistemas de información existentes en la Entidad (entorno tecnológico).
    * Señalar los sistemas de información sobre los que se ha focalizado la revisión (alcance).
* **Pestañas "*CBCS [1..7]*"** : Hay una pestaña por cada uno de los 7 primeros controles básicos de ciberseguridad incluidos en el programa de trabajo.
En cada una de estas pestañas se encuentra la siguiente información:
    * CBCS x: Número del control de ciberseguridad 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.
    * Evaluación del subcontrol: Evaluación de la efectividad de cada subcontrol, de acuerdo a los criterios establecidos en el apartado 7 de la guía (GPF-OCEX 5313).
    * Recomendación: Columna a completar en los casos en los que el subcontrol no sea efectivo y se considere oportuno realizar una recomendación.
    * Riesgo: Nnivel de riesgo valorado 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 "Evaluación global del control" según el modelo de madurez.
* **Pestaña *"CBCS 8"*** : En esta pestaña se recogen los controles relacionados con el cumplimiento normativo y los resultados de la revisión realizada.
* ***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 acciones corresponc
* ***Pestaña "C) Conclusión"*** : Incluye un resumen de la "Evaluación global" de cada uno de los controles básicos de ciberseguridad junto con el de cumplimiento de la legalidad.

Descripción del trabajo a realizar

La revisión se realizará de la siguiente forma:

* En primer lugar, se completará la ficha o pestaña "A) Entorno 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 "CBCSx" del Anexo 3.

Se cumplimentarán las pestañas CBCSx 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.

Cómo evaluar 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.

B) DESCRIPCIÓN DEL ENTORNO TECNOLÓGICO Y DETERMINACIÓN DEL ALCANCE DEL TRABAJO

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* (1) * SW Gestor de Base de Datos: *Oracle* (1) * Sistema operativo: *RHEL 7* (1)
* 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	*sindicom.es* (1)
Software de virtualización	*VMWare* (1)
Equipos de usuario	*A0987654321 (Epinar)* (1) *y B0987654321 (Asalom)* (1)
Un elemento de la red de comunicaciones (ej. router, switches, punto de acceso a red wifi, etc.)	*rou01 (router de Internet)* (1)
Un elemento de seguridad (ej: firewall, IPS, proxy de correo, proxy de navegación, etc.)	*Ironport01* (1)

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					
CBCS1	x (1)	x (1)	x (1)	x (1)	x (1)	x (1)			x (1)		
CBCS2	x (1)	x (1)	x (1)	x (1)	x (1)	x (1)					x (1)
CBCS3	x (1)	x (1)	x (1)	x (1)	x (1)	x (1)				x (1)	
CBCS4											
CBCS5											
CBCS6											
CBCS7											
CBCS8											

(1): Los sistemas y aplicaciones señalados (y que aparecen en cursiva) son ejemplos. En la realización del trabajo de campo, el equipo auditor deberá registrar la información específica del entorno tecnológico a auditar y el alcance del trabajo que se determine.

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	Evaluación 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:				

Evaluación global del control CBCS 1:	1 - Inicial / ad hoc

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	Evaluación 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. *<u>Prueba complementaria para evaluar este control:</u>* 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:				

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	Evaluación 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:				

Evaluación global del control CBCS 2:	1 - Inicial / ad hoc

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	Evaluación 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:				

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	Evaluación 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:				

Evaluación global del control CBCS 3:	2 - Repetible, pero intuitivo.

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	Evaluación 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 (en este caso administrador). Existe evidencia documental de cuáles son los privilegios que debe tener cada usuario en función de sus obligaciones. Confirmar con los responsables que los usuarios que disponen de privilegios de administración son los que tienen atribuidas las funciones de administrador. 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 un procedimiento que describe 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). y confirmar para una muestra de los usuarios con privilegios de administración que han sido solicitados, autorizados y concedidos por las personas autorizadas para ello. 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 congruentes con las del inventario. NOTA: Una buena práctica de seguridad que, además permite tener un inventario, es el uso de un servidor de autenticación (Radius, TACACs, etc.). En este tipo de equipos se dan de alta todas las cuentas de administrador con sus contraseñas, de forma que para validar usuario y cuenta, el sistema no lo comprueba de forma local al propio sistema, sino que lo valida contra el servidor de autenticación centralizado.		☐ 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:				

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	Evaluación 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: 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?		☐ Documento: ☐ Muestreo: Observaciones:				

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	Evaluación del subcontrol	Recomendación	Riesgo	Coste de implantación recomend.
			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:				

Evaluación global del control CBCS 4:	3 - Proceso definido

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 cambio 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	Evaluación del subcontrol
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.- ¿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			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:	

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 cambio 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	Evaluación del subcontrol
o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.	op.exp.3		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:	

Evaluación global del control CBCS 5:	4 - Gestionado y medible.

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	Evaluación del subcontrol
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 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	Evaluación del subcontrol
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 --> NOTA: por la criticidad de este control, a pesar de que el ENS lo exige sólo a partir de Nivel Alto, se considerará SIEMPRE en las revisiones de ciberseguridad.** 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:	
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 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	Evaluación del subcontrol
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:	Cumple el objetivo de control

Evaluación global del control CBCS 6:	5 - Optimizado.

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	Evaluación del subcontrol
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 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	Evaluación del subcontrol
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:	

Evaluación global del control CBCS 7:	**4 - Gestionado y medible.**

CLCS 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
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:	

CLCS 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
	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:	
	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 la entidad ha publicado en su sede electrónica la declaraciones de conformidad y los distintivos de seguridad correspondientes, según los resultados de la autoevaluación o auditoría. 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			***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:	

CLCS 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
	No		***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:	

CLCS 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
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:	

Evaluación global del control CBCS 8:	4 - Gestionado y medible.

C) RESULTADO DE LA EVALUACIÓN GLOBAL DE LOS CBCS	
Evaluación global del control CBCS 1:	1 - Inicial / ad hoc
Evaluación global del control CBCS 2:	1 - Inicial / ad hoc
Evaluación global del control CBCS 3:	2 - Repetible, pero intuitivo.
Evaluación global del control CBCS 4:	3 - Proceso definido
Evaluación global del control CBCS 5:	4 - Gestionado y medible.
Evaluación global del control CBCS 6:	5 - Optimizado.
Evaluación global del control CBCS 7:	4 - Gestionado y medible.
Evaluación general de los CBCS:	

Evaluación global del control CBCS 8:	

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).		