Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 26/06/2024

ÁREA C. OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN

INTRODUCCIÓN

Esta GPF-OCEX 5333 forma parte del conjunto de guías que, junto con la GPF-OCEX 5330 (Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica), están diseñadas para revisar/auditar los CGTI en una entidad que opera en un entorno de administración electrónica avanzada utilizando sistemas de información complejos e interconectados.

En esta guía se aborda la revisión de los controles del área **C. Operaciones de los sistemas de información** y está diseñada para:

- Ayudar a obtener información avanzada sobre el entorno TI de la entidad fiscalizada y de los CGTI.
- Ayudar a identificar riesgos derivados del uso de TI y los CGTI que los aborden.
- Ayudar a evaluar el diseño, implementación y eficacia operativa de los CGTI.
- Ayudar a identificar la existencia de deficiencias en esos controles que puedan derivar en riesgos significativos.
- Documentar los procedimientos llevados a cabo, la evidencia obtenida y las conclusiones alcanzadas respecto al diseño, implementación y eficacia operativa de los CGTI.

Tal y como se indica en GPF-OCEX 5330 (apartado 14), **los controles de esta área son importantes** por los siguientes motivos:

> *"Los controles del área de operaciones de los sistemas permiten la explotación segura de los sistemas de la entidad. Este conjunto de controles está formado por controles técnicos y por controles organizativos o de gestión, y son importantes porque permiten asegurar que la operación de los sistemas se realiza conforme a los niveles de seguridad establecidos.*
>
> *Los controles de esta área pueden ser de cualquier naturaleza, preventivos, detectivos o correctivos, y corresponden a una gran diversidad de aspectos de la explotación de los sistemas."*

El contenido de la presente guía, con carácter general, no debe ser considerado para su aplicación de manera exhaustiva. Tal y como se indica en el apartado 2 de la GPF-OCEX 5330, únicamente se deberán evaluar aquellos controles identificados que sean relevantes o significativos, en función de los objetivos y alcance de la auditoría que se esté realizando.

Una vez identificados los controles relevantes, se deberá realizar una selección de los procedimientos de auditoría de las guías 5331 a 5335 correspondientes a estos controles relevantes, incluyendo aspectos a evaluar, preguntas, propuesta de evidencias, etc. Este subconjunto de procedimientos constituirá el programa de trabajo de cada auditoría en particular.

Como se señala en la guía GPF-OCEX 5330, el conjunto de guías de esta serie mantiene "*la máxima coherencia con los postulados del ENS, puesto que es de obligado cumplimiento para todos los entes públicos y esta alineación facilita la realización de las auditorías de CGTI y coadyuvan a la implantación del ENS*". El contenido de esta guía ha sido desarrollado utilizando como base la "Guía de Seguridad de las TIC CCN-STIC 808" y, aunque se han incluido determinadas modificaciones y ampliaciones sobre los procedimientos de revisión, mantiene total compatibilidad con la guía STIC.

C1 – INVENTARIOS

C.1.1: Inventario de activos físicos autorizados

La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.

Requisitos:

op.exp.1.1	Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.
org.4	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos.

Propuesta de evidencias:

	☐	Procedimiento de gestión del inventario.
	☐	Si se emplea una herramienta de ticketing, evidencia de tickets de petición de alta y baja de nuevos activos físicos en el inventario.
	☐	Evidencia de las herramientas utilizadas para la gestión del inventario.
	☐	Evidencia de las revisiones periódicas realizadas para asegurar que el inventario se encuentra actualizado.
	☐	Evidencia del inventario de activos, que incluya al responsable de cada activo.
	☐	Evidencia de herramienta de monitorización / descubrimiento de activos.
	☐	Evidencia de herramienta que muestre relaciones y dependencias entre activos.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de un inventario de todos los elementos del sistema?** *NOTA: Es admisible el concepto de inventario federado, que consiste en la suma de varios inventarios independientes que en su conjunto constituyen el inventario completo, aunque siempre es más efectivo disponer de un único inventario con diferentes criterios de acceso a los activos.* *NOTA* *Verificar si existen inventarios distintos para distintas tipologías de activos que, en conjunto, constituyan un inventario completo de activos físicos. Incluyendo:* • *software específico de gestión de activos.* • *software de gestión de electrónica de red.* • *software de virtualización de servidores.* • *etc.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N2	¿Disponen de un procedimiento formalizado (escrito y formalmente aprobado) para la gestión del inventario? *NOTA* *Verificar que el proceso descrito por el procedimiento se corresponde con el proceso realmente implantado.* *Revisar el proceso de gestión del inventario (quién, cómo, cuándo) realiza el alta de los elementos y cómo se gestionan las bajas y modificaciones en la información de los elementos.*
N0	¿Se mantiene el inventario de activos completo y actualizado? *NOTA* *Obtener el/los inventarios de activos hardware.* *Realizar un muestreo de X elementos para verificar su existencia en el inventario y la exactitud de la información disponible.*
	¿Se detalla en el inventario la naturaleza de cada activo, identificando a su responsable? *NOTA* *Verificar que el inventario identifica:* *Equipos de usuario. Usuario asignado. Responsable de su seguridad y mantenimiento* *Electrónica y equipos de infraestructura. Responsable de su seguridad y mantenimiento.* *Software y aplicaciones. Responsable de su seguridad y mantenimiento.*
	¿Se realizan verificaciones periódicas respecto a la exactitud del inventario? *NOTA* *Verificar la existencia de informes internos o externos sobre el resultado de las revisiones.* *Verificar la existencia de tareas incluidas en la herramienta de ticketing.*
	¿Se utilizan herramientas automáticas que garanticen que el inventario está actualizado? *NOTA* *Verificar si existe una herramienta que realice el descubrimiento automático de activos físicos.* *Verificar que la gestión de activos, incluyendo el alta y baja de activos, se encuentran respaldada por el uso de herramientas de control de flujos de trabajo o ticketing.* *Verificar si existe un control manual o automático (herramienta de ticketing) que requiera de la autorización de nuevos elementos para su inclusión en el sistema.*
	El procedimiento para la autorización de nuevos elementos del sistema, ¿se encuentra enlazado con el inventario? *NOTA* *Verificar si las solicitudes de nuevos activos, realizadas en la herramienta de ticketing, se relacionan con los activos de la herramienta de gestión.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.1.2: Inventario de activos SW

La entidad dispone de un inventario de activos software autorizados completo, actualizado y detallado.

Requisitos:

op.exp.1.1	Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.
org.4	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos.

Propuesta de evidencias:

	☐	Procedimiento de gestión del inventario software.
	☐	Lista de software autorizado
	☐	Evidencia del inventario de activos software, que incluya al responsable de cada activo.
	☐	Evidencia de las herramientas utilizadas para la gestión del inventario software.
	☐	Evidencia de las revisiones periódicas realizadas para asegurar que el inventario se encuentra actualizado.
	☐	Evidencia de solicitud y autorización para instalación de software autorizado.
	☐	Evidencia de solicitud de inclusión en la lista de software autorizado, nuevo software. Y autorización previa a la incorporación.
	☐	Evidencia de herramienta de descubrimiento de activos software instalados.
	☐	Evidencia de herramienta que muestre relaciones y dependencias entre activos, incluyendo activos software y hardware.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de un inventario de todos los activos software del sistema?** *NOTA: Es admisible el concepto de inventario federado, que consiste en la suma de varios inventarios independientes que en su conjunto constituyen el inventario completo, aunque siempre es más efectivo disponer de un único inventario con diferentes criterios de acceso a los activos.* *NOTA* *Verificar si existen inventarios distintos que, en conjunto, constituyan un inventario completo de activos para distintas tipologías de activos software, incluyendo:* • *software de endpoint.* • *software de servidores.* • *software proporcionado por terceros.* ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N2	¿Disponen de un procedimiento formalizado (escrito y formalmente aprobado) para la gestión del inventario software? *NOTA* *Verificar que el proceso descrito por el procedimiento se corresponde con el proceso realmente implantado.* *Revisar el proceso de gestión del inventario (quién, cómo, cuándo) realiza la autorización, instalación e inventariado de software.*
N0	¿Se mantiene el inventario de activos software completo y actualizado? *NOTA* *Obtener el inventario de activos software.* *Realizar un muestreo de X elementos para verificar que el software instalado se encuentra inventariado y la exactitud de la información disponible.*
	¿Se detalla en el inventario la información necesaria sobre cada activo software, identificando a su responsable? *NOTA* *Verificar que el inventario identifica:* *Software y aplicaciones. Responsable de su seguridad y mantenimiento.*
	¿Se realizan verificaciones periódicas respecto a la exactitud del inventario? *NOTA* *Verificar la existencia de informes internos o externos sobre el resultado de las revisiones.* *Verificar la existencia de tareas incluidas en la herramienta de ticketing*.
	¿Se utilizan herramientas automáticas que garanticen que el inventario está actualizado? *NOTA* *Verificar si existe una herramienta que realice el descubrimiento automático de activos software, para aquellas tipologías de software que lo requieran.* *Verificar que la gestión de activos software, incluyendo la solicitud de instalación de software, se encuentran respaldada por el uso de herramientas de control de flujos de trabajo o ticketing.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.1.3: Control de HW no autorizados

La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados.

Requisitos:

	Se dispondrá de procesos de gestión para la autorización de nuevos dispositivos por parte del personal responsable.
	Se dispondrá de mecanismos y medidas técnicas que permitan restringir el acceso únicamente a los dispositivos físicos autorizados.

Propuesta de evidencias*:*

	☐	Procedimiento de gestión de activos.
	☐	Normativa de seguridad.
	☐	Evidencia del inventario de activos, que incluya al responsable de cada activo.
	☐	Evidencia de las herramientas utilizadas para la gestión del inventario/activos del sistema.
	☐	Evidencia de las revisiones periódicas realizadas para asegurar que el inventario se encuentra actualizado.
	☐	Evidencia de herramienta de monitorización / descubrimiento de activos.
	☐	Evidencia de medidas de seguridad en interfaces de electrónica de red.
	☐	Evidencia de la existencia de sistemas NAC
	☐	Evidencia de medidas de seguridad para autorización de activos en firewall.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se dispone de medidas que permitan detectar el acceso de dispositivos no autorizados en el sistema? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se realizan revisiones periódicas, manuales o automáticas, de los activos físicos para detectar dispositivos no autorizados en el sistema? *NOTA* *Verificar que se dispone de un inventario de activos, para poder identificar aquellos no autorizados en el sistema.*
L2	¿Se dispone de una normativa que establezca que únicamente pueden ser utilizados aquellos dispositivos que hayan sido previamente autorizados y se encuentren controlados por la entidad?
	¿Se ha informado al personal de la entidad de la prohibición de conectar dispositivos no autorizados al sistema?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	NOTA *Verificar si existe una normativa o política que establezca que únicamente los dispositivos autorizados pueden acceder al sistema y que diche normativa o política es conocida por todo el personal de la organización.*
	¿Se dispone de medidas que permitan restringir automáticamente el acceso de dispositivos no autorizados en el sistema?
	¿Se realiza una gestión de los puntos de red de manera se impida o dificulte la conexión de dispositivos no autorizados a la red? *NOTA* *Verificar si se dispone de una gestión de los puntos de red de manera se impida o dificulte la conexión de dispositivos no autorizados a la red, desactivando aquellos puntos de red que no se encuentren utilizados por un dispositivo autorizado.*
	¿Se dispone de medidas en la electrónica de red que permitan restringir el acceso de dispositivos no autorizados a la misma? *NOTA* *Verificar si se dispone de medidas en la electrónica de red que permitan restringir el acceso de dispositivos no autorizados a la misma, tales como restringir el número de macs por interfaz de red, la autorización de macs concretas en las interfaces de red.*
	¿Se dispone de medidas en el sistema WIFI que permitan restringir el acceso de dispositivos no autorizados a la misma? *NOTA* *Verificar si se dispone de medidas en la electrónica de red que permitan restringir el acceso de dispositivos no autorizados a la misma, tales como restringir el número de macs por interfaz de red, la autorización de macs concretas en las interfaces de red.*
	¿Se dispone de sistemas de seguridad específicos que permitan identificar y autenticar a los dispositivos que permitan restringir el acceso de dispositivos no autorizados en el sistema? *NOTA* *Verificar si se dispone de sistemas de seguridad específicos de control de acceso a red NAC, que permitan identificar y autenticar a los dispositivos que permitan restringir el acceso de dispositivos no autorizados en el sistema*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.1.4: Control de SW no autorizados

La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el uso de software no autorizado.

Requisitos:

	Se dispondrá de procesos de gestión para la autorización de nuevo software por parte del personal responsable.
	Se dispondrá de mecanismos y medidas técnicas que permitas restringir la ejecución únicamente al software autorizados.

Propuesta de evidencias*:*

	☐	Procedimiento de gestión del inventario software.
	☐	Lista de software autorizado
	☐	Evidencia de las herramientas utilizadas para la gestión del inventario software.
	☐	Evidencia de las revisiones periódicas realizadas para asegurar que el inventario se encuentra actualizado.
	☐	Evidencia de herramienta de descubrimiento de activos software instalados.
	☐	Evidencia de configuraciones de seguridad de los equipos de usuario para limitar los privilegios de instalación y/o ejecución de software no autorizado.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se dispone de medidas que permitan detectar el uso de software no autorizado? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se dispone de medidas que permitan evitar el uso de software no autorizado? *NOTA* *Verificar si se dispone de medidas que permitan restringir el uso de software no autorizados en el sistema, incluyendo:* • *el uso de cuentas sin privilegios administrativos en los equipos de usuarios. Se realizará un muestreo, mediante conexiones remotas o mediante las herramientas administrativas de Windows.* • *el uso de aplicaciones específicas para el control de la ejecución de software no autorizado, tales como Applocker o antivirus con listas blancas.* • *el uso de configuraciones de seguridad iniciales para los equipos de usuario, incluyendo únicamente instalación de software de lista blanca.*
L2	¿Se dispone de una normativa que establezca que únicamente pueden ser utilizado software y aplicaciones que hayan sido previamente autorizadas y se encuentren controladas por la entidad?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se realizan revisiones periódicas del software instalado para detectar el uso de software no autorizados el sistema? *NOTA* *Verificar que las revisiones realizadas son planificadas y controladas mediante herramientas de ticketing o de gestión de flujos de trabajo. Y que las tareas registradas incluyen información sobre el alcance de las revisiones, el personal responsable, el resultado de la revisión, las acciones posteriores y la periodicidad en la ejecución de las revisiones.*
	¿Se dispone de una lista de software autorizado? *NOTA* *Verificar si existe dicha lista y su aprobación, de acuerdo con procedimiento o política correspondiente.* *Verificar si existe un control que requiera de autorización para la inclusión de nuevos activos software en la lista de software actualizado.* *Verificar que se dispone de un inventario de software instalado y una lista de software autorizado, para poder identificar el software instalado sin autorización.*
	¿Se ha informado al personal de la entidad de la prohibición de utilizar software no autorizados? *NOTA* *Verificar si existe una normativa o política que establezca que únicamente puede utilizarse software autorizado y que dicha normativa o política y lista blanca de aplicaciones es conocida por todo el personal de la organización.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C2 – PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

C.2.1: Gestión de vulnerabilidades

Existe un proceso para identificar, priorizar y corregir las vulnerabilidades de los componentes del sistema.

Requisitos:

op.exp.4.1	Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos
op.exp.4.2	Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización
op.exp.4.r4.1	Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará: 1. Los indicadores críticos de seguridad a emplear. 2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]). 3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.
op.mon.3.r2.1	Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Propuesta de evidencias:

	☐	Procedimiento de gestión de vulnerabilidades.
	☐	Evidencia de seguimiento de anuncios CCN y/o fabricantes y/o organismos de referencia.
	☐	Evidencia de sonda CCN instalada.
	☐	Evidencia de servicios de hacking ético.
	☐	Evidencia de herramienta de escaneo de vulnerabilidades.
	☐	Evidencia de la inclusión en los pliegos de prescripciones técnicas para contratación de servicios o sistemas, de cláusulas para la gestión de vulnerabilidades.
	☐	Evidencia de sistemas o procesos para la gestión, priorización y seguimiento de resolución de vulnerabilidades.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se dispone de análisis dinámico de vulnerabilidades? ¿Se dispone de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración? ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se dispone de un proceso de identificación de vulnerabilidades? Incluyendo alguno de los siguientes: seguimiento de anuncios CCN y/o fabricantes y/o organismos de referencia, sondas, servicios de hacking ético, herramienta de escaneo de vulnerabilidades. *Nota* *Verificar si se hace uso de herramientas o medidas específicas para la gestión de vulnerabilidades, particularmente su identificación.*
N2	¿Se dispone de un procedimiento que detalle las acciones para la identificación de vulnerabilidades, su priorización en base a riesgo mitigado y la resolución de estas?
	¿Se dispone de un proceso para analizar y priorizar la resolución de las vulnerabilidades y defectos de seguridad identificados?
	¿Se realiza el seguimiento de la corrección de las vulnerabilidades identificadas que se ha decidido resolver?
	¿Se dispone de herramientas que automaticen o asistan en la gestión de los procesos de gestión de vulnerabilidades?

C.2.2: Parcheo

La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.

Requisitos:

	¿Se gestiona de forma continua la configuración de los componentes del sistema?
op.exp.3.r4	¿Se mantiene actualizada la configuración de seguridad del sistema operativo y de las aplicaciones?

Propuesta de evidencias:

	☐	Evidencia de herramienta o procedimiento de actualización de la configuración de seguridad.
	☐	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 del uso de sistemas de gestión de parches, por cada una de las tipologías de activos existentes, y, si están disponibles, revisar registros de ejecución.
	☐	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.
	☐	Si se emplea una herramienta de ticketing para la gestión en la aplicación de parches, evidencia de tickets que recojan las tareas relacionadas, como parte del proceso de gestión de cambios.

Procedimientos de auditoría (aspectos a evaluar):

	¿La configuración de seguridad del sistema operativo y de las aplicaciones se mantiene actualizada a través de una herramienta automática, o mediante un procedimiento manual, que permite la

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas? *NOTA* *Verificar si existen un proceso organizado que asegure que se realiza la instalación de modificaciones de versión y actualizaciones de seguridad oportunas para cada una de las tipologías de activos existentes.* *Verificar si existen sistemas de gestión de parches, por cada una de las tipologías de activos existentes.* *Verificar que el proceso de parcheo, se encuentra respaldado por el uso de herramientas de control de flujos de trabajo o ticketing.* *Obtener el inventario de activos hardware. Realizar un muestreo de X elementos para verificar que son aplicados los parches correspondientes, por cada una de las tipologías de activos existentes, verificando el nivel de parcheo y actualización y su fecha de realización.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	¿Se dispone de un procedimiento que detalle las acciones establecidas para asegurar la aplicación de parches necesarios en los sistemas de la entidad? ¿Establece dicho procedimiento responsabilidades y funciones en el proceso? ¿Especifica el documento sobre la periodicidad en la revisión de parches disponibles y la aplicación de los mismos?
	¿Los sistemas que se encuentran administrados por terceros, se mantienen actualizados mediante la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas? ¿Se recogen dichas obligaciones por parte del mantenedor en los pliegos de prescripciones técnicas para la contratación de sus servicios? *NOTA* *Obtener los pliegos de prescripciones técnicas (de los sistemas incluidos en el alcance del trabajo) para la contratación de servicios de mantenimiento o sistemas y verificar que recogen el compromiso del adjudicatario para la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.* *Verificar que se realiza, por parte de la entidad, un control sobre los servicios prestados por parte de terceros que asegure que se cumplen los acuerdos de nivel de servicio relativos a la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.2.3: SW soportado por el fabricante

El SW utilizado por la entidad tiene soporte del fabricante. En caso contrario, se identifica en el inventario como fuera de soporte.

Requisitos:

op.exp.4	¿Se realiza, de forma sistemática, el mantenimiento del equipamiento físico y lógico del sistema?

Propuesta de evidencias:

	☐	Evidencia de la existencia de un plan de mantenimiento del software.
	☐	Evidencia de la existencia de un proceso de gestión, soportado o no por herramientas o por documentos, que considere el control de las fechas de fin de soporte por parte de los fabricantes.
	☐	Evidencia sobre la existencia o no de software fuera de soporte por parte del fabricante
	☐	Evidencia sobre la existencia de contratos de mantenimiento (que garanticen el acceso a actualizaciones y parches) para cada una de las tipologías de activos.

Procedimientos de auditoría (aspectos a evaluar):

	¿Dispone de un plan de mantenimiento del software? ¿Atiende este plan a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas?
	¿Se controlan las fechas de fin de soporte del SW? *NOTA* *Verificar si existen un proceso organizado que asegure el control de las fechas de fin de soporte por parte de los fabricantes* *Verificar si dicho procedo se encuentra respaldado por herramientas específicas o por el uso de herramientas de gestión de flujo de trabajo o ticketing.* ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
N2	¿Dispone de un procedimiento para la revisión del SW autorizado en la entidad y las fechas dadas por los fabricantes de fin de soporte? *NOTA* *Verificar si se dispone de un procedimiento para la revisión del SW autorizado en la entidad y las fechas dadas por los fabricantes de fin de soporte y si 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.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	- 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.
	¿Existe software fuera de soporte por parte del fabricante? *NOTA* *Revisar el inventario de hardware y software y, para una muestra de elementos, comprobar que estos se encuentran dentro del soporte del fabricante, incluyendo adicionalmente a las aplicaciones incluidos en el inventario software, los sistemas operativos de equipos de usuario y servidores, el firmware de firewall, electrónica de red, el hipervisor del sistema de virtualización y las consolas de gestión correspondientes.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.3 - CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE DE DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES

C.3.1: Configuración de seguridad

La entidad ha definido, documento e implantado estándares de configuración segura para todos los sistemas operativos y sistemas previa a su entrada en producción.

Requisitos:

op.exp.2	Se configurarán los equipos previamente a su entrada en operación, de forma que:
op.exp.2.1	– Se retiren cuentas y contraseñas estándar.
op.exp.2.2	– Se aplicará la regla de «mínima funcionalidad», es decir: a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos. b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.
op.exp.2.3	– Se aplicará la regla de «seguridad por defecto», es decir: a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes. c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.
op.exp.2.4	– Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Propuesta de evidencias:

	☐	Evidencia de guías de bastionado, particularizadas a los equipos a revisar.
	☐	Evidencia de listas de comprobación cumplimentadas (checklist) de los equipos bastionados.
	☐	Evidencias al azar, solicitadas por el auditor, para verificar que diferentes aspectos considerados en las guías de bastionado se hayan configurado en la realidad.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	¿Se realiza una configuración de seguridad (bastionado) a los equipos, previamente a su puesta en producción? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	1.- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación? Respecto a dicho procedimiento de bastionado: a) Alcance: ¿Qué tipo de dispositivos cubre (servidores, equipos de sobremesa, portátiles, móviles y tabletas, etc.)? b) ¿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)? c) Está basado en checklist, guías y recomendaciones de fabricantes y/o organismos de referencia? (ENS, NIST (https://nvd.nist.gov/ncp/repository), CIS e) ¿Detalla los mecanismos a utilizar para mantener el reloj del sistema en hora
N0	¿Se han configurado los equipos, previamente a su entrada en operación, retirándoles cuentas y contraseñas standard? ¿Está esta medida establecida en el procedimiento aprobado?
N0	¿Se han configurado los equipos, previamente a su entrada en operación, aplicándoles la regla de 'mínima funcionalidad', es decir, que el sistema proporcione la funcionalidad mínima imprescindible para que la organización alcance sus objetivos? ¿Está esta medida establecida en el procedimiento aprobado? *NOTA: la 'mínima funcionalidad' se traduce en que el sistema no proporcione funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su superficie de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.*
N0	¿Se han configurado los equipos, previamente a su entrada en operación, de manera que se aplique la regla de 'seguridad por defecto'? *NOTA: La 'seguridad por defecto' se concreta estableciendo medidas de seguridad respetuosas con el usuario y que le protejan, salvo que éste se exponga conscientemente a un riesgo; En otras palabras, para reducir la seguridad el usuario tiene que realizar acciones conscientes, por lo que el uso natural, en los casos que el usuario no ha consultado el manual, ni realizado acciones específicas, será un uso seguro.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se han configurado y gestionado las máquinas virtuales, previamente a su entrada en operación, de un modo igual de seguro al empleado para las máquinas físicas? *NOTA: La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.3.2: Gestión y mantenimiento de la configuración de seguridad

La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.

Requisitos:

op.exp.3	Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:
op.exp.3.1	– Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
op.exp.3.2	– Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
op.exp.3.3	– El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
op.exp.3.4	– El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
op.exp.3.5	– El sistema reaccione a incidentes. (Ver [op.exp.7]).
op.exp.3.6	– La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.
op.exp.3.r1	R1-Mantenimiento regular de la configuración.
op.exp.3.r1.1	– Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
op.exp.3.r1.2	– Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
op.exp.3.r1.3	– Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Propuesta de evidencias:

	☐	Registros (quizás en una herramienta de ticketing) que evidencien la gestión continua de la configuración de seguridad.
	☐	Informes de Auditoria de bastionado
	☐	Informe de verificaciones de ausencia de elementos no autorizados en el sistema.
	☐	Lista de servicios autorizados en servidores y en estaciones de trabajo.
	☐	Evidencia del número e identificación de los administradores de las configuraciones de seguridad del sistema operativo y las aplicaciones.
	☐	Evidencia de la realización de copias de seguridad de las configuraciones.
	☐	Evidencia de herramienta o procedimiento de actualización de la configuración de seguridad.
	☐	Evidencia de herramientas de monitorización de la seguridad.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	¿Se gestiona de forma continua la configuración de los componentes del sistema? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se gestiona de forma continua la configuración de los componentes del sistema, manteniéndose en todo momento la regla de 'funcionalidad mínima'? NOTA: la 'mínima funcionalidad' se traduce en que el sistema no proporcione funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.
	¿Se gestiona de forma continua la configuración de los componentes del sistema, manteniéndose en todo momento la regla de 'mínimo privilegio'?
N0	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema se adapta a las posibles nuevas necesidades, previamente autorizadas?
N0	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema reacciona a posibles vulnerabilidades notificadas?
N0	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema reacciona a posibles incidentes?
N0	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que la configuración de seguridad únicamente puede editarse por personal debidamente autorizado?
N2	La gestión continuada de la configuración anterior (preguntas anteriores) se establece en el/los procedimiento/s de seguridad pertinentes.
	¿Se dispone, para los componentes del sistema, de configuraciones autorizadas, mantenidas y verificadas, junto a la identificación de servicios autorizados? ☐ SI ☐ NO
	Espacio disponible para la redacción
	¿Se dispone de configuraciones hardware/software autorizadas y mantenidas regularmente para los servidores, elementos de red y estaciones de trabajo?
	¿Se verifica periódicamente la configuración hardware/software del sistema, para asegurarse que no se han introducido ni instalado elementos no autorizados?
	¿Se mantiene una lista de servicios autorizados para servidores y estaciones de trabajo?
	¿Se han establecido responsabilidades sobre la configuración de seguridad del sistema? ☐ SI ☐ NO

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Espacio disponible para la redacción	
	¿La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores, como de la electrónica de red del sistema, es responsabilidad de un número muy limitado de administradores del sistema?
	¿Se realizan copias de seguridad de la configuración del sistema? ☐ SI ☐ NO
Espacio disponible para la redacción	
	¿Se realizan copias de seguridad de la configuración del sistema de forma que sea posible reconstruir éste, en parte o en su totalidad, tras un incidente?
	¿Se mantiene actualizada la configuración de seguridad del sistema operativo y de las aplicaciones? ☐ SI ☐ NO
Espacio disponible para la redacción	
	¿La configuración de seguridad del sistema operativo y de las aplicaciones se mantiene actualizada a través de una herramienta automática, o mediante un procedimiento manual, que permite la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas?
	¿Se dispone de herramientas de monitorización de la seguridad?
Espacio disponible para la redacción	
	¿Se dispone de herramientas que permitan conocer el estado de seguridad de la configuración de los dispositivos de red de forma periódica y, en el caso de que resulte deficiente, poder corregirlo?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.3.3: Mantenimiento

Se realiza un mantenimiento adecuado del equipamiento físico y lógico de la entidad.

Requisitos:

op.exp.4	Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:
op.exp.4.1	– Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
op.exp.4.2	– Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
op.exp.4.*3*	– El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Propuesta de evidencias:

	☐	Evidencias de contratos de mantenimiento del equipamiento físico y lógico relevante.
	☐	Protocolo o sistemática seguida para la actualización y mantenimiento de los sistemas.
	☐	Evidencias de actualizaciones.
	☐	Evidencia de pruebas de preproducción previas a la instalación de parches o versiones completas.
	☐	Procedimiento formal de actualización y mantenimiento de sistemas.
	☐	Evidencias de planes de vuelta atrás previos a la actualización de sistemas.
	☐	Evidencias de actualización del firmware de los dispositivos

Procedimientos de auditoría (aspectos a evaluar):

N0	¿Se realiza, de forma sistemática, el mantenimiento del equipamiento físico y lógico del sistema? ☐ SI ☐ NO
N0	¿En lo relativo a instalación y mantenimiento del equipamiento físico y lógico que constituye el sistema, se atiende a las especificaciones de los fabricantes? NOTA: Esta atención se concreta en un seguimiento continuo de los anuncios de defectos. Se entiende por mantenimiento del equipamiento, por ejemplo, a la liberación de espacio en disco cuando sea necesario, limpieza de archivos obsoletos, comprobación de las luces de estado en las máquinas físicas, verificación del funcionamiento correcto de aparatos, instalación de parches de seguridad cuando se requiera, etc.
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N2	¿Se dispone de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones? *NOTA: La priorización debe tener en cuenta la variación del riesgo en función de la aplicación o no del parche o de la actualización disponible*
	¿El mantenimiento es realizado únicamente por personal debidamente autorizado?
	Antes de poner en producción una nueva versión o una versión parcheada, ¿se comprueba en un entorno de prueba controlado, consistente en cuanto a configuración con el entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario? ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad, ¿se prevé un mecanismo de vuelta atrás para revertirlos en caso de la aparición de efectos adversos? ☐ SI ☐ NO
Espacio disponible para la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C4 – REGISTRO DE EVENTOS Y DE LA ACTIVIDAD DE LOS USUARIOS (*Logs*)

C.4.1: Activación de logs de auditoría

Los registros de actividad, tanto de los eventos del sistema como de la actividad de los usuarios, (logs de auditoría), están activados en todos los sistemas y dispositivos de red y contienen el detalle suficiente para la detección, análisis, investigación y prevención de ciberataques.

Requisitos:

Op.exp.8 op.exp.8.1 op.exp.8.2	Se registrarán las actividades en el sistema, de forma que: – Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma. – Se activarán los registros de actividad en los servidores.
op.exp.8.r3.1	– En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.
op.exp.8.r4.1	– Los registros de actividad y, en su caso, sus copias de seguridad solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.
mp.s.3.r1.1	Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.

Propuesta de evidencias:

	☐	Política o normativa de seguridad asociada, relativa al registro de eventos y actividad de los usuarios en los sistemas.
	☐	Evidencia de los *logs* conservados.
	☐	Evidencia de configuración de *logs* en los servidores.
	☐	Evidencia de la modificación de las configuraciones por defecto en los sistemas en cuanto al registro de eventos.
	☐	Evidencias de registros de monitorización de la navegación web

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se registran los eventos y actividades de usuarios y entidades que acceden a los sistemas?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	**En la documentación de seguridad del sistema, ¿se indican los eventos de seguridad que serán auditados?** ☐ SI ☐ NO *NOTA: Se debe verificar la existencia, bien en la política de seguridad o bien en el cuerpo normativo que la desarrolla, de la normativa correspondiente a la gestión de los logs de auditoría, para confirmar que refleja explícitamente los eventos de seguridad que serán auditados, cómo se realizará su almacenamiento, el tiempo de retención de los registros y los controles de acceso establecidos sobre estos registros y sus copias de seguridad.*
	Espacio disponible para la redacción de la respuesta
N0	¿Se registran las actividades del sistema generando un registro de auditoría que incluye, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma?
N0	¿Se han activado los registros de actividad en los servidores?
	¿Se registra el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.4.2: Registro de la actividad de las cuentas con privilegios de administración

El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.

Requisitos:

	El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.

Propuesta de evidencias:

	☐	Política o normativa de seguridad asociada, relativa al registro de eventos y actividad de los usuarios en los sistemas.
	☐	Evidencia de la configuración de los logs relativa a las cuentas/usuarios sujetos a política de auditoría.
	☐	Evidencia de los logs conservados.
	☐	Evidencia de los controles de acceso implantados para impedir que los usuarios con privilegios de administración puedan modificar o eliminar, por error o intencionadamente, los registros de actividad y eventos.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Los *logs* de auditoría incluyen la actividad de los operadores y administradores del sistema?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se ha establecido la necesidad de registrar la actividad de los administradores y operadores del sistema, así como todas aquellas cuentas que dispongan de privilegios elevados? *NOTA: Este requisito debe estar recogido en la política de seguridad o en la normativa de seguridad que la desarrolle.* *Además, para verificar la adecuada implantación de este control, se debe Seleccionar una muestra de sistemas y comprobar si los mecanismos de registro almacenan esta información, es decir, las acciones realizadas por cuentas de usuario con elevados privilegios.*
	¿Los usuarios privilegiados tienen la posibilidad de modificar los registros de auditoría?
	¿Se dispone de controles que impidan la modificación ilegítima de los losg por parte de los administradores? *Nota: Una de las posibles estrategias para cumplir este requisito es utilizar como repositorio de los logs de auditoría un sistema externo en el que el administrador del sistema del que se requiere tener el log no tenga privilegios de acceso.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.4.3: Sincronización, retención y protección de logs

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.

Requisitos:

op.exp.8.r2.1	– El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.
op.exp.8.r3.1	– En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.
op.exp.8.r4.1	– Los registros de actividad y, en su caso, sus copias de seguridad solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Propuesta de evidencias*:*

	☐	Documentación de seguridad del sistema relacionada con la definición del periodo de retención de los *logs*.
	☐	Evidencia de servidores NTP o equivalentes.
	☐	Evidencia de la configuración del periodo de retención de los *logs* en los distintos sistemas auditados.
	☐	Evidencia de protección del acceso de los *logs* (p.e., permisos sobre carpetas y directorios a nivel de sistema operativo, permisos a nivel de tablas de base de datos, etc.).
	☐	Evidencia de protección del acceso de la copia de seguridad de los *logs*.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se sincronizan los relojes del sistema?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Dispone el sistema de elementos de referencia de tiempo (servidores NTP, sellado de tiempo…) para facilitar las funciones de registro de eventos y auditoría? *NOTA: La modificación de la referencia de tiempo del sistema debe ser una función de administración y esta debe estar adecuadamente restringida.* *En caso de realizarse la sincronización de los sistemas con otros dispositivos distintos de los de referencia de tiempo, se deberán utilizarse mecanismos de autenticación e integridad.*
N0	**En la documentación de seguridad del sistema, ¿se indica el tiempo de retención de los *logs* antes de ser eliminados?** ☐ SI ☐ NO

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Espacio disponible para la redacción de la respuesta	
N0	¿Se encuentra configurado el tiempo de retención de los logs de los distintos sistemas de acuerdo con lo establecido en la documentación de seguridad del sistema? *NOTA: Para verificar la efectiva implantación de este control, se puede comprobar, para una muestra de los sistemas, que el tiempo de retención configurado está alineado con lo establecido en la documentación de seguridad del sistema.*
N0	**Los registros de actividad y, en su caso, las copias de seguridad ¿únicamente pueden ser accedidos, alterarse o eliminarse por personal debidamente autorizado?** ☐ SI ☐ NO *Nota:* Identificar la ubicación en la que se almacenan los *logs* y analizar las medidas de control de acceso existentes. Es importante tener en cuenta que un mismo log pueden encontrarse en diferentes ubicaciones: sistema origen que lo ha generado, copia de seguridad de ese sistema y un repositorio secundario si la entidad ha optado por llevar una copia del log original a un repositorio centralizado. En función de los repositorios utilizados esto puede realizarse, por ejemplo, de la siguiente forma: • Permisos a los directorios y carpetas en las que se guardan los *logs*. • Permisos a las tablas de base de datos en las que se almacenan los *logs*. • Permisos de acceso a los soportes/rutas que albergan la copia de seguridad de los *logs*. • Permisos de acceso sobre los ficheros, tablas, etc. que se utilice para el almacenamiento centralizado de los *logs*.
Espacio disponible para la redacción de la respuesta	

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.4.4: 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.

Requisitos:

op.exp.8.r1.1	Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.
op.exp.8.r5.1	– El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
op.exp.8.r5.2	– Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Propuesta de evidencias:

	☐	Evidencia de la existencia de un repositorio centralizado de almacenamiento de *logs*.
	☐	Evidencia de revisión de los *logs* centralizados.
	☐	Evidencia de revisión de los *logs* centralizados.
	☐	Evidencia de herramientas de análisis de *logs.*
	☐	Evidencia de sistemas automáticos de recolección de registros y correlación de eventos (tipo SIEM).

Procedimientos de auditoría (aspectos a evaluar):

¿Se realizan revisiones de los *logs*?

☐ SI ☐ NO

NOTA: Los controles incluidos en CGTI C9 sobre la monitorización del sistema y de su seguridad, complementan a esta medida.

NOTA 2: Con respecto a este control:

- *Revisar los siguientes aspectos:*
  - *la existencia de herramientas o sistemas externos para la centralización de los logs.*
  - *la existencia de procesos de revisión de los registros de actividad.*
  - *la existencia de tareas relacionadas con la revisión, planificada o reactiva, de los registros de actividad.*
- *Revisar el modo de explotación de la herramienta y la inclusión como información de entrada al sistema de los logs de actividad de los sistemas incluidos en el alcance.*
- *Obtener evidencia del tipo de revisión de logs realizados y evaluar alcance y frecuencia de las revisiones realizadas.*
- *En caso de no existir un sistema SIEM, evaluar la existencia de otro tipo de utilidades (SIM o SEM) que apoyen la revisión de logs.*

Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	¿Se dispone de un almacenamiento centralizado *logs*?
N0	¿Se realiza una revisión, aunque sea informal, de dichos registros?
	¿Se dispone de herramientas para apoyar la revisión de los *logs*? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se utilizan herramientas para analizar y revisar de forma centralizada los *logs* en búsqueda de incidencias?
	¿Se dispone de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos, como puede ser un SIEM?

NOTA:

- Gestión de logs: Centrados en recolección y almacenamiento básico de mensajes de log y de pistas de auditoría.
- SIM *(Security information management*): Almacenamiento durante periodos más extensos así como capacidades de análisis y reporte.
- SEM (*Security Event Manager*): Monitorización en tiempo real correlación de eventos, alertas y consola de gestión.
- SIEM (*Security information and event management*): Combina SIM y SEM y proporciona análisis en tiempo real de las alertas detectadas.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C5 – SERVICIOS EXTERNOS

C.5.1: Autorización de uso de servicios externos

La utilización de servicios de terceros, bajo contrato o convenio, encargo, concesión, etc. debe estar debidamente autorizada.

Requisitos:

org.4 org.4.8	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos: – Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Propuesta de evidencias:

	☐	Documentos o registros, que muestren la aprobación formal a los distintos servicios externos utilizados por la entidad e incluidos en la muestra.
	☐	Si se emplea una herramienta de ticketing que las consolide, evidencia de tickets de peticiones de autorización.
	☐	Información sobre la contratación de servicios durante el periodo auditado realizada por la entidad (p.e. obtenida de la Plataforma de Contratación del Sector Público).
	☐	Relación de los servicios externos de los que haga uso la entidad.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se gestionan las autorizaciones para la utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.?** ☐ SI ☐ NO *NOTA: Se entiende por servicios de terceros los de almacenamiento remoto en la nube, backup remoto, servicio de correo, aplicaciones entregadas como servicio (SaaS) como puede ser una gestión de inventario o una herramienta de ticketing, etc.* NOTA 2: La relación de servicios externos se puede obtener en la PCSP (Plataforma de Contratación del Sector Público), en donde se puede ver qué han contratado durante el periodo auditado, por ejemplo.
	Espacio disponible para la redacción de la respuesta
N2	¿Se registran las autorizaciones concedidas a efectos de trazabilidad, siguiendo un procedimiento formal establecido en la organización? NOTA: En relación con este punto, se debe comprobar: • La existencia de la autorización formal para cada uno de los servicios externos incluidos en la muestra. • El proceso seguido por la organización para gestionar este tipo de autorizaciones y guardar la documentación necesaria para asegurar la trazabilidad de todo el proceso.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.5.2: Requisitos de seguridad de los servicios externos

Se planifican y gestionan los requisitos de seguridad de las empresas externas contratadas para la provisión de servicios.

Requisitos:

	¿Se suscriben acuerdos de nivel de servicio con los proveedores, a la vez que se les requiere estar en posesión del correspondiente certificado de conformidad respecto al ENS?

Propuesta de evidencias:

	☐	Pliego de Prescripciones Técnicas (PPT) y Pliego de Condiciones Administrativas.
	☐	Otra documentación relacionada con la contratación del servicio que recoja los requisitos de seguridad que debe cumplir el servicio.
	☐	Certificados de cumplimiento del ENS del proveedor.
	☐	Análisis de riesgos del servicio, previo a la contratación, orientado a determinar los requisitos de seguridad.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se han establecido contractualmente los requisitos de seguridad que debe cumplir el proveedor del servicio?** ☐ SI ☐ NO *NOTA: Se debe analizar la inclusión de los requisitos de seguridad en los pliegos de contratación.*
	Espacio disponible para la redacción de la respuesta
	¿Se requiere a los proveedores de servicios externos estar en posesión del correspondiente certificado de conformidad respecto al ENS? *Nota: Para confirmar este punto se debe revisar el certificado de cumplimiento del ENS aportado por cada uno de los proveedores del servicio y contrastar esta información con el registro de proveedores certificados* (https://gobernanza.ccn-cert.cni.es/certificados). *Sobre este punto, profundizar en el análisis de la certificación con el objetivo de asegurar que el certificado de conformidad cubre los sistemas del proveedor involucrados en la prestación del servicio y no otros.*
	¿Se han recogido en los pliegos los requisitos de seguridad que debe cumplir el proveedor del servicio?
	Con carácter previo a la contratación del servicio, ¿se ha realizado un análisis de riesgos en base al cual la entidad haya determinado los requisitos de seguridad del servicio?
	¿Se controla la renovación del certificado de conformidad del ENS del proveedor durante toda la duración del contrato?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.5.3: Contratación y acuerdos de nivel de servicio

Se ha establecido el nivel de cumplimiento de los servicios externos.

Requisitos:

Op.ext.1.1	Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Propuesta de evidencias:

	☐	Evidencias de acuerdos de nivel de servicio (ANS/SLA) suscritos con proveedores.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se suscriben acuerdos de nivel de servicio con los proveedores?** ☐ SI ☐ NO *NOTA: Estos ANS/SLA deben estar recogidos contractualmente. Revisar los pliegos y la documentación del proceso de contratación.*
	Espacio disponible para la redacción de la respuesta
N0	Con anterioridad a la efectiva utilización de los recursos externos, ¿se establece contractualmente un Acuerdo de Nivel de Servicio (ANS/SLA) que incluya las características del servicio prestado, lo que debe entenderse como 'servicio mínimo admisible', así como, la responsabilidad del proveedor y las consecuencias de eventuales incumplimientos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.5.4: Gestión diaria

Se gestiona de manera continuada el nivel de cumplimiento de servicios externos.

Requisitos:

Op.ext.2.1 op.ext.2.2	Se establecerá lo siguiente: – Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]). – El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Propuesta de evidencias:

	☐	Evidencia de seguimiento de proveedores.
	☐	Actas de posibles reuniones de seguimiento con un proveedor.
	☐	Informes de gestión/informes de nivel de servicio, proporcionado por el proveedor.
	☐	Evidencia de designación del punto de contacto del proveedor (POC).
	☐	Evidencia de mecanismo establecido para notificar incidentes al proveedor (portal cliente, correo electrónico…).
	☐	Evidencia de incidentes abiertos a un proveedor y su seguimiento.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de mecanismos de seguimiento y supervisión del desarrollo del servicio, así como de reporte y coordinación ante posibles incidencias?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	¿Se dispone de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado? *NOTA: Algunos proveedores facilitan, motu proprio o bajo solicitud, informes de cumplimiento del servicio.*
	¿Se ha establecido un mecanismo y los procedimientos de coordinación necesarios para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de ocurrencia de posibles incidentes y desastres?
	¿Se ha designado por parte del proveedor un punto de contacto (POC) para cualquier cuestión relacionada con el servicio? ¿Se ha establecido el mecanismo establecido de contacto, especialmente para notificar incidentes del servicio?
	¿Se ha pactado con proveedores la entrega periódica de informes de servicio?
	¿Se realizan reuniones de seguimiento con determinados proveedores relevantes?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C6 – PROTECCIÓN DEL ENTORNO TI

C.6.1: Protección frente a código dañino

La entidad implementa una adecuada protección frente a código dañino en servidores y puestos de trabajo.

Requisitos:

op.exp.6.1 op.exp.6.2 op.exp.6.3 op.exp.6.4 op.exp.6.5	– Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo con las recomendaciones del fabricante. – Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales. – Todo fichero procedente de fuentes externas será analizado antes de trabajar con él. – Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas. – El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo con las recomendaciones del fabricante.
op.exp.6.r1.1	Todo el sistema se escaneará regularmente para detectar código dañino.
op.exp.6.r2.1	Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.
op.exp.6.r3.1	Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.
op.exp.6.r4.1	Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - Endpoint Detection and Response).
op.exp.6.r5.1	El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
op.exp.6.r5.2	El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo con las recomendaciones del fabricante.

Propuesta de evidencias:

	☐	Evidencia en los equipos de la instalación de una solución antimalware para su protección.
	☐	Evidencia de consola centralizada de la solución antimalware y su configuración.
	☐	Licencia de uso de la solución antimalware, con número máximo de equipos gestionados.
	☐	Evidencia de última actualización de la base de datos de detección del producto antivirus/antimalware.
	☐	Normativas, procedimientos o instrucciones que regulen la gestión de la protección antimalware.
	☐	Contrato o acuerdo de soporte de la solución antimalware.
	☐	Informes generados por la solución antimalware.
	☐	Evidencia de verificaciones de la solución antimalware.
	☐	Evidencia de otras soluciones antimalware adicionales, por ejemplo, en el FW.
	☐	Lista blanca de aplicaciones autorizadas.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de una solución de protección contra código dañino (antivirus, antimalware, EDR o solución similar) desplegada en todos los puestos de trabajo, servidores y elementos perimetrales del sistema?** ☐ SI ☐ NO *NOTA: Al revisar la solución antivirus/antimalware tener en cuenta lo siguiente:* • *¿Está instalada en todos los puestos de usuario?* *Nota: Considerar equipos de sobremesa, portátiles y otros dispositivos que tengan acceso a la red corporativa (tablets, teléfonos, etc.).* • *¿Está instalada en todos los servidores? ¿Y en los servidores no Windows?* • *¿Está instalada en todos los elementos perimetrales (firewall, proxies de correo y navegación, etc.)?* • *¿Se dispone de contrato vigente de soporte y mantenimiento de la solución para todos los equipos?* • *¿Garantiza la protección en tiempo real?* *Con respecto a la configuración de dicha solución, revisar los siguientes aspectos:* • *Cómo y cada cuánto se actualiza la base de datos de detección.* • *Cómo se garantiza que el usuario no pueda inhabilitar la solución.* • *Existencia y uso de una consola central de monitorización.*
	Espacio disponible para la redacción de la respuesta
N0	¿Se ha configurado la solución antimalware instalada en los puestos de usuario de forma adecuada, implementando protección en tiempo real de acuerdo con las recomendaciones del fabricante y las características del entorno operativo?
N0	¿Se ha instalado dicho software de protección frente a código dañino en todos los equipos, incluyendo puestos de usuario, servidores y elementos perimetrales?
	¿Se trata de una solución corporativa con consola centralizada de administración?
N0	¿Se requiere una contraseña de administración o se dispone de cualquier otro mecanismo que impida que el usuario final detenga o altere el funcionamiento de la solución?
N0	La licencia de uso de la solución ¿cubre la totalidad de equipos presentes en la organización?
	¿Se dispone de garantías de que todo fichero procedente de fuentes externas será analizado antes de trabajar con él? *NOTA: Considerar:* • *Los ficheros que se reciben por correo.* • *Los ficheros que se pueden descargar en la navegación.* • *Los ficheros que se envían por herramientas tipo whatsapp, Teams, etc.* • *El uso de unidades externas de almacenamiento.*
	¿Está amparada la solución antimalware por un acuerdo de soporte y actualización, tanto del software como de la base de datos de detección?
	¿Se comprueba regularmente que las bases de datos de detección de código dañino se estén actualizando con la frecuencia prevista?
	¿Los elementos de seguridad (firewalls, proxys de correo y navegación, etc.) disponen de solución antimalware especializada que, por ejemplo, verifique navegación web y correos recibidos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se verifica regularmente la configuración de la(s) solución(es) antimalware para garantizar que se adecuan a las operaciones de los sistemas protegidos?
N0	**R1. ¿Se ejecutan análisis y escaneos, de forma regular en los sistemas, en búsqueda de código dañino?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	¿Existe algún mecanismo o procedimiento que escanee regularmente los sistemas para detectar código dañino?
	¿Se revisan regularmente los informes de resultados generados como consecuencia de los escaneos de los sistemas, así como otra información generada de forma consolidada desde la consola de administración?
	R2. Al arrancar los sistemas, ¿se analizan las funciones críticas en prevención de modificaciones no autorizadas? ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	R3. ¿Se ha implementado una lista blanca que impida la ejecución de aplicaciones no autorizadas previamente y, en consecuencia, que no estén en dicha lista? ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	R4. ¿Se han implementado soluciones de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en los equipos (*EDR - Endpoint Defense and Response*)? ☐ SI ☐ NO *NOTA: Analizar el uso por parte de la entidad de listas blancas de aplicaciones y de soluciones EDR.*
Espacio disponible para la redacción de la respuesta	
	R5. ¿La solución antimalware, además de implementar protección en tiempo real, permite realizar configuraciones avanzadas y revisar el sistema al arrancar, así como cada vez que se conecte algún dispositivo extraíble? ☐ SI ☐ NO

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.6.2: Protección del correo electrónico

La entidad implementa una adecuada protección frente a las amenazas propias del servicio de correo electrónico.

Requisitos:

Mp.s.1	El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo: – La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos. – Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones. Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto: – Correo no solicitado, en su expresión inglesa «spam». – Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga. – Código móvil de tipo micro-aplicación, en su expresión inglesa «applet». Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán: – [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas. – [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Propuesta de evidencias:

	☐	Normativa de uso seguro del correo electrónico.
	☐	Opciones empleadas para el cifrado de mensajes de correo electrónico, si es necesario.
	☐	Configuración y logs del filtro 'antispam'.
	☐	Evidencia del análisis y protección antivirus del correo electrónico y de otras amenazas (configuración del AV, configuración de la solución de sandboxing, bloqueo de ciertas extensiones, etc.).
	☐	Informes sobre el servicio de correo (correos entregados/descartados frente a recibidos, orígenes de correos bloqueados, etc.).
	☐	Campañas de concienciación y de formación sobre el uso seguro del correo electrónico.
	☐	Bastionado empleado para proteger el servidor de correo, si es propio.
	☐	Certificado de cumplimiento del ENS (u otro tipo de documentación correspondiente a las medidas de seguridad implantadas) por parte del proveedor del servicio de correo electrónico, si este se tiene externalizado.
	☐	Evidencia de la configuración de mecanismos como SPF, DKIM y DMARC.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se protege el correo electrónico frente a las amenazas que le son propias?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se protege el servidor de correo electrónico, cuando es interno y/o gestionado por la propia organización, mediante una arquitectura y configuración de seguridad adecuadas a la relevancia del servicio de correo dentro del sistema de información, atendiendo a lo dispuesto en [op.exp.2]? *Nota: op.exp.2 requiere la configuración segura de los equipos con carácter previo a su puesta en producción (cuentas y contraseñas estándar, mínima funcionalidad, aplicación de guías de bastionados, etc.).*
	Si el servicio de correo es externo, revisar la documentación asociada a la seguridad y configuración del servicio, y evaluar si están implementados y cómo el resto de subcontroles (antispam, antimalware, etc.).
	¿Se protege la información distribuida por medio de correo electrónico, tanto en el cuerpo de los mensajes, como en los anexos? ¿Si se emplea criptografía, ésta es acorde con la información a proteger?
N0	**¿Se protege a la organización frente a problemas que se materializan por medio del correo electrónico?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se dispone de herramientas de filtrado del correo no deseado o 'spam'?
N0	¿Se dispone de herramientas de protección contra el código dañino que pueda estar presente en los mensajes de correo electrónico (AV de correo, sandbox, etc.)?
	¿Se dispone de herramientas que detecten el código móvil de tipo micro aplicación, en su expresión inglesa 'applet'?
	¿Se bloquea el envío/recepción de archivos de ciertas extensiones? NOTA: Ejemplos de extensiones que potencialmente pueden suponer una amenaza: .exe, .bat, .vbs, .cab, .scr, .ps1, .js, etc.).
	¿Se han implantado medidas de seguridad para prevenir la suplantación de identidad (por ejemplo, SPF, DKIM y DMARC)?
N0	**¿Se han establecido para el personal normas de uso seguro del correo electrónico?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

N0	¿Se organizan actividades de concienciación y formación relativas al uso del correo electrónico?
	¿Se establecen en la normativa limitaciones al uso del correo electrónico como soporte de comunicaciones privadas?

NOTA sobre SPF, DKIM y DMARC

Los registros o protocolos de autenticación SPF, DKIM y DMARC ayudan a evitar que se manden correos suplantando nuestra identidad (*phishing*). También sirven para dar más seguridad a los servidores de destino de nuestros correos y así evitar, dentro de lo posible, que sean marcados como SPAM.

***SPF** (Sender Policy Framework)*

Se encarga de certificar qué IP pueden mandar correo utilizando el dominio en cuestión. Este registro es eficaz contra los ataques de phishing. También ayuda a que los servidores de destino tengan más confianza y no cataloguen correos legítimos enviados por ti como SPAM.

***DKIM** (Domain Keys Identified Mail)*

Es un registro que permite firmar el correo con tu dominio mediante claves públicas indicadas en las zonas de tu dominio. De este modo, el destinatario está seguro de que el correo ha sido enviado desde tu servidor y no ha sido interceptado y/o reenviado desde otro servidor no autorizado.

***DMARC** (Domain-based Message Authentication, Reporting and Conformance)*

DMARC complementa al SPF y DKIM. Este registro indica qué hacer cuando dan error los registros anteriores, para así poder tomar las medidas necesarias lo antes posible.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.6.3: Protección de la navegación web

La entidad implementa una adecuada protección frente a las amenazas propias del servicio de navegación web.

Requisitos:

Mp.s.3	El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:
Mp.s.3.1	–Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
Mp.s.3.2	–Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
Mp.s.3.3	–Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
Mp.s.3.4	–Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
Mp.s.3.5	–Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
Mp.s.3.6	–Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo spyware, ransomware, etc.
Mp.s.3.7	–Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.
mp.s.3.r1.1	Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
mp.s.3.r1.2	Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

Propuesta de evidencias:

	☐	Normativa de uso seguro de navegación web.
	☐	Evidencias de campañas sobre navegación web segura.
	☐	Evidencia de las acciones formativas dirigidas al personal encargado de la monitorización.
	☐	Evidencias de protecciones implementadas frente a amenazas de la navegación web.
	☐	Política de cookies.
	☐	Evidencias de registros de monitorización de la navegación web.
	☐	Evidencias de listas negras de URL o destinos no permitidos.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se protege, frente a las amenazas que le son propias, el acceso de los usuarios internos a navegar por internet?** ☐ SI ☐ NO *NOTA: Dependiendo de la arquitectura de red de la entidad, lo más probable es que la navegación web se realice y gestione o bien a través del firewall de perímetro o bien a través de un proxy de*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	navegación dedicado. Teniendo en cuenta esta consideración, analizar en el dispositivo que corresponda, la configuración de los aspectos recogidos en el requisito. Entre otros: • Protección frente a la descarga de código potencialmente malicioso (AV, sandboxing, bloqueo de archivos por extensiones, etc.). • Filtrado de la navegación web basado en criterios reputacionales. • Implementación de listas negras • …
Espacio disponible para la redacción de la respuesta	
N0	¿Se ha establecido una normativa destacando el uso de internet que se autoriza y las limitaciones de uso personal? ¿se concreta el uso permitido de conexiones cifradas?
N0	¿Se llevan a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos? NOTA: *Obtener evidencia de las acciones de formación y concienciación con contenidos relacionados con la navegación web, considerando su periodicidad y número de asistentes.*
N0	¿Se protege a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web? *NOTA: Por ejemplo, efectuando una configuración de seguridad de los navegadores siguiendo orientaciones de guías de configuración segura como es la CCN-CERT BP/17 Recomendaciones de seguridad de Mozilla Firefox.*
	Revisar el uso de guías de configuración segura para los dispositivos que permiten la navegación (firewall, proxy de navegación, etc.).
	¿Se forma al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes? *NOTA:* Obtener evidencia de la formación impartida al personal responsable de la administración y gestión del servicio de navegación web, para confirmar que se les ha formado en monitorización y respuesta a incidentes. Revisar contenido del curso, fecha de impartición, duración y asistentes.
	¿Se protege contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo spyware, ransomware, etc.?
	¿Se ha establecido una política ejecutiva de control de cookies?
N0	**¿Se han establecido restricciones a la navegación y la monitorización de esta?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
N0	¿Se registra el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos?
N0	¿Se ha establecido una lista negra de destinos vetados?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.6.4: Protección de servicios y aplicaciones web

La entidad implementa una adecuada protección de los servicios y aplicaciones web.

Requisitos:

mp.s.2.1 mp.s.2.2 mp.s.2.3	Los sistemas que prestan servicios web deberán ser protegidos frente a las siguientes amenazas: – Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos: a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado. b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*). c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como cookies. d) Se prevendrán ataques de inyección de código. – Se prevendrán intentos de escalado de privilegios. – Se prevendrán ataques de cross site scripting.
mp.s.2.r1	– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción. – [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.
mp.s.2.r2	– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo. – [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web. – [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].
mp.s.2.r3.1	Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés".

Propuesta de evidencias:

	☐	Evidencias de uso de metodología de desarrollo seguro de aplicaciones web.
	☐	Procedimiento de auditoría.
	☐	Evidencias de uso de herramientas de detección de vulnerabilidades utilizadas en las auditorías.
	☐	Evidencias sobre el uso de otras herramientas para realizar las auditorías de caja negra y caja blanca.
	☐	Informes de auditorías técnicas de 'caja negra'.
	☐	Informes de auditorías técnicas de 'caja blanca'.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	☐	Evidencias sobre la corrección de los defectos identificados en las pruebas y auditorías de seguridad previos a la puesta en producción de la aplicación web.
	☐	Evidencias de prevención de ataques a 'proxies' y 'cachés.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Cuando la información requiera control de acceso ¿Se garantiza la imposibilidad de acceder a la información obviando la autenticación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado?
N0	¿Se previenen ataques de manipulación de URL?
N0	¿Se previenen ataques de manipulación de 'cookies'?
	¿Se previenen ataques de inyección de código?
	¿Se previenen intentos de escalado de privilegios?
	¿Se previenen ataques de 'cross site scripting'?
NOTA: Para categorías BÁSICA y MEDIA, debe cumplirse al menos con una de las medidas de refuerzo R1 o R2, que siguen a continuación, mientras que, para categoría ALTA, se requiere cumplir con R2 y R3.	
N0	**R1. ¿Se realizan auditorías de seguridad de 'caja negra' sobre las aplicaciones web?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se realizan auditorías técnicas de seguridad de "caja negra", de forma periódica, sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción?
N0	¿La frecuencia de las auditorías técnicas de seguridad está definido en un procedimiento de auditoría?
N0	**R2. ¿Se realizan auditorías de seguridad de 'caja blanca sobre las aplicaciones web?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se ha establecido una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones? *NOTA: Sin perjuicio que se puedan autorizar accesos cifrados singulares a destinos de confianza.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.7: Registro de entrada y salida de equipamiento

La entrada y salida de equipamiento del CPD y así como otro equipamiento esencial está adecuadamente controlada.

Requisitos:

mp.if.7.1	Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Propuesta de evidencias:

	☐	Evidencia del registro de entrada/salida.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se lleva un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se mantiene un registro de todo hardware y equipamiento esencial que entra y sale del CPD y salas técnicas, incluyendo la identificación de la persona que autoriza el movimiento y cualquier otra información que la organización estime conveniente?
	En caso de no ser el comportamiento habitual en la organización, ¿Se registra la entrada y salida de equipamiento portátil, por ejemplo, equipos personales y otros medios?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C7 – PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

C.7.1: Áreas separadas con control de acceso

El equipamiento del CPD y así como otro equipamiento esencial se encuentra ubicado en áreas que garantizan un control de acceso adecuado.

Requisitos:

mp.if.1.1 mp.if.1.2	– El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función. – Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Propuesta de evidencias:

	☐	Evidencia existencia de CPD y salas técnicas.
	☐	Evidencia existencia de mecanismos de seguridad para controlar el acceso.
	☐	Evidencia existencia de elementos de vigilancia y planos de ubicación debidamente protegidos.
	☐	Evidencia existencia de mecanismos de cierre en los racks

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se instala el equipamiento del sistema de información en áreas dotadas de adecuadas medidas de seguridad?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se instala el equipamiento del sistema de información, en la medida de lo posible, en áreas separadas específicas para su función dotadas con medidas de seguridad, como puede ser un CPD o una sala técnica?
N0	¿Se controlan los accesos a CPD y salas técnicas de forma que sólo se pueda acceder por las entradas previstas?
N0	¿Se dispone de mecanismos de seguridad para restringir el acceso únicamente al personal autorizado?
	Si el CPD es compartido por varias organizaciones, ¿se dispone de mecanismos de cierre en los armarios donde se ubique el equipamiento propio, o en las jaulas que albergan un conjunto de armarios, de forma que ningún tercero no autorizado pueda tener acceso?
	¿Se dispone de cámaras de videovigilancia (CCTV) y/o detectores de intrusión para proteger las instalaciones, especialmente fuera del horario laboral?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.2: Identificación de personas

El control de acceso al equipamiento del CPD y a otro equipamiento esencial se encuentra adecuadamente gestionado.

Requisitos:

mp.if.2.1	[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Propuesta de evidencias:

	☐	Protocolo de solicitud y concesión de autorizaciones de acceso a CPD, esporádicas y permanentes.
	☐	Evidencia del sistema de gestión y control de accesos.
	☐	Evidencia de consultas a la base de datos de entradas y salidas del CPD.
	☐	Libro de visitas del CPD.
	☐	Evidencia de comunicado de confirmación de acceso a las visitas, incluyendo normas de uso del CPD.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de una sistemática de control de acceso a los CPD?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se dispone de procedimientos de solicitud de acceso a CPD y salas técnicas, gestionando la concesión de autorizaciones temporales y permanentes?
N0	¿Se dispone de un sistema de control de acceso que identifique a las personas que accedan a los CPD donde hay equipamiento esencial para el sistema de información, registrando las correspondientes entradas y salidas?
	¿Se les comunica a las visitas externas junto a la autorización de acceso (por ejemplo, por correo electrónico), un ejemplar de las normas de uso del CPD?
	¿Dichas normas de uso determinan que las visitas externas estén siempre acompañadas?
	¿Se dispone de mecanismos ágiles para poder determinar quién estaba presente en el CPD, o sala técnica, en el momento de producirse un incidente de seguridad?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.3: Acondicionamiento de los locales

El acondicionamiento de los locales donde está el CPD y otro equipamiento esencial es el adecuado.

Requisitos:

mp.if.3.1 mp.if.3.1 mp.if.3.2 mp.if.3.3	Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar: – Las condiciones de temperatura y humedad. – La protección frente a las amenazas identificadas en el análisis de riesgos. – La protección del cableado frente a incidentes fortuitos o deliberados.

Propuesta de evidencias:

	☐	Evidencia de gráficos o listados de evolución de temperatura (T) y humedad relativa (HR) en el CPD o sala técnica.
	☐	Evidencia de cables de alimentación y de señal, organizados y etiquetados.
	☐	Evidencia de posible herramienta software de representación del conexionado entre el equipamiento.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se acondicionan y controlan ambientalmente los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, así como se dispone en ellos de un trazado organizado e identificado de los cables de señal y de alimentación?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se controlan las condiciones de temperatura y humedad en los locales donde se ubica el equipamiento, de modo que se asegure su eficaz funcionamiento de acuerdo con las especificaciones del fabricante? *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos.*
	¿Los equipos de climatización, están amparados por el correspondiente contrato de mantenimiento con revisiones periódicas?
	¿Se ha implementado en los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, la protección frente a las amenazas identificadas en el análisis de riesgos?
N0	¿Está protegido eficazmente el cableado en los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, de modo que se asegure su función frente a incidentes fortuitos o deliberados?
	¿Están organizados y peinados el cableado y las fibras ópticas en los armarios rack, mediante sistemas pasacables? ¿están etiquetados los extremos de cables y fibras? ¿las canalizaciones de cables entre racks están protegidas, organizadas y con la separación adecuada entre alimentación y datos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.4: Energía eléctrica

El equipamiento del CPD y así como otro equipamiento esencial dispone de medidas que garantizan el suministro adecuado de energía eléctrica.

Requisitos:

mp.if.4.1	– Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.
mp.if.4.r1.1	En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Propuesta de evidencias:

	☐	Evidencia SAI y generadores, % de carga y duración baterías.
	☐	Posible acuerdo de aprovisionamiento preferente de gasóleo para generadores eléctricos.
	☐	Evidencia de contratos de mantenimiento y boletines de la última revisión.
	☐	Informes de baja/media/alta tensión.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Los locales donde se ubican los sistemas de información y sus componentes esenciales (CPD, sala técnica), ¿disponen de tomas de energía eléctrica adecuadas, de modo que se garantice tanto el suministro como el correcto funcionamiento de las luces de emergencia?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	**En caso de fallo del suministro principal, ¿se garantiza el abastecimiento eléctrico durante el tiempo requerido, de forma armonizada con el BIA?** **¿se realizan pruebas de carga o en vacío de los grupos electrógenos?** ☐ SI ☐ NO *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos y/o en el BIA.*
	Espacio disponible para la redacción de la respuesta
	En caso de no disponerse de generador eléctrico de gasóleo (grupo electrógeno), ¿la duración de las baterías del SAI permite soportar cortes de suministro lo suficientemente amplios para cubrir los requisitos del BIA o, al menos, para permitir una parada ordenada de los equipos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿En caso de disponerse de generador eléctrico, ¿la capacidad del depósito de gasóleo o suministro de gas es suficiente para mantener la alimentación eléctrica del equipamiento el tiempo requerido? ¿la duración de las baterías del SAI es suficiente para la puesta en marcha del generador? *NOTA: Únicamente en caso de ser necesario el uso del grupo electrógeno para el mantenimiento de la alimentación eléctrica debido al tamaño y condiciones del CPD.*
	¿Los SAI (incluyendo las baterías internas o, en su caso, las bancadas externas) y los generadores eléctricos, en el caso de disponerse de estos últimos, están amparados por un contrato de mantenimiento, con revisiones periódicas? ¿se dispone de partes de mantenimiento acordes a la legislación vigente y a las instrucciones de los fabricantes?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.5: Protección frente a incendios

El equipamiento del CPD y así como otro equipamiento esencial se encuentra ubicado en áreas que disponen de la protección adecuada frente a incendios.

Requisitos:

mp.if.5.1	– Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Propuesta de evidencias:

	☐	Evidencia de los sistemas de detección y alerta.
	☐	Evidencia de los sistemas de extinción.
	☐	Evidencia de contratos de mantenimiento y partes de mantenimiento conforme a la legislación vigente.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Los locales donde se ubican los sistemas de información y sus componentes esenciales (CPD y salas técnicas) ¿están protegidos frente a los incendios atendiendo, al menos, a la normativa industrial de aplicación?** *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos. En ocasiones, será necesario disponer de sistemas de extinción automática.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se dispone de sistemas de detección de incendios?
	Si se activa un sensor (o en ocasiones dos de ellos para obviar falsos positivos), ¿la centralita de alarmas envía mensajes por los cauces previstos al personal de seguridad o de mantenimiento, a un centro externo coordinador de avisos de alarma, dispara una sirena, etc.?
N0	¿Se dispone de sistemas, manuales o automáticos, de extinción de incendios?
N0	¿Los sistemas de detección y extinción están amparados por un contrato de mantenimiento, con revisiones periódicas?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.6: Protección frente a inundaciones

El equipamiento del CPD y así como otro equipamiento esencial se encuentra ubicado en áreas que disponen de la protección adecuada frente a inundaciones.

Requisitos:

mp.if.6.1	– Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Propuesta de evidencias:

	☐	Evidencia de los sistemas detectores de líquidos.
	☐	Evidencia de la existencia de bombas de achique, si procede.
	☐	Evidencia de posibles contratos de mantenimiento y boletines de la última revisión.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Los locales donde se ubican los sistemas de información y sus componentes esenciales ¿están protegidos frente a incidentes causados por el agua?** *NOTA: En función de la ubicación del CPD (sótano o planta elevada), de la existencia de suelo técnico, etc., podrá variar el nivel de exigencia de esta medida (empleo de detectores de líquidos, bombas de achique automáticas, etc.).* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se dispone de sistemas de detección de humedad y de líquidos, habitualmente bajo el suelo técnico de CPD y salas técnicas, con atención a las pérdidas de los equipos de refrigeración ubicados en la sala, especialmente si funcionan con agua?
	¿Se dispone bombas de achique automático en pozuelas de recogida de aguas o, en su defecto, de la preinstalación para ubicar una bomba portátil?
	¿Los sistemas de detección de líquidos y de achique están amparados por un contrato de mantenimiento, con revisiones periódicas? ¿se realizan pruebas de arranque de las bombas de achique?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.7.7: Registro de entrada y salida de equipamiento

La entrada y salida de equipamiento del CPD y así como otro equipamiento esencial está adecuadamente controlada.

Requisitos:

mp.if.7.1	Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Propuesta de evidencias:

	☐	Evidencia del registro de entrada/salida.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se lleva un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se mantiene un registro de todo hardware y equipamiento esencial que entra y sale del CPD y salas técnicas, incluyendo la identificación de la persona que autoriza el movimiento y cualquier otra información que la organización estime conveniente?
	En caso de no ser el comportamiento habitual en la organización, ¿Se registra la entrada y salida de equipamiento portátil, por ejemplo, equipos personales y otros medios?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.8 – GESTIÓN DE INCIDENTES

C.8.1: Procedimiento, notificación, detección y respuesta de incidentes

La entidad dispone de procedimientos para la gestión de incidentes de seguridad.

Requisitos:

op.exp.7.1	– Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
op.exp.7.2	– La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.
op.exp.7.r1	Notificación.
op.exp.7.r1.1	– Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.
op.exp.7.r2	Detección y Respuesta. El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:
op.exp.7.r2.1	– Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
p.exp.7.r2.2	– Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
op.exp.7.r2.3	– Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.
op.exp.7.r2.4	– Medidas para: a) Prevenir que se repita el incidente. b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente. c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Propuesta de evidencias:

	☐	Proceso de tratamiento de incidentes.
	☐	Evidencia de que se distinguen y tratan adecuadamente los incidentes que afecten a datos personales.
	☐	Evidencia de instrumentos para notificar incidentes al CCN-CERT cuando corresponda
	☐	Evidencia de que se dispone de una completa gestión de incidentes
	☐	Proceso recogido en un procedimiento aprobado formalmente.

Procedimientos de auditoría (aspectos a evaluar):

N0	¿Se dispone de un proceso integral para tratar los incidentes que puedan tener un impacto en la seguridad del sistema? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	El proceso implantado para la gestión de incidentes ha sido documentado en un procedimiento aprobado formalmente.
N0	Se dispone de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación?
N0	La gestión de incidentes que afecten a datos personales, ¿tiene en cuenta lo dispuesto en el RGPD y en la LO 3/2018 (LOPDGDD), en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el RD 311/2022, de 3 de mayo?
	¿Se dispone de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT? ¿permite la distribución de notificaciones a las diferentes entidades de manera federada, si es el caso, utilizando para ello dependencias administrativas jerárquicas?
	Espacio disponible para la redacción de la respuesta

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿consiste en una completa gestión de los mismos?
	Espacio disponible para la redacción de la respuesta
	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye la implementación de medidas urgentes según convenga al caso? *NOTA: Se entiende por medidas urgentes la posibilidad de detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, etc.*
	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente?
	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye instrumentos o directrices para informar a los responsables de la información y servicios afectados, respecto al incidente acaecido y las actuaciones llevadas a cabo para su resolución?
	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye medidas para prevenir que se repita el incidente, incluir en los procedimientos de usuario la identificación y forma de tratar el incidente y actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.8.2: Registro de los incidentes de seguridad

La entidad ha definido, documento e implantado estándares de configuración segura para todos los sistemas operativos y sistemas previa a su entrada en producción.

Requisitos:

op.exp.9	Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:
op.exp.9.1	– Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
op.exp.9.2	– Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
op.exp.9.3	– Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Propuesta de evidencias:

	☐	Evidencia de que se registran los incidentes clasificándolos por tipología.
	☐	Evidencia de acciones adoptadas, en base al análisis de los incidentes registrados.

Procedimientos de auditoría (aspectos a evaluar):

N0	¿Se realiza un proceso de extracción de conclusiones y aprendizaje, a partir de los incidentes de seguridad registrados? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se registran los reportes iniciales, intermedios y finales, las actuaciones de emergencia y las modificaciones del sistema derivadas de un incidente?
	¿Se registran aquellas evidencias que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos? *NOTA: En la determinación de la composición y detalle de estas evidencias, así como la forma de preservar la cadena de custodia, se recurrirá a asesoramiento legal especializado y/o a peritos judiciales.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	Como consecuencia del análisis de los incidentes, ¿se revisan aquellos eventos que deben seguir auditándose y la necesidad de reducirlos o incrementarlos?
N0	¿Se realiza un aprendizaje, a partir del análisis de los incidentes registrados, que permita poner de manifiesto aspectos a mejorar en la seguridad del sistema?
N0	Para aprender de los incidentes, ¿se registran éstos indicando su tipología concreta y no solo diferenciando los de seguridad de los que no lo son? *NOTA: Se dispone de una clasificación o taxonomía de los ciberincidentes en la guía CCN-STIC 817 Gestión de ciberincidentes*.

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C9 – MONITORIZACIÓN DEL SISTEMA Y SU SEGURIDAD

C.9.1: Herramienta de monitorización de redes y sistemas

La entidad dispone de una herramienta de monitorización de redes y sistemas.

Requisitos:

	Se dispone de herramientas que monitorizan el estado de los activos de la entidad, incluyendo redes y sistemas.
	Los eventos detectados por el sistema de monitorización son registrados, para su consulta y procesamiento posterior.

Propuesta de evidencias:

	☐	Evidencia de acceso a la consola de monitorización de la herramienta.
	☐	Evidencia de la tipología de activos monitorizados por la herramienta.
	☐	Evidencia de las capacidades de monitorización de la herramienta, incluyendo estado de los dispositivos, estado de los servicios, rendimiento, etc.
	☐	Evidencia sobre la información almacenada por la herramienta de monitorización y su adecuación para procesamientos posteriores, incluyendo: - revisión de eventos para ejecución de mantenimiento preventivo - correlación eventos para identificar causa raíz. - detección de incidentes de seguridad. - consulta de históricos para análisis forense de incidentes de seguridad.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se dispone de herramientas que permitan la monitorización del estado de redes y sistemas? NOTA Verificar si existen una o varias herramientas para la monitorización de cada una de las tipologías de activos existentes. Verificar las capacidades de monitorización de la herramienta, incluyendo estado de los dispositivos, estado de los servicios, rendimiento. ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Existe personal asignado a la monitorización para la detección de eventos?
	¿Existen procedimientos o automatizaciones para el tratamiento de la información y alarmas generadas por el sistema o los sistemas de monitorización?
	¿Proporciona la herramienta información sobre los eventos detectados en las redes y sistemas?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Es almacenada esa información para su consulta o explotación posterior? ¿Durante cuánto tiempo? *NOTA* *Verificar si la información recopilada por la herramienta de monitorización incluye el registro y almacenamiento de los eventos detectados, para aplicación de controles posteriores, incluyendo controles preventivos e investigación de incidentes.*
	¿Se dispone o se han previsto interfaces o accesos para permitir la explotación de dicha información por otros sistemas?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.9.2: Detección de intrusión

Se dispone de sistemas o herramientas que permiten la detección o prevención de intrusiones.

Requisitos:

op.mon.1.1	Se dispondrá de herramientas de detección o prevención de intrusiones
op.mon.1.r1.1	El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.
op.mon.1.r2.1	Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.
op.mon.1.r3.1	El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Propuesta de evidencias:

	☐	Evidencia de la herramienta de IPS/IDS.
	☐	Para el sector público, posible evidencia de sonda tipo SAT-INET del CCN-CERT.
	☐	Evidencia de las reglas definidas en el IPS/IDS.
	☐	Evidencia del procedimiento de respuesta a las alertas generadas por el IDS.
	☐	Evidencia de acciones automáticas generadas por el IDS.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de herramientas de detección y/o prevención de intrusiones (IDS/IPS)?** *NOTA* *Verificar que las herramientas con capacidades IDS/IPS tienen estas funcionalidades habilitadas.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se dispone de elementos que analicen el tráfico de red y muestren eventos de seguridad en caso de detectar posibles intrusiones en la misma? *NOTA* *Por ejemplo, sondas IDS/IPS, capacidad IDS/IPS en los cortafuegos, panel de monitorización de eventos en Cloud, sonda SAT-INET del CCN-CERT, etc.*
	¿Dispone el sistema de herramientas de detección y/o prevención de intrusiones basadas en reglas?
	¿Se han configurado reglas específicas para la generación de eventos de seguridad y la detección de intrusiones?
	¿Se dispone de procedimientos de respuesta a las alertas generadas por el sistema de detección y/o prevención de intrusiones?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	NOTA *Verificar si existe un proceso establecido para el tratamiento adecuado de los eventos detectados o tratados por la herramienta*
	¿El sistema ejecuta automáticamente acciones predeterminadas de respuesta a las alertas generadas por las herramientas de detección y/o prevención de intrusiones? *NOTA* *Dichas acciones automáticas pueden incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.9.3: Vigilancia

Se dispone de un sistema automático de recolección de eventos de seguridad.

Requisitos:

op.mon.3.1	Se dispondrá de un sistema automático de recolección de eventos de seguridad
op.mon.3.r1.1	Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos
op.mon.3.r3.1	Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.
op.mon.3.r3.2	Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat, APT) mediante la detección de anomalías significativas en el tráfico de la red.
op.mon.3.r4.1	Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.
op.mon.3.r5.1	Limitación de las consultas, monitorizando volumen y frecuencia.
op.mon.3.r5.2	Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.
op.mon.3.r6.1	Verificación de configuración.
op.mon.3.r6.3	Pruebas de penetración.
op.mon.3.r7.1	En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Propuesta de evidencias:

	☐	Evidencia del sistema empleado para recolección de eventos de seguridad.
	☐	Evidencia del sistema de correlación de LOGS.
	☐	Evidencia de sistema de generación de alertas según el tráfico de red.
	☐	Evidencia de contrato de prestación de servicios de vigilancia y monitorización remota, tipo SOC, de estar externalizado
	☐	Evidencia de limitación y monitorización de posibilidades de minería de datos.
	☐	Evidencia de pruebas de penetración y acciones correctivas derivadas.
	☐	Evidencia de informes de verificación de la configuración y acciones correctivas derivadas.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de un sistema automático de recolección de eventos de seguridad?** *NOTA* *Verificar que existe un proceso organizado que se ha establecido, mediante distintas herramientas o medidas de vigilancia, con el objeto de mantener a la organización informada de eventos de seguridad.* *Verificar que la gestión de este proceso se encuentra respaldado mediante el uso de herramientas de gestión de flujos de trabajo o ticketing, o mediante medios alternativos de control* ☐ SI ☐ NO

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	Espacio disponible para la redacción de la respuesta
N0	¿Se dispone de un sistema automático de recolección de eventos de seguridad, como puede ser un servidor syslog en base, por ejemplo, al protocolo del mismo nombre?
	¿Se dispone de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos? *NOTA* *Por ejemplo, un repositorio centralizado de eventos, un SIEM, paneles de control de monitorización de eventos en soluciones Cloud, etc.*
	¿Se dispone de sistemas para detección de amenazas avanzadas?
	¿Se dispone de sistemas para la detección de amenazas avanzadas y comportamientos anómalos?
	¿Se dispone de sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat - APT) mediante la detección de anomalías significativas en el tráfico de la red?
	¿Se dispone de observatorios de cibervigilancia, propios o contratados como prestación de servicios?
	¿Se dispone de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías, que pudieran representar indicadores de amenaza, en contenidos digitales? *NOTA* *Puede tratarse, por ejemplo, de un SOC interno, o externo, contratado como prestación del servicio de monitorización remota y gestión de alertas; servicios de vigilancia, por ejemplo, de existencia de cuentas de la Organización comprometidas tras ataques de phishing, exfiltraciones de datos en un ciberincidente, o simplemente en venta en la 'Dark web'.*
	¿Se dispone de medidas frente a la minería de datos?
	¿Se aplican medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos, limitando las consultas y monitorizando su volumen y frecuencia?
	¿Se dispone de medidas que alerten a los administradores de seguridad de comportamientos sospechosos en tiempo real que puedan representar intentos de minería de datos?
	¿Se realizan inspecciones y auditorías técnicas periódicamente o tras un incidente?
	¿Se verifica la configuración periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema, ya sean estas nuevas, o que hubieran sido subestimadas en su momento?
	¿Se realizan pruebas de penetración periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema, ya sean estas nuevas, o que hubieran sido subestimadas en su momento?
	En las interconexiones que lo requieran, ¿se aplican controles en los flujos de intercambio de información a través del uso de metadatos?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.9.4: 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.

Requisitos:

op.exp.8.1	Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
op.exp.8.2	Se activarán los registros de actividad en los servidores.
op.exp.8.r5.1	El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
op.exp.8.r5.2	Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Propuesta de evidencias:

	☐	Evidencia de los registros de actividad conservados.
	☐	Evidencia de configuración de los registros de actividad (LOGS) en los servidores.
	☐	Evidencia de revisión de los registros de actividad centralizados.
	☐	Evidencia de servidores NTP o equivalentes.
	☐	Documentación de seguridad del sistema sobre gestión de registros de actividad.
	☐	Evidencia de protección del acceso a los registros de actividad
	☐	Evidencia de herramientas de análisis de LOGS.
	☐	Evidencia de sistemas automáticos de recolección de registros y correlación de eventos (tipo SIEM).

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

Procedimientos de auditoría (aspectos a evaluar):

NI	**¿Se registran los eventos y actividades de usuarios y entidades que acceden a los sistemas?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
NI	¿Se registran las actividades del sistema generando un registro de auditoría que incluye, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma?
NI	¿Se han activado los registros de actividad en los servidores?
	¿Se dispone de herramientas para apoyar la gestión de los registros de actividad? *NOTA* *Verificar que existe un proceso organizado que se ha establecido, mediante distintas herramientas, con el objeto realizar un análisis avanzado de los eventos de seguridad registrados para la detección de amenazas.* *Verificar que la gestión de este proceso se encuentra respaldado mediante el uso de herramientas de gestión de flujos de trabajo o ticketing, o mediante medios alternativos de control.*
	¿El sistema implementa herramientas para analizar y revisar de forma centralizada la actividad del sistema y la información de auditoría en búsqueda de comprometimientos de la seguridad posibles o reales?
	¿Se dispone de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos, como puede ser un SIEM?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C10 – PROTECCIÓN DE REDES Y COMUNICACIONES

C.10.1: Protección por Firewall

La entidad dispone de protección por Firewall y se encuentra correctamente configurado y mantenido.

Requisitos:

mp.com.1.1	Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
mp.com.1.2	Todos los flujos de información a través del perímetro deben estar autorizados previamente

Propuesta de evidencias:

	☐	Esquema de red.
	☐	Configuración del sistema de protección perimetral.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se dispone de algún sistema que asegure el perímetro lógico?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se dispone de un sistema de protección perimetral que separe la red interna del exterior? *NOTA* *Verificar en el esquema de red que se dispone de un perímetro concreto, delimitado y acotado, reflejado en la arquitectura del sistema. Confirmar que, por diseño, todo el tráfico con el exterior pasa a través del cortafuegos y sólo se permite el tráfico que ha sido previamente autorizado.*
	Caso de disponerse de varias sedes o centros de datos ¿disponen todos ellos de protección perimetral?
	El sistema empleado para asegurar el perímetro ¿Es atravesado por todo el tráfico, sin excepción?
	¿Ofrece la solución de firewall por arquitectura y tecnología el nivel de seguridad propias del tipo NGFW (Next Generation Firewall) o UTM (Unified Threat Management)? *NOTA* *Verificar si la solución de firewall implementada ofrece funcionalidades propias del tipo NGFW (Next Generation Firewall) o UTM (Unified Threat Management):* *-IDS* *-IPS* *-DPI (Deep Packet Inspection)* *-Application Inspection* *-DLP (Data Leak Prevention)* *-Inspección de tráfico encriptado.*
	Los cambios en las reglas del firewall llevan un proceso de revisión y aprobación. (Control de gestión cambios).

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.10.2: Arquitectura de protección

Se tienen en cuenta las necesidades de seguridad en el diseño de la red.

Requisitos:

op.pl.2	La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:
op.pl.2.2	Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración)
op.pl.2.3	Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa
mp.com.1.1	Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.

Propuesta de evidencias:

	☐	Planos de CPD y salas técnicas, incluyendo sus instalaciones (climatización, extinción, alimentación eléctrica, etc.).
	☐	Documentación y diagramas de red, incluyendo comunicaciones y líneas de defensa.
	☐	Documentos de arquitectura del sistema.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se ha realizado un diseño adecuado de la arquitectura de la solución para proporcionar el nivel de seguridad requerido? *NOTA* *Verificar si el diseño de red se ha realizado considerando criterios de seguridad, bien mediante el asesoramiento de expertos internos o externos o la consideración de guías de diseño de fabricantes y/o organismos de referencia*. ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se dispone de documentación que en su conjunto describa la arquitectura de sistema de la entidad? ¿Se dispone en dicha documentación de diagramas de red detallados, incluyendo diagramas físicos y lógicos? ¿Se dispone de un plan de direccionamiento? ¿Se encuentra la documentación actualizada?
	¿El sistema de cortafuegos consta de dos o más equipos de diferente fabricante dispuestos en cascada?
	¿Se ha implementado una DMZ mediante el uso de firewalls en cascada?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Se ha implementado una arquitectura de protección de perímetro de acuerdo con lo descrito en la Guía de Seguridad de las TIC CCN-STIC 811 Interconexión en el ENS? ¿Qué arquitectura se ha utilizado?
	¿Se dispone de sistemas redundantes?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.10.3: Conexiones Exteriores Seguras

Se utilizan conexiones seguras para conexiones desde el exterior de la entidad.

Requisitos:

mp.com.2.1	Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
mp.com.2.r1.1	Se emplearán algoritmos y parámetros autorizados por el CCN.

Propuesta de evidencias:

	☐	Evidencia empleo de VPN.
	☐	Evidencia de los algoritmos de cifrado que se emplean en las VPN.

Procedimientos de auditoría (aspectos a evaluar):

	¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad, por lo que deba cifrarse? *NOTA* *Verificar los terminadores de túneles existentes en la electrónica de red o la electrónica perimetral.* *Verificar el historial de conexiones en dichos terminadores.* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se emplean algoritmos y parámetros autorizados por el CCN para cifrar las comunicaciones que discurran fuera del dominio de seguridad? *NOTA* *Verificar las configuraciones técnicas de las conexiones privadas virtuales, para confirma el uso de protocolos criptográficos adecuados. Y, en caso de utilizarse, los dispositivos cifradores.* *Utilizar para la verificación de los protocolos, confirma con los contenidos en las secciones 3 y 4 de la Guía de Seguridad de las TIC CCN-STIC 807 de Mayo 2022 (https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file?format=html).*

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

C.10.4: Segmentación de Redes

Las redes se encuentran segmentadas.

Requisitos:

mp.com.4.1	El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita
mp.com.4.2	Si se emplean comunicaciones inalámbricas, será en un segmento separado
mp.com.4.r1.1	Los segmentos de red se implementarán por medio de redes de área local virtuales (Virtual Local Area Network, VLAN).
mp.com.4.r1.2	La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo: Usuarios. Servicios. Administración.
mp.com.4.r2.1	Los segmentos de red se implementarán por medio de redes privadas virtuales (Virtual Private Network, VPN).
mp.com.4.r3.1	Los segmentos de red se implementarán con medios físicos separados.

Propuesta de evidencias:

	☐	Evidencia de segmentación de red, incluyendo diagramas o listado de segmentos, si se dispone
	☐	Evidencia de monitorización de la interconexión de segmentos de red.
	☐	Evidencia de documento que defina el plan de direccionamiento IP de la entidad.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se ha segmentado la red, segregando el tráfico?** *NOTAS* *Verificar la configuración del elemento que realiza el routing entre subredes en la red de la entidad, bien sea el firewall o la electrónica de red.* *Verificar la existencia de distintas subredes y vlans, y la concordancia de la información contenida en el plan de direccionamiento.* ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	¿Se han separado en segmentos los flujos de información, segregando el tráfico por la red, de modo que cada equipo únicamente tenga acceso a la información que necesita?
	Si se emplean comunicaciones inalámbricas, ¿se concentran éstas mediante un segmento separado?
	¿Se han segregado al menos 3 segmentos de red mediante VLAN?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*

	¿Los segmentos de red se han implementado por medio de redes de área local virtuales (Virtual Local Area Network - VLAN)?
	¿Se ha segregado en distintas subredes la red que conforma el sistema, contemplando como mínimo la red de usuarios, la de servicios y la de administración?
	¿Se han implementado los segmentos de red por medio de redes privadas virtuales (Virtual Private Network - VPN)?
	¿Se han implementado los segmentos de red con medios físicos separados?

Leyenda y códigos de color:

	No es un requisito del ENS, pero por su importancia se añade a los CGTI
	Requisito "BASE" exigible a todas las categorías
	Requisito "BASE" o de "REFUERZO", exigible a las categorías MEDIA y ALTA
	Requisito "BASE" o de "REFUERZO", exigible a la categoría ALTA
	Requisito de "REFUERZO" a considerar
N0	*Requisito esencial. Si no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como 'no implementada'*
N2	*Procedimiento o normativa esencial. Si no se tiene formalizada, la calificación del control no puede pasar de N2.*
Negrita	*Pregunta principal del control*

*Sobre los niveles de madurez **N0** y **N2** ver apartado 16.2 de GPF-OCEX 5330.*