ÁREA B. GESTIÓN DE CAMBIOS EN APLICACIONES Y SISTEMAS

INTRODUCCIÓN

Esta GPF-OCEX 5332 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 **B. Gestión de cambios en aplicaciones y sistemas** 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 gestión de cambios deben ser implantados con el objeto de velar por una gestión sistemática y organizada de todas las modificaciones realizadas en el entorno TI, bien sean cambios en la configuración de los sistemas, en su arquitectura, o debidos a la adquisición o desarrollo y posterior puesta en operación de aplicaciones o nuevos equipos.*
>
> *Estos controles permiten asegurar que las actuaciones realizadas sobre el entorno TI se llevan a cabo manteniendo la operatividad de los sistemas y los niveles de seguridad establecidos.*
>
> *La gestión de cambios incluye la designación de responsables y la autorización de aquellos previamente a su ejecución, lo que permite asegurar que no se realizan cambios no controlados, asegurando que se cumplen todos los requisitos del proceso de gestión para cada actuación.*
>
> *La planificación previa de cada cambio permite que estos sean diseñados conforme a la arquitectura de seguridad de la entidad, y que se encuentren alineados con políticas, normativas y estrategias corporativas, evitando las actuaciones con objetivos no alienados con los generales de la entidad.*
>
> *La gestión correcta de cambios permite además asegurar que las modificaciones realizadas se integran adecuadamente, evitando interferir en la operatividad de los sistemas afectados y en el resto de los sistemas de la entidad, mediante la ejecución de pruebas planificadas en entornos seguros."*

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.

B1 – ADQUISICIÓN DE APLICACIONES Y SISTEMAS

B.1.1: Adquisición de aplicaciones y sistemas por objetivos estratégicos

Las aplicaciones y los sistemas se compran en base a un procedimiento establecido que tiene en consideración los objetivos estratégicos de la entidad.

Requisitos:

	El proceso seguido para planificar la adquisición de nuevos componentes del sistema tiene en consideración los objetivos estratégicos de la entidad.
	El proceso considera cómo TI puede dar soporte a los objetivos estratégicos de la entidad e incluye lo siguiente: ▪ Identificación de posibles soluciones ▪ Propuestas de adquisición ▪ Comparación de productos ▪ Aprobación ▪ Coherencia entre plan estratégico de la entidad y plan de sistemas

Propuesta de evidencias:

	☐	Procedimiento para identificar necesidades
	☐	Plan estratégico de TI
	☐	Plan anual de TI
	☐	Evidencia de aprobación de la adquisición

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿El proceso formal para planificar la adquisición de nuevos componentes del sistema tiene en consideración los objetivos estratégicos de la entidad?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	Existe un proceso gestionado para la identificación de necesidades y posterior adquisición del sistema/aplicación de TI.
	El proceso anterior se encuentra recogido en un procedimiento formalmente aprobado.
	Las necesidades identificadas se registran. En el registro se incluye toda la información necesaria para realizar el seguimiento de la petición, evaluarla, etc.
	La estructura de responsabilidades de la entidad establece claramente quién puede autorizar las solicitudes.
	La selección de la solución se realiza en base a criterios objetivos (definición clara de requisitos como base y posterior investigación de mercado, comparación de productos, análisis de estudios de referencia, etc.).
N0	Las soluciones propuestas están alineadas con el plan anual de sistemas y, a su vez, con el plan estratégico TI. La persona u órgano con competencias para ello, según la política, autoriza la adquisición.

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' o N0*
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.*

B.1.2: Adquisición de aplicaciones y sistemas atendiendo a las necesidades de seguridad

Las aplicaciones y los sistemas se compran en base a un procedimiento establecido que tiene en consideración los criterios de seguridad de la entidad, considera la totalidad de necesidades y la aprobación de la adquisición.

Requisitos:

Op.pl.3 3.1 3.2 3.3	Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que: ▪ Atenderá a las conclusiones del análisis de riesgos (op.pl.1). ▪ Será acorde a la arquitectura de seguridad escogida (op.pl.2). ▪ Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.
org.4.1	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos (hardware, aplicaciones, comunicaciones, etc.).

Propuesta de evidencias*:*

	☐	Documento sobre el proceso de adquisiciones que contemple la inclusión de las necesidades de seguridad.
	☐	Procedimiento que establezca cómo se formalizará la autorización de los nuevos elementos del sistema TI (hardware, aplicaciones, comunicaciones, etc.)
	☐	Pliegos de prescripciones técnicas (PPT) y de pliegos de cláusulas administrativas particulares (PCAP) correspondientes a los últimos procesos de adquisición de productos y/o servicios.
	☐	Documentos o registros de solicitud de adquisición de aplicaciones o sistemas con el contenido relativo a las necesidades de seguridad.
	☐	Si se emplea una herramienta de ticketing que las consolide, evidencia de tickets de peticiones de autorización.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se realiza una planificación previa a la adquisición de nuevos componentes del sistema, teniendo en cuenta, por ejemplo, la obsolescencia de los actualmente en producción, la finalización de contratos, los cambios del contexto, etc.?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
N2	¿Se dispone de un procedimiento formalizado y aprobado de planificación para la adquisición de nuevos componentes y que contemple la autorización de estas adquisiciones?
	¿La adquisición de sistemas requiere la autorización formal del órgano al que, en la política de seguridad, se le atribuyan las competencias en esta materia?
	Para los nuevos componentes a ser adquiridos ¿se verifica que sean acordes o compatibles con la arquitectura de seguridad implementada o escogida para la organización? De manera concreta, ¿contemplan los requisitos de seguridad que debe cumplir la nueva solución?

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' o N0*
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 de adquisición tiene en cuenta las conclusiones del análisis de riesgos, o bien provoca que deba realizarse una nueva iteración de dicho análisis, debido a los cambios que introduce en el sistema de información?
N0	¿El proceso de adquisiciones contempla conjuntamente las necesidades de financiación, de formación y las técnicas (características, configuración, soporte y mantenimiento)? *NOTA: La principal razón de ser de esta medida es que no se realicen adquisiciones de componentes en la organización considerando únicamente cuestiones económicas, sino que se base en razones técnicas que contemplen requisitos de seguridad para minimizar el riesgo.*

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' o N0*
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.*

B.1.3: Dimensionamiento en la adquisición de aplicaciones y sistemas

Las aplicaciones y los sistemas se compran considerando el correcto dimensionamiento para responder a las necesidades de la entidad.

Requisitos:

op.pl.4 4.1 4.2 4.3 4.4 4.5	Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos: ▪ Necesidades de procesamiento. ▪ Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse. ▪ Necesidades de comunicación. ▪ Necesidades de personal: cantidad y cualificación profesional. ▪ Necesidades de instalaciones y medios auxiliares.
op.pl.4.r1 op.pl.4.r1.1 op.pl.4.r1.2	Mejora continua de la gestión de la capacidad: ▪ Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema. ▪ Se emplearán herramientas y recursos para la monitorización de la capacidad.

Propuesta de evidencias:

	☐	Estudio previo de capacidad asociado a una adquisición, contemplando todos los aspectos necesarios.
	☐	Análisis de costes previo a la adquisición.
	☐	Evidencia de adquisiciones dimensionadas de forma alineada con el estudio previo.
	☐	Plan de capacidad, contemplando todos los aspectos necesarios.
	☐	Evidencia de herramientas de monitorización de la capacidad.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Con carácter previo a la entrada en producción del sistema, ¿se consideran las necesidades de capacidad?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se han considerado las necesidades de software y hardware, al menos con carácter previo a la puesta en explotación de los sistemas? *NOTA: Se entiende por software y hardware a las aplicaciones, CPU y memoria de servidores y estaciones de trabajo, VM necesarias, balanceadores de ser necesarios, etc.*
	¿Se ha realizado un estudio respecto a las necesidades de almacenamiento de información durante procesamiento y durante el período que deba retenerse, al menos con carácter previo a la puesta en explotación de los 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' o N0*
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 realizado un estudio respecto a las necesidades de capacidad de procesamiento, ya sea en hosts físicos, entornos virtualizados, o entornos de computación en la nube, al menos con carácter previo a la puesta en explotación del sistema?
	¿Se ha realizado un estudio respecto a las necesidades de comunicaciones (líneas y ancho de banda necesario), al menos con carácter previo a la puesta en explotación del sistema?
	¿Se ha realizado un estudio respecto a las necesidades de personal y carga de trabajo en cuánto a su número y cualificaciones profesionales, al menos con carácter previo a la puesta en explotación del sistema?
	¿Se ha realizado un estudio respecto a las necesidades de instalaciones, al menos con carácter previo a la puesta en explotación del sistema? *NOTA: Se entiende por necesidad de instalaciones a la posibilidad de adición de racks a los CPD, bahías libres en racks existentes, número de bocas libres en conmutadores, número máximo de VPN contra un cortafuegos, además de potencia frigorífica suficiente en los CPD, % de carga libre en los SAI, etc.*
N0	**¿Se puede evidenciar que el estudio de capacidad no solo se realiza con carácter previo a la entrada en producción del sistema, sino que se mantiene actualizado durante todo su ciclo de vida?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se puede evidenciar la existencia de un plan de capacidad, que se mantiene actualizado durante todo el ciclo de vida del sistema?
	¿Se emplean herramientas y recursos para la monitorización de la capacidad? *NOTA: La monitorización es básica para poder elaborar un plan de capacidad. Incluso existen herramientas que conservan datos históricos y permiten ver tendencias gráficamente, durante determinado período de tiempo seleccionado, posibilitando así poder tomar decisiones respecto a la previsión del consumo de recursos y su posible necesidad de ampliación.*

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' o N0*
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.*

B2 – DESARROLLO DE APLICACIONES

B.2.1: Metodología de desarrollo

El desarrollo de aplicaciones se realiza de manera metodológica. La metodología utilizada contempla la gestión de la seguridad durante todo el ciclo de vida y está alineada con los estándares y metodologías de desarrollo seguro.

Requisitos:

	La entidad dispone de una metodología de desarrollo que regula este proceso y establece los principales requisitos y controles que se deben observar durante todo su ciclo de vida.
mp.sw.1.r1 mp.sw.1.r1.1	Mínimo privilegio Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.
mp.sw.1.r2 mp.sw.1.r2.1	Metodología de desarrollo seguro. Se aplicará una metodología de desarrollo seguro reconocida que: a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida. b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (overflow). c) Tratará específicamente los datos usados en pruebas. d) Permitirá la inspección del código fuente.
mp.sw.1.r3 mp.sw.1.r3.1	Seguridad desde el diseño. Los siguientes elementos serán parte integral del diseño del sistema: a) Los mecanismos de identificación y autenticación. b) Los mecanismos de protección de la información tratada. c) La generación y tratamiento de pistas de auditoría.

Propuesta de evidencias:

	☐	Metodología de desarrollo utilizada por la entidad.
	☐	Metodología de desarrollo seguro utilizada por la entidad.
	☐	Evidencias sobre la implantación de los controles recogidos en la metodología (registro de solicitud de desarrollo, formalización y aceptación de requerimientos funcionales, documentación a generar durante el desarrollo, tipos de prueba a realizar, aceptación del resultado de las pruebas, etc.).
	☐	Análisis funcionales y técnicos de una muestra de los desarrollos realizados para verificar la inclusión del principio de seguridad desde el diseño y los criterios recogidos en la metodología de desarrollo 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' o N0*
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/N2	**¿La entidad dispone de una metodología o procedimiento de desarrollo de aplicaciones que contempla las fases y controles a lo largo de todo el ciclo de vida de desarrollo?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	El procedimiento de desarrollo regula la gestión de las peticiones (quién, a quién, cómo se registran, etc.).
	El procedimiento de desarrollo establece qué documentación se debe generar (formalización de requisitos, análisis funcional, análisis técnico, modelo de datos, arquitectura, etc.).
	El procedimiento de desarrollo establece la necesidad de utilizar entornos de desarrollo diferentes al entorno de producción.
	El procedimiento so de desarrollo recoge la tipología de pruebas a realizar y el detalle de cómo realizarlas y documentarlas.
	¿Se aplica una metodología de desarrollo seguro reconocida? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	**¿Se tienen en cuenta aspectos de seguridad como parte integral del diseño del sistema?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Forman parte integral del diseño del sistema los mecanismos de identificación y autenticación?
N0	¿Forman parte integral del diseño del sistema los mecanismos de protección de la información tratada?
	¿Forman parte integral del diseño del sistema la generación y tratamiento de pistas de auditoría?

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' o N0*
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.*

B.2.2: Entornos de desarrollo

El desarrollo de aplicaciones se realiza en sistemas o entornos separados de producción.

Requisitos:

Mp.sw.1.1	El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Propuesta de evidencias:

	☐	Evidencia de separación de los entornos de producción y desarrollo.
	☐	Evidencia de medidas de seguridad del repositorio de código fuente del entorno de desarrollo y del de producción (por ejemplo, usuarios con permisos de lectura, escritura y modificación sobre directorios, usuarios con acceso a las bbdd de cada entorno, etc.).
	☐	Evidencia de uso de una herramienta de control de versiones para la gestión del código fuente.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Está separado a todos los efectos el entorno de desarrollo del de producción?** *NOTA: Habitualmente se dispone de entornos de desarrollo, preproducción o test, y producción.* *NOTA: Se debe valorar la "completitud" de los entornos de desarrollo, considerando todos los elementos que intervienen en el correcto funcionamiento de las aplicaciones (frontales, middleware, bases de datos, LDAPs, etc.).* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	La metodología de desarrollo contempla la existencia de los diferentes entornos (desarrollo, preproducción, etc.).
	¿Se han separado los entornos de desarrollo y pruebas del de producción, realizándose el desarrollo sobre sistemas diferenciados de los productivos?
	¿Existen herramientas de desarrollo o datos de prueba en el entorno de producción o elementos productivos o datos reales en el entorno de desarrollo?
	¿Se han aplicado medidas de seguridad sobre los repositorios de código fuente?
	¿Se han aplicado medidas de seguridad sobre los repositorios donde se encuentra el código en desarrollo?
	¿Se utiliza una herramienta para la gestión del versionado de código fuente? ¿La herramienta anterior facilita la implementación de controles de integridad sobre el código desarrollado (*no permite modificaciones en paralelo simultáneas del mismo elemento, registro de fechas de última modificación, etc.)*?
	¿Se utiliza una herramienta/scripts de pase a producción? En caso afirmativo, ¿se utiliza esta utilidad para restringir el acceso al código existente en los distintos entornos?

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' o N0*
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.*

B.2.3: Datos de prueba

El desarrollo de aplicaciones se realiza en sistemas o entornos separados de producción. En las pruebas no se utilizarán datos reales. En caso contrario, se garantizará el nivel de seguridad correspondiente.

Requisitos:

Mp.sw.1.r4.1	Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Propuesta de evidencias:

	☐	Evidencia del proceso de generación de los datos de prueba.
	☐	Evidencia de la seguridad en los datos de prueba reales, si procede.
	☐	Metodología/procedimiento de desarrollo que establezca los criterios sobre los datos a utilizar en las pruebas.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se aseguran los datos reales empleados para las pruebas previas, evitando su uso en la medida de lo posible?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	¿La metodología aplicada tiene en cuenta los datos empleados en las pruebas?
	¿Se evita realizar con datos reales las pruebas previas a la implementación o modificación de los sistemas de información?
	¿Se utiliza una herramienta específica o scripts desarrollados por la entidad para la generación de los datos de prueba? *NOTA: Analizar cómo se generan los datos de prueba (ofuscando datos, mezclando datos, creando datos, etc.).*
	En caso de que fuese necesario recurrir a datos reales para las pruebas previas, ¿se garantiza el nivel de seguridad correspondiente, principalmente, garantiza el control de acceso a la información?

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' o N0*
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.*

B.2.4: Aceptación

La aceptación de aplicaciones desarrolladas se realiza de manera metodológica y considera los criterios de seguridad de la entidad.

Requisitos:

Mp.sw.2 Mp.sw.2.1	Aceptación y puesta en servicio. Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se comprobará que: a) Se cumplen los criterios de aceptación en materia de seguridad. b) No se deteriora la seguridad de otros componentes del servicio.
R2	Inspección de código fuente. Se comprobará que: a) Se cumplen los criterios de aceptación en materia de seguridad. b) No se deteriora la seguridad de otros componentes del servicio.

Propuesta de evidencias:

	☐	Evidencia de las pruebas y la verificación de los criterios de aceptación en materia de seguridad.
	☐	Evidencia de las pruebas y la verificación de los criterios de aceptación funcionales.
	☐	Evidencia de pruebas y comprobaciones realizadas para asegurar que el nuevo desarrollo no afecta a la seguridad de otros elementos del entorno TI.
	☐	Evidencia de auditorías de código fuente.
	☐	Informes de pentesting.
	☐	Si procede, guías de instalación y configuración segura del sistema, facilitadas por los proveedores.
	☐	Si procede, guías de uso seguro del sistema, facilitadas por los proveedores.
	☐	Si procede, guías de relación entre cliente y proveedor, facilitadas por los proveedores.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Antes del paso a producción, ¿se comprueba el correcto funcionamiento de la aplicación y de sus aspectos de seguridad?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta.
N0	Antes del paso a producción de las aplicaciones, ¿se comprueban los criterios de aceptación en materia de seguridad? *NOTA: Se han verificado, en la medida de lo posible, el cumplimiento de requisitos de seguridad, por ejemplo, realizando pruebas básicas de funcionamiento, mediante solicitud de certificaciones, solicitud de manuales de seguridad, verificando configuraciones de seguridad, etc.*
	Antes del paso a producción de las aplicaciones, ¿se comprueba que no se deteriora la seguridad de otros componentes del servicio?
	¿Se utilizan herramientas específicas para la realización de pruebas 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' o N0*
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 documenta el plan de pruebas de seguridad a realizar y los resultados obtenidos?
	¿Se dispone de evidencias de la aceptación por parte del personal con competencias para ello de la aceptación del desarrollo?
N0	**¿Caso de aplicaciones desarrolladas externamente implementadas en modo local (on-premise), el proveedor aporta suficientes evidencias de la seguridad de la aplicación?** ☐ SI ☐ NO
N0	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de instalación y configuración segura del sistema*' dirigida a los administradores? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise.*
N0	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de uso seguro del sistema*' dirigida a los usuarios? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise.*
	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de la relación entre cliente y proveedor*' dirigida a los administradores? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise.*
	¿Se realizan auditorías de código fuente como parte de las pruebas de seguridad? ☐ 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' o N0*
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.*

B3 – GESTIÓN DE CAMBIOS (APLICACIONES, SISTEMAS Y SUS CONFIGURACIONES)

B.3.1: Procedimientos para la gestión de cambios

Se dispone de un procedimiento formalizado que regula la gestión de cambios en los sistemas y aplicaciones y sus configuraciones. El procedimiento contempla todos los aspectos requeridos en el ENS.

Requisitos:

Op.exp.5	Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:
op.exp.5.1	– Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
op.exp.5.2	– La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
op.exp.5.3	– Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
op.exp.5.4	– Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.
op.exp.5.5	– Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Propuesta de evidencias:

	☐	Procedimiento formalizado (escrito y aprobado) de gestión de cambios.
	☐	Evidencias de la implantación de los controles recogidos en este punto.

Procedimientos de auditoría (aspectos a evaluar):

	El procedimiento de gestión de cambios, ¿contempla los siguientes aspectos y establece claramente cómo y quién los realizará?	
N0	Planificación de los cambios, para reducir el impacto sobre la prestación de los servicios afectados.	☐ SI ☐ NO
	Registro de los cambios, asignándoles un número de referencia para su seguimiento.	☐ SI ☐ NO
	La información a registrar para cada petición de cambio, que deberá ser suficiente para permitir su autorización o no	☐ SI ☐ NO
	Aprobación del cambio.	☐ SI ☐ NO
	Análisis de riesgos y comunicación de los cambios de riesgo alto al responsable de seguridad del sistema.	☐ SI ☐ NO
	Realización de pruebas de preproducción en equipos equivalentes a los de producción.	☐ SI ☐ NO
	Realización de pruebas de aceptación.	☐ 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' o N0*
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.*

	Autorización para el pase a producción del cambio.	☐ SI ☐ NO
	Actualización de la documentación de configuración tras el cambio.	☐ SI ☐ NO
	Procedimiento de reversión de cambios	☐ 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' o N0*
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.*

B.3.2: Responsabilidades para la gestión de cambios de aplicaciones o sistemas

Se han asignado responsabilidades para la gestión de los cambios en aplicaciones y sistemas.

Requisitos:

Org 4	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos (instalaciones, equipos, aplicaciones, enlaces de comunicaciones, etc.).
op.exp.5.4	Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el RS.

Propuesta de evidencias:

	☐	Política de seguridad
	☐	Procedimiento de autorización que cubra todos los elementos del sistema de información concernidos.
	☐	Documentos o registros, con el contenido esperado, de diferentes tipos de autorizaciones.
	☐	Si se emplea una herramienta de ticketing que las consolide, evidencia de tickets de peticiones de autorización.
	☐	Evidencia de informes de riesgos asociados a determinados cambios.
	☐	Evidencia de aprobación del cambio por parte del Responsable de Seguridad para los cambios que se han determinado de riesgo alto.
	☐	Procedimiento de gestión de cambios.
	☐	Evidencias que acrediten que los cambios se planifican para reducir el impacto (por ejemplo, actas de reuniones, calendario de días 'rojos' (días en los que no se pueden realizar cambios en el entorno de producción), acuerdos/actas sobre ventanas de mantenimiento del entorno de producción acordadas con los usuarios, etc.
	☐	Procedimiento de gestión de cambios urgentes

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿El procedimiento de gestión de cambios aplicado, ¿contempla la autorización previa a la entrada en producción del cambio si este conlleva la introducción de un nuevo componente del sistema (equipo, aplicación, enlaces de comunicación con otros sistemas, etc.)?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se gestionan las autorizaciones para la entrada de equipos en producción, especialmente los equipos que involucren criptografía?
N0	¿Se gestionan las autorizaciones para la entrada de aplicaciones en producción?
N0	¿Se gestionan las autorizaciones para el establecimiento de enlaces de comunicaciones con 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' o N0*
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: Las autorizaciones pueden corresponder a enlaces entre sistemas propios, por ejemplo, entre sedes, o de terceros, como puede ser con un proveedor.
N0	¿Se gestionan las autorizaciones para la utilización de medios de comunicación, habituales y alternativos? *NOTA: Podría tratarse de una conexión remota VPN contra la red de la organización, determinada salida a Internet, la solicitud de apertura de puertos en un cortafuegos (FW) corporativo, etc.*
N0	**¿La política de seguridad o la normativa relacionada contempla la asignación de responsabilidades relativas a la gestión de los cambios en aplicaciones y sistemas? En concreto contempla los roles o figuras encargadas de:** • Revisar las solicitudes para realizar cambios en los sistemas y aplicaciones • Autorizar/Rechazar las solicitudes • Planificar la puesta en producción de los cambios • Aprobar o rechazar la puesta en producción del cambio tras las pruebas realizadas
	¿Se determina mediante análisis de riesgos si los cambios son relevantes para la seguridad del sistema? ¿Se puede evidenciar que aquellos cambios que implican una situación de riesgo ALTO son aprobados explícitamente, de forma previa a su implementación, por el Responsable de Seguridad (RS) además de quienes tengan competencia asignada para ello?
N0	¿Se planifican los cambios para reducir el impacto sobre la prestación de los servicios afectados? ¿Se han definido ventanas de mantenimiento acordadas con los usuarios?
	¿Dispone la entidad de un procedimiento para la gestión de cambios urgentes, que permita gestionar adecuadamente la necesidad de realizar un cambio en producción que no había sido planificado previamente o que se debe realizar fuera de las ventanas de mantenimiento acordadas?
	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' o N0*
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.*

B.3.3: Entornos para pruebas separados de producción

Se dispone de entornos separados del de producción para la realización de pruebas.

Requisitos:

op.exp.5.3	Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.

Propuesta de evidencias:

	☐	Evidencia de separación de los entornos de producción y desarrollo.
	☐	Informes de pruebas de preproducción.
	☐	Evidencia de medidas de seguridad del repositorio de código fuente del entorno de desarrollo y del de producción (por ejemplo, usuarios con permisos de lectura, escritura y modificación sobre directorios, usuarios con acceso a las bbdd de cada entorno, etc.).
	☐	Evidencia de uso de una herramienta para el pase a producción.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Está separado a todos los efectos el entorno de desarrollo del de producción?** *NOTA: Revisar el mapa de sistemas para identificar los recursos que forman el entorno de desarrollo, y en su caso, otros entornos asociados al desarrollo (preproducción, calidad, etc.). Para ello, considerar todos los elementos que puede contener cada aplicación (frontales, middleware, bases de datos, LDAPs, etc.).* ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se han separado ambos entornos, realizándose el desarrollo sobre sistemas diferenciados de los productivos?
	¿Existen herramientas de desarrollo o datos de prueba en el entorno de producción?
	¿Se han aplicado medidas de seguridad sobre los repositorios de código fuente utilizados en los entornos de desarrollo y preproducción?
	¿Se utiliza una herramienta de gestión de versiones para la promoción del cambio entre los diferentes entornos? En caso afirmativo, analizar si se utiliza y cómo para restringir el acceso al código existente en los distintos entornos.
	¿Se utiliza una herramienta para realizar el pase a producción? En caso afirmativo, ¿la herramienta tiene configurada las rutas de los entornos de desarrollo, preproducción y producción de forma que garantice la separación entre entornos?
	¿Se han aplicado medidas de seguridad sobre los repositorios de código ejecutable del entorno de producción?

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' o N0*
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.*

B.3.4: Datos en los entornos de prueba

No se utilizan datos reales en pruebas. En caso contrario, se garantiza su seguridad.

Requisitos:

Mp.sw.1.r4.1	Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Propuesta de evidencias:

	☐	Evidencia del proceso de generación de los datos de prueba.
	☐	Evidencia de la seguridad en los datos de prueba reales, si procede.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se aseguran los datos reales empleados para las pruebas previas, evitando su uso en la medida de lo posible?** ☐ SI ☐ NO *NOTA: Analizar cómo se generan los datos de prueba (ofuscando datos, mezclando datos, creando datos, etc.).*
	Espacio disponible para la redacción de la respuesta
	¿Se utiliza una herramienta específica o scripts desarrollados por la entidad para la generación de los datos de prueba
	¿Se evita realizar con datos reales las pruebas previas a la implementación o modificación de los sistemas de información?
	En caso de que fuese necesario recurrir a datos reales para las pruebas previas, ¿se garantiza el nivel de seguridad correspondiente?

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' o N0*
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.*

B.3.5: Segregación de funciones

Se gestiona la separación de las tareas y el control de los accesos a los distintos entornos utilizados para desarrollo y pruebas de testeo en aplicaciones y sistemas.

Requisitos:

op.acc.3.1	Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
op.acc.3.r1 op.acc.3.r1.1 op.acc.3.r1.1	Segregación rigurosa. ▪ Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema. ▪ La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Propuesta de evidencias:

	☐	Organigrama detallado de la organización que evidencie la segregación de funciones
	☐	Procedimiento de gestión de cambios, para analizar la etapa de paso a producción.
	☐	Evidencia sobre los permisos del personal de desarrollo en las herramientas que permiten el paso a producción o sobre las carpetas/directorios en los que se almacenan los ejecutables de producción.
	☐	Evidencia sobre los permisos del personal responsable del desarrollo y aquellos que disponen de los permisos para el mantenimiento de los sistemas.
	☐	Evidencia sobre los permisos del personal responsable de la configuración de sistemas y aquellos que disponen de los permisos para el mantenimiento de los sistemas.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se segregan aquellas funciones que, ante determinadas circunstancias, podrían culminar en conflicto de interés como, por ejemplo, desarrollo y operación?** ☐ SI ☐ NO *NOTA: Se debe obtener evidencia de que, tanto a nivel orgánico como a nivel de accesos lógicos, las siguientes tareas son realizadas por personas diferentes.* • *Desarrollo de aplicaciones / Pase a producción y mantenimiento del entorno de producción.* • *Configuración de sistemas / Mantenimiento del entorno de producción* • *Obtener una lista de usuarios con acceso a los entornos de desarrollo. Verificar si existe una autorización formal.*
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' o N0*
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 evita, siempre que sea posible, que las capacidades de desarrollo y operación recaigan en la misma persona o en el mismo equipo? *Nota: Cuando no sea posible, la organización deberá justificarlo.*
N0	¿Se evita, siempre que sea posible, ¿que las personas que autorizan sean las mismas que controlan el uso? *Nota: Cuando no sea posible, la organización deberá evidenciarlo.*
	¿Se previenen más circunstancias de conflicto de interés, como puede ser, evitando concurran las funciones de configuración y las de mantenimiento? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se evita, siempre que sea posible, que una misma persona aúne funciones de configuración y de mantenimiento del sistema? *Nota: Cuando no sea posible, la Organización deberá evidenciarlo.*
	¿Quienes realizan funciones de auditoría o supervisión, no realizan ninguna otra función relacionada con lo auditado o supervisado? *Nota: Esto afecta, en relación con las auditorías, especialmente al auditor interno, ya sea éste de la propia organización o contratado como prestación de servicios a una empresa externa*.

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' o N0*
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.*

B.3.6: Pruebas de aceptación

Se requiere la aprobación de las pruebas de aceptación previamente al paso a producción.

Requisitos:

op.exp.5.5	Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Propuesta de evidencias:

	☐	Informes de pruebas de aceptación.
	☐	Evidencia de la aceptación del cambio.
	☐	Evidencia de actualización de configuración (inventario, manuales, diagramas de red…), tras un cambio implementado.
	☐	Informes de pruebas de aceptación.

Procedimientos de auditoría (aspectos a evaluar):

N0	**Una vez implementado un cambio, ¿se realizan pruebas de aceptación y se cuenta con la aprobación previa al pase a producción?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se registra la aceptación formal del cambio antes de su paso a producción?
	¿La persona que acepta el cambio tiene las competencias adecuadas para ello?
	Si las pruebas de aceptación son positivas, ¿se actualiza la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda?

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' o N0*
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.*

B.3.7: Registro de cambios y solicitudes

Se documentan y registran los cambios y las solicitudes.

Requisitos:

op.exp.5.2	La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.

Propuesta de evidencias:

	☐	Evidencia de un registro de peticiones de cambio (RFC), quizá en una herramienta de ticketing.
	☐	Evidencias generadas durante todo el ciclo de vida del cambio, que permitan a los responsables de autorizar el cambio tomar las decisiones adecuadas.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se realiza la gestión documental y registro de las peticiones y los cambios en las aplicaciones y sistemas significativos?** ☐ SI ☐ NO
Espacio disponible para la redacción de la respuesta	
	¿Se registra suficiente información para que quien deba autorizarla no tenga dudas al respecto y pueda gestionarla hasta su desestimación o implementación?

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' o N0*
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.*

B.3.8: Procedimientos de reversión de los cambios

Se dispone de mecanismos que permiten la vuelta atrás de los cambios realizados.

Requisitos:

op.exp.5.r1.1	Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.

Propuesta de evidencias:

	☐	Evidencia de plan de marcha atrás respecto a un cambio.
	☐	Evidencia de copias de seguridad de ficheros de configuración, ejecutables de aplicaciones, etc.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se prevé algún mecanismo de vuelta atrás de los cambios?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N2	El procedimiento de reversión de cambios está formalizado y aprobado.
	Entre la documentación asociada al histórico de cambios realizados, ¿se dispone de la relativa al procedimiento de marcha atrás?
	¿Se dispone de una copia de seguridad de la configuración de los sistemas y aplicaciones antes de realizar el cambio, que permita reestablecer el estado de los sistemas en caso de errores en la puesta en producción del cambio?

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' o N0*
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.*