ÁREA E. CONTINUIDAD DEL SERVICIO

INTRODUCCIÓN

Esta GPF-OCEX 5335 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 **E. Continuidad del servicio** 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:

> *"Estos controles son principalmente controles técnicos y su importancia radica en que suponen una salvaguarda adicional ante la materialización de una amenaza, permitiendo la recuperación de datos, en caso de estos sean vulnerados, o la recuperación de sistemas y servicios que hayan perdido su operatividad."*

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.

Tal y como se indica 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.

E1 – COPIAS DE SEGURIDAD DE DATOS Y SISTEMAS

E.1.1: Realización de copias de seguridad

La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.

Requisitos:

mp.info.6.1	Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.
mp.info.6.2	Los procedimientos de respaldo establecidos indicarán: a) Frecuencia de las copias. b) Requisitos de almacenamiento en el propio lugar. c) Requisitos de almacenamiento en otros lugares. d) Controles para el acceso autorizado a las copias de respaldo.

Propuesta de evidencias:

	☐	Normativa/Procedimientos relativos a las copias de seguridad.
	☐	Evidencia de que las copias de seguridad están configuradas y se realizan de acuerdo a la normativa específica.
	☐	Comparativa entre el RPO del BIA (si se dispone) con la normativa de copias de seguridad.
	☐	Evidencia almacenamiento de copias dentro y/o fuera de las instalaciones.
	☐	Evidencias de realización de copias y actuaciones en caso de error.
	☐	Informes del proveedor, caso de copia externalizadas.
	☐	Comparativa entre el RPO del BIA (si se dispone) con la normativa de copias de seguridad.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se realizan copias de seguridad que permitan recuperar los datos perdidos accidental o intencionadamente?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	¿Se realizan copias de seguridad con la periodicidad y plazos de retención requeridos por los servicios que soporta el sistema de información? *NOTA: Asimismo debe establecerse su forma, por ejemplo, totales diarias, totales semanales más incrementales diarias, etc.*
N2	¿Existe un procedimiento formalmente aprobado que describe las copias de seguridad (tipos, datos que tratan, periodicidad, mecanismos de protección y restauración de datos, pruebas de recuperación, etc.)?

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.*

	¿Las copias de seguridad se realizan acorde a lo que se determinan en normativa relativa a copias de seguridad?
	¿La normativa de copias de seguridad está armonizada con el RPO calculado en el BIA, caso de disponerse de este último?
	¿Si la herramienta informa, se ha determinado cómo actuar en caso de fallo en su realización?
N0	Si se externalizan las copias ¿Se reciben informes detallados del proveedor?
	¿Los procedimientos de respaldo establecen la frecuencia de las copias de seguridad?
	¿Los procedimientos de respaldo establecen la necesidad de realizar copias semanales, mensuales, etc., adicionalmente a las copias diarias? *NOTA: Esta práctica es útil en el caso, por ejemplo, de un ataque de Ransomware donde deban desestimarse varias copias contaminadas.*

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.*

E.1.2: Realización de pruebas de recuperación

Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.

Requisitos:

mp.info.6.1.R1	Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Propuesta de evidencias*:*

	☐	Dispone de un procedimiento documentado en el que se determina la frecuencia con la que deben realizarse las pruebas de recuperación y el alcance de dichas pruebas.
	☐	Comprobar la efectiva realización de dichas pruebas, según la frecuencia y el alcance definidos en el procedimiento.

Procedimientos de auditoría (aspectos a evaluar):

	¿La organización ha establecido y aprobado procedimientos formales de restauración de datos y sistemas desde las copias de seguridad? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Están las pruebas de restauración incluidas en el procedimiento de copias de seguridad?
	¿Se prueban regularmente los procedimientos de copia de seguridad y restauración, con una frecuencia dependiendo de la criticidad de los datos y del impacto que causaría la falta de disponibilidad?
N2	¿Está la realización de pruebas de recuperación incluidas en el procedimiento aprobado de copias de seguridad?
	¿Qué sistemas y con qué periodicidad se realizan pruebas planificadas de restauración?
	¿Existe un proceso de autorización para la recuperación de información de las copias de seguridad?
	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.*

E.1.3: Protección de las copias de seguridad

Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.

Requisitos:

mp.info.6.R2	Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

Propuesta de evidencias:

	☐	Procedimiento de realización de copias de seguridad que describa el proceso implantado.
	☐	Evidencia almacenamiento de copias dentro y/o fuera de las instalaciones.
	☐	Normativa determinando requisitos de almacenamiento en otros lugares.
	☐	Evidencia de la existencia de la copia desconectada y los controles implantados.

Procedimientos de auditoría (aspectos a evaluar):

	¿Los procedimientos de respaldo establecen los controles para el acceso autorizado a las copias de respaldo?
	¿Los procedimientos de respaldo establecen los requisitos de almacenamiento en el propio lugar en que se realizan las copias?
	¿Se preservan las copias de seguridad de aquellos riesgos que también podrían afectar a la información original? ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿La normativa de respaldo establece los requisitos de almacenamiento en otros lugares?
	¿Al menos una de las copias de seguridad se almacena de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar simultáneamente tanto al repositorio original como a la copia? *NOTA: está ganando adeptos el llamado método del '3, 2, 1' que consiste en realizar tres (3) copias de seguridad, en al menos dos (2) tipos de soporte distintos, y una (1) de ellas almacenada en otra ubicación.*
N2	¿Están los mecanismos de protección de las copias incluidos en el procedimiento aprobado?
	¿Las copias de seguridad están accesibles de forma directa a nivel de red?
	¿Se dispone de una copia de seguridad en offline? ¿Cómo y con qué frecuencia se realiza?

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.*

E2 – PLAN DE CONTINUIDAD

E.2.1: Identificación de elementos críticos del negocio

Se ha realizado un Análisis de Impacto en la Actividad (BIA) para identificar los elementos críticos del negocio

Requisitos:

op.cont.1	Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Propuesta de evidencias:

	☐	Análisis de Impacto en el Negocio (BIA), incluyendo cálculos de RTO y RPO, con su fecha de actualización.
	☐	Diagrama de dependencias de los activos que soportan los servicios.
	☐	Evidencia de aprobación del BIA.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se ha realizado un análisis de impacto (BIA) en los servicios en el ámbito del ENS?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿El análisis de impacto (BIA) se actualiza al menos cada año y siempre que varíen las circunstancias, de modo que permita en todo momento determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado)?
	Como consecuencia del BIA ¿se determinan los elementos que son críticos para la prestación de cada servicio? ¿se han determinado las dependencias entre ellos de forma que se pongan de manifiesto los elementos que son críticos para la prestación de los servicios?

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.*

E.2.2: Plan de recuperación de desastres (DRP). Pruebas.

Se dispone de un Plan de Recuperación de Desastres (DRP, Disaster Recovery Plan) o se han implantado medidas que permitan el restablecimiento de los servicios. El DRP se engloba dentro del Plan de continuidad del negocio (PCN o BCP, Business Continuity Plan).

Requisitos:

	Se desarrollará un plan de recuperación de desastres que establezca las acciones a ejecutar en caso de contingencia. Dicho plan contemplará los siguientes aspectos: Se identificarán funciones, responsabilidades y actividades a realizar. – Existirá una previsión para coordinar la recuperación y restablecimiento de procesos e infraestructuras TI que dan soporte a los servicios esenciales de la organización.

Propuesta de evidencias:

	☐	Planes de Recuperación (DRP) específicos, de emergencia, etc., asociados al Plan de Continuidad general.
	☐	Evidencias de comprobaciones tras la discontinuidad del sistema.

Procedimientos de auditoría (aspectos a evaluar):

N2	Partiendo del Plan de Continuidad general ¿existen definidos planes de emergencia, contingencia o recuperación, en consonancia? *NOTA: Si se realiza el Plan de Continuidad considerando diferentes escenarios de contingencia, puede establecerse para dichos escenarios un conjunto de Planes de Recuperación ante Desastres (DRP) específicos.*
	Ante una caída o discontinuidad del sistema, ¿se comprueba la integridad del sistema operativo, firmware y ficheros de configuración de los equipos afectados?

Procedimientos de auditoría

- Revisar si la entidad dispone de un DRP y este ha sido formalmente aprobado.
- Revisar si el plan anterior incluye la realización de pruebas del DRP y comprobar que se realizan dichas pruebas.

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.*

E.2.3: Plan de continuidad. Pruebas.

Se dispone de un Plan de Continuidad o se han implantado medidas que permitan la continuidad de los servicios ante una contingencia, recuperando los procesos críticos.

Se realizan pruebas periódicas de PCN o de las medidas de continuidad implementadas.

Requisitos:

op.cont.2	Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:
op.cont.2.1	Se identificarán funciones, responsabilidades y actividades a realizar.
op.cont.2.2	– Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
op.cont.2.3	– Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
op.cont.2.4	– Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
op.cont.2.5	– El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.
op.cont.3.1	Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Propuesta de evidencias:

	☐	Plan de Continuidad acorde con el BIA.
	☐	Otros planes de continuidad de la organización vinculados.
	☐	Evidencias de formación relacionada con el Plan de Continuidad.
	☐	Informe de las pruebas de continuidad, con relación de fases y su duración individual, además de la total de la prueba.
	☐	Comparativa de las pruebas con los RTO obtenidos en el BIA.
	☐	Posibles tickets con acciones correctivas, consecuencia de pruebas del Plan de Continuidad no satisfactorias.

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	**¿Se dispone de un Plan de Continuidad documentado, coherente con los resultados del BIA?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
N0	En el Plan de Continuidad ¿se identifican las funciones, responsabilidades y actividades a realizar?
	En el Plan de Continuidad ¿existe una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización, aunque sea con menor rendimiento?
	En el Plan de Continuidad ¿todos los medios alternativos están planificados y se han materializado mediante acuerdos o contratos con los proveedores correspondientes?
	¿Las personas afectadas por el Plan de Continuidad reciben formación específica relativa a su papel en dicho plan?
	¿El Plan de Continuidad es parte integral y armónica de los planes de continuidad de la organización, armonizados con otras materias ajenas a la seguridad?
N0	**¿Se realizan pruebas periódicas del Plan de Continuidad?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se puede evidenciar la realización de pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir entre lo previsto en el plan y el resultado de ejecutarlo?
	¿Las pruebas de continuidad se planifican con antelación, dividiéndose en fases, para poder incidir en aquellas que sean más determinantes con miras a poder reducir los tiempos de recuperación, caso de constatar durante la prueba que se incumplen los RTO establecidos en el BIA?
	¿Se elabora un informe al finalizar la prueba del plan, que indique claramente aquellos aspectos que se pueden mejorar o, en su caso, corregir? ¿Se toma en cuenta los resultados de las pruebas para alinear estos tiempos con lo identificado en los BIAS?
	¿Se registran en alguna herramienta las acciones correctivas o de mejora necesarias, para poder efectuar su seguimiento?

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.*

E.2.4: Medios alternativos (alta disponibilidad)

Se considera la alta disponibilidad en los criterios de diseño, adquisición e implementación de los sistemas críticos.

Requisitos:

op.cont.4.1	Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema: a) Servicios contratados a terceros. b) Instalaciones alternativas. c) Personal alternativo. d) Equipamiento informático alternativo (servidores críticos). e) Medios de comunicación alternativos.
op.cont.4.2	Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
op.cont.4.3	Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.
op.cont.4.r1	Automatización de la transición a medios alternativos. El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.
	Otros elementos críticos redundados: a) Dispositivos críticos con doble tarjeta de red b) Dispositivos críticos con doble fuente de alimentación c) Servicio eléctrico redundado

Propuesta de evidencias:

	☐	Inventario constando los medios alternativos involucrados en la recuperación.
	☐	Contratos y cuerdos de nivel de servicio de los medios alternativos contratados a terceros.
	☐	Evidencia de personal alternativo.
	☐	Evidencia de instalaciones alternativas.
	☐	Evidencia de medios de comunicaciones alternativos.
	☐	Evidencia de transferencia automática a los medios alternativos.
	☐	La alta disponibilidad se encuentra contemplada en los procedimientos para la compra y el desarrollo de sistemas.
	☐	Evidencia de otros dispositivos redundados (fuentes de alimentación o tarjeta de red en los dispositivos críticos, suministro eléctrico…)

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	**¿Está prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se dispone inventario de los medios alternativos y sus componentes están actualizados?
N0	¿Se ha establecido un tiempo máximo para que los medios alternativos entren en funcionamiento?
	¿Los medios alternativos están sometidos a las mismas garantías de seguridad que los medios originales?
	¿Se cubren los elementos relevantes del sistema? Describir elementos redundados
	Espacio disponible para la redacción de la respuesta
	¿Se cubren los servicios contratados a terceros?
	¿Se dispone de instalaciones alternativas en caso de que las instalaciones habituales no estén disponibles?
	¿Se dispone de personal alternativo?
	¿Se dispone de equipamiento informático redundado?
	¿Se dispone de medios de comunicación alternativos?
	¿Dispone el sistema de elementos hardware y/o software que permitan la transferencia de los servicios automáticamente a los medios alternativos?
	¿Dispone de otros dispositivos redundados (fuentes de alimentación o tarjeta de red en los dispositivos críticos, suministro eléctrico…)? Detallar.

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.*

E.2.5: Protección de la cadena de suministro

Se analiza el riesgo e impacto que puede tener sobre el sistema un incidente originado en la cadena de suministro.

Requisitos:

op.exp.3.1	Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
op.exp.3.2	Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
op.exp.3.3	Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.
op.exp.3.r1.1	El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
op.exp.3.r2.1	Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Propuesta de evidencias:

	☐	Estudio de impacto respecto a producirse un posible incidente en los proveedores.
	☐	Evidencia de que se contempla en el BIA la dependencia de proveedores.
	☐	Análisis de riesgos incluyendo proveedores y posible Plan de Tratamiento (PTR) de los riesgos asociados a la cadena de suministro.
	☐	Plan de Continuidad con referencia a la cadena de suministro.
	☐	Pruebas del Plan de continuidad en relación al escenario de indisponibilidad proveedores.

Procedimientos de auditoría (aspectos a evaluar):

N0	**¿Se analizan los riesgos y se adoptan medidas respecto a un posible incidente originado en la cadena de suministro?** ☐ SI ☐ NO
	Espacio disponible para la redacción de la respuesta
	¿Se puede evidenciar que se analiza el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro? *NOTA: Suele analizarse incluyendo a la cadena de suministro en el Análisis de Riesgos, así como en el BIA (caso de disponerse de él).*
	¿Se puede evidenciar que se estiman los riesgos sobre el sistema por causa de un incidente accidental o deliberado que tenga su origen en la cadena de suministro? *NOTA: Suele analizarse incluyendo a la cadena de suministro en el Análisis de Riesgos*

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 puede evidenciar que se adoptan medidas de contención de los impactos estimados sobre el sistema debido a un incidente accidental o deliberado que tenga su origen en la cadena de suministro? *NOTA: Estas medidas habitualmente se encontrarán en el Plan de Tratamiento de Riesgos (PTR).*
	¿Se considera la cadena de suministro en el Plan de Continuidad de la organización y en sus pruebas?
Espacio disponible para la redacción de la respuesta	
	¿El Plan de Continuidad de la organización tiene en cuenta la dependencia de proveedores externos críticos?
	¿Se realizan pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor?

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.*