Guía práctica de fiscalización de los OCEX

GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica

Referencia: GPF-OCEX 5300, GPF-OCEX 1315R, GPF-OCEX 1316R y GPF-OCEX 5340

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

*La Conferencia de Presidentes de los OCEX aprobó el 12/11/2018 la primera versión de la **GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica**. Han transcurrido más de cinco años desde entonces y se han producido dos circunstancias que aconsejan la revisión completa de la guía: la entrada en vigor de la NIA-ES 315R/GPF-OCEX 1315R y la aprobación del nuevo Esquema Nacional de Seguridad (ENS) mediante el Decreto 311/2022. Ambas normas afectan de forma importante al contenido de la guía y junto con la experiencia adquirida durante estos años en su aplicación práctica han dado lugar a la nueva versión contenida en el presente documento. Pese a los numerosos cambios y adaptaciones, los conceptos esenciales y los principales procedimientos de auditoría se mantienen vigentes, por lo que la transición entre ambas versiones de la guía no debe plantear ningún problema importante a los auditores de los OCEX que ya aplicaran la versión anterior.*

En el desarrollo de esta GPF-OCEX 5330, cuyo contenido está fundamentalmente relacionado con la auditoría de la seguridad de la información, se ha tenido especial cuidado en mantener 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.

Para la adecuada comprensión de esta guía deben leerse previamente las GPF-OCEX 1315R y GPF-OCEX 1316R a las que no sustituye, sino que las desarrolla para facilitar su aplicación práctica.

*Junto con esta guía también se ha actualizado la complementaria **GPF-OCEX 5340 Revisión de los controles de procesamiento de la información (CPI) en un entorno de administración electrónica,*** con la que está totalmente interrelacionada y hay que conocer simultáneamente.

1. Introducción

El enfoque de auditoría basado en el análisis de los riesgos es el fundamento central de la actividad auditora desarrollada de acuerdo con las Normas Internacionales de Auditoría (NIA-ES) y las ISSAI-ES. De acuerdo con este enfoque, el objetivo del auditor es obtener una **seguridad razonable** de que las cuentas anuales en su conjunto están libres de incorrecciones materiales, debidas a fraude o error.

Una seguridad razonable es un grado alto de seguridad y se alcanza cuando el auditor ha obtenido evidencia de auditoría suficiente y adecuada para reducir el riesgo de auditoría (es decir, el riesgo de expresar una opinión inadecuada cuando las cuentas anuales contengan incorrecciones materiales) a un nivel aceptablemente bajo. No obstante, una seguridad razonable no significa un grado absoluto de seguridad, debido a que existen limitaciones inherentes a la auditoría que hacen que gran parte de la evidencia de auditoría a partir de la cual el auditor alcanza sus conclusiones y en la que basa su opinión sea más convincente que concluyente.

En una auditoría financiera basada en el análisis de los riesgos, el estudio y revisión de los sistemas de información que sustentan la gestión de una entidad es una actividad de importancia fundamental, en la medida en que esa gestión se apoya en unos **sistemas de información interconectados** que, con la plena implantación de la administración electrónica, han ido adquiriendo una **complejidad cada vez mayor**.

Esta situación ha generado una serie de nuevos e importantes riesgos de auditoría (inherentes y de control) derivados del uso de las TI que deben ser considerados en la estrategia de auditoría. En estas circunstancias la revisión de los **controles generales de tecnologías de información (CGTI) y de los controles de procesamiento de la información (CPI)** es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.

De acuerdo con las GPF-OCEX/NIA-ES-SP, en una auditoría financiera, una vez adquirido un conocimiento general de la entidad, incluyendo sus sistemas de información y de control interno y antes de revisar la eficacia operativa de los CPI se debe revisar la situación de los CGTI, ya que el grado de confianza que el auditor pueda depositar en ellos determinará la posterior estrategia de auditoría.

En un entorno informatizado de complejidad media o alta, la revisión de los CGTI requerirá la colaboración de especialistas en auditoría de sistemas de información, bien personal propio del OCEX o bien expertos externos contratados, y la aplicación de una metodología específica como la recogida en esta guía.

Además de las NIA-ES-SP, las normas reguladoras de la auditoría pública, en general, recogen la necesidad de que los auditores revisen la fiabilidad de los sistemas de información, los controles internos y la seguridad de la información[1].

Esta revisión puede hacerse en el marco de una auditoría financiera, de cumplimiento, operativa, o como una auditoría específica de sistemas de información.

En la GPF-OCEX 5340 se ha incluido un apartado de **definiciones** que también es aplicable a la presente guía.

[1] A modo de ejemplo:

a) La Ley 6/1985, de 11 de mayo, de Sindicatura de Comptes de la Comunitat Valenciana establece:

"*Artículo 11. Medios de información para el ejercicio de la función fiscalizadora y consecuencias derivadas de la obstrucción al ejercicio de la actividad fiscalizadora.*
Uno. En el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para: …
d) ***Verificar la seguridad y fiabilidad de los sistemas informáticos*** *que soportan la información económico-financiera, contable y de gestión.*"

b) El Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local establece:

"Artículo 33. Ejecución de las actuaciones de auditoría pública.
4. Para la aplicación de los procedimientos de auditoría podrán desarrollarse las siguientes actuaciones: …
e) ***Verificar la seguridad y fiabilidad de los sistemas informáticos*** *que soportan la información económico-financiera y contable."*

c) La Resolución de 30 de julio de 2015, de la Intervención General de la Administración del Estado, por la que se dictan instrucciones para el ejercicio de la auditoría pública, establece:

"Duodécima. Procedimientos para el ejercicio de la auditoría pública.
2. Para la aplicación de los procedimientos de auditoría podrán desarrollarse las siguientes actuaciones:
e) ***Verificar la seguridad y fiabilidad de los sistemas informáticos*** *que soportan la información económico-financiera y contable."*

La guía tiene como finalidad ayudar al equipo de auditoría a:

- Adquirir o corroborar un conocimiento general de la estructura y organización de los sistemas de información de la entidad y un conocimiento profundo de aquellos que afectan a los procesos de gestión / aplicaciones TI significativas que van a ser revisadas.
- Identificar riesgos derivados del uso de las tecnologías de la información (TI).
- Identificar, analizar y revisar el adecuado diseño, implementación y funcionamiento de los CGTI que han de hacer frente a los riesgos derivados del uso de las TI.
- Determinar si el adecuado funcionamiento de los CGTI apoya el funcionamiento correcto de los CPI.
- Confirmar si la estrategia de auditoría adoptada de forma preliminar en la planificación es válida.
- Formular recomendaciones.

2. Objetivos y alcance de la revisión de los CGTI

La revisión/auditoría de los CGTI puede tener varias motivaciones con objetivos y alcances distintos. Básicamente pueden resumirse en dos:

a) Revisión[2] de los CGTI en el marco de una auditoría financiera y/o de cumplimiento.

b) Auditoría de los CGTI como auditoría específica de los sistemas de información.

2.1 Revisión de los CGTI en el marco de una auditoría financiera de cuentas anuales (o de elementos de las cuentas anuales) y/o de cumplimiento

El **objetivo de la revisión** de los CGTI será obtener una seguridad razonable de que estos permiten y apoyan el funcionamiento continuo y apropiado del entorno de TI, **incluido el funcionamiento continuo y efectivo de los controles de procesamiento de la información** y la integridad de la información (es decir, la completitud, exactitud y validez de la información) en el sistema de información de la entidad.

En una auditoría financiera los CGTI son importantes ya que si funcionan debidamente aseguran razonablemente la consecución de los objetivos generales de control interno y posibilitan el correcto funcionamiento de los CPI.

La guía también será de utilidad en auditorías de cumplimiento y operativas en las que la gestión auditada está sustentada fundamentalmente en sistemas informáticos y se plantean necesidades similares a las auditorías financieras. Por ejemplo, al ejecutar una auditoría de cumplimiento del área de subvenciones se requerirá revisar el adecuado funcionamiento del control interno, incluyendo los CPI y los CGTI que dan soporte a estos, ya que entre los objetivos de los CPI está el de cumplimiento de la legalidad.

El **alcance** de la revisión vendrá determinado por el auditor financiero respecto a su necesidad de obtener confianza sobre el funcionamiento efectivo de los CPI relevantes. Para ello se seguirá la metodología descrita en los apartados siguientes.

Los **criterios de auditoría** son los establecidos en esta guía, que está alineada con el ENS.

Los destinatarios de la guía serán los miembros de los equipos de fiscalización que deban planificar y ejecutar una auditoría financiera y/o una auditoría de cumplimiento u operativa, que deberán contar con asistencia especializada para el conocimiento de las TI y los CGTI y la ejecución de las pruebas de controles.

2.2 Auditoría de los CGTI como trabajo específico e independiente

Los **objetivos** de una auditoría de los CGTI, no integrada en una auditoría financiera, que también se puede denominar auditoría de seguridad de la información o auditoría de ciberseguridad, consisten en **auditar los controles de seguridad de acuerdo con los criterios establecidos en el ENS**, que se desarrollan en el apartado 14 de esta guía y en las GPF-OCEX 5331 a 5335. Todas las categorías de CGTI pueden ser relevantes según se establezca en el alcance de la auditoría.

[2] A las auditorías de los CGTI integradas en una auditoría financiera y/o de cumplimento las denominaremos “revisiones” de CGTI y normalmente no resultarán en un informe independiente.

Los objetivos pueden incluir, por ejemplo:

- complementar las auditorías evaluando la eficacia de la ciberseguridad en el contexto de una revisión más amplia de los sistemas de información;
- apoyar otras auditorías operativas, mediante la evaluación de la fiabilidad de los datos o el grado en que un sistema de información protege la confidencialidad, la integridad y la disponibilidad de los datos;
- determinar la eficacia de los controles de ciberseguridad e identificar cualquier riesgo relacionado con su implementación; y
- examinar cualquiera de los CGTI señalados en esta guía.

El **alcance** de una auditoría está formado por el ámbito subjetivo, objetivo y temporal, refleja los límites o contorno de la auditoría y está directamente vinculado a los objetivos de esta. El alcance define el tema, materia o grupo de controles que los auditores evaluarán (ámbito objetivo), el período de tiempo revisado (ámbito temporal) y las entidades y sistemas que se auditarán (ámbito subjetivo).

El alcance de una auditoría de CGTI/ciberseguridad implica decidir sobre los sistemas informáticos, las funcionalidades y los procesos a evaluar. Por ejemplo, el alcance puede:

- abordar de manera integral toda una organización, un componente o una red, o puede dirigirse concretamente a una aplicación, tecnología específica (por ejemplo, la aplicación de nómina, la de recaudación, la red inalámbrica, gestión de la nube, del blockchain o la inteligencia artificial); o
- incluir todos los controles o solo un número seleccionado de controles dentro de una categoría de las indicadas en la figura 10, o de varias de ellas.

Al determinar el alcance de la auditoría es importante priorizar los activos críticos. Los criterios utilizados para priorizar los sistemas deben reflejar los objetivos de auditoría. Por ejemplo, un auditor puede priorizar los sistemas a auditar basándose en la categorización del ENS. Si el alcance se ve limitado debido a un tiempo o recursos limitados, el enfoque debe centrarse en los ítems de mayor riesgo y prioridad de la organización.

Antes de determinar el alcance de la auditoría, debe tenerse en cuenta el entorno TI de la organización auditada. Esto es particularmente importante si alguno o todos los sistemas de la organización operan en la nube.

Por último, la dirección del OCEX debe garantizar que el equipo de auditoría tenga colectivamente las **habilidades** necesarias para llevar a cabo la auditoría. Por ejemplo, el equipo debe tener conocimientos técnicos suficientes y especializados para evaluar las tecnologías y sistemas que están dentro del alcance de la auditoría.

En estas auditorías se requerirán procedimientos específicamente diseñados, basados en esta guía y en las GPF-OCEX 5331 a 5335, de acuerdo con los objetivos y alcance que se determine en cada auditoría. Los objetivos, el alcance y la metodología pueden ajustarse a medida que se realiza el trabajo.

En estos casos los destinatarios de la guía serán los miembros de los equipos de fiscalización que deban planificar y ejecutar dichas auditorías de CGTI, que normalmente serán auditores de sistemas de información.

3. Conocimiento del sistema de control interno de la entidad y de sus componentes

3.1 El sistema de control interno y los controles

(Apartados 19 y 20 de la GPF-OCEX 1316R y Anexo 3 de la NIA-ES 315R/GPF-OCEX 1315R.)

El auditor debe aplicar procedimientos de valoración del riesgo (**PVR**) y adquirir un conocimiento del sistema de control interno que le permitan identificar y valorar los riesgos de incorrección material (**RIM**).

A los efectos de las NIA-ES, un sistema de control interno comprende cinco componentes interrelacionados:

a) el entorno de control *(ver apartado 4)*;
b) el proceso de valoración del riesgo por la entidad;
c) el proceso de la entidad para el seguimiento del sistema de control interno;
d) el sistema de información y comunicación *(ver apartado 5)* y
e) las actividades de control *(ver apartado 6)*.

Los controles son las ***políticas y procedimientos***[3] integrados **dentro de los distintos componentes** del sistema de control interno de la entidad *(A2 de NIA-ES 315R)*.

Es importante la distinción entre controles directos e indirectos. Los **controles directos** son aquellos suficientemente precisos para prevenir, detectar o corregir incorrecciones en las afirmaciones (normalmente se encuentran dentro del componente actividades de control). Los **controles indirectos** no son lo suficientemente precisos para prevenir, detectar o corregir incorrecciones en las afirmaciones, pero apoyan otros controles y, por lo tanto, tienen un efecto indirecto en el funcionamiento adecuado de dichos controles.

El **componente de actividades de control**, sobre el que se profundiza más adelante, está formado por controles individuales específicos que se clasifican en:

- Los **controles de procesamiento de la información (CPI).** Controles relacionados con el procesamiento de la información en aplicaciones de TI o procesamientos manuales de la información en el sistema de información de la entidad que responden directamente a los riesgos para la integridad de la información (es decir, la completitud, exactitud, validez y legalidad de las transacciones y otra información). Son analizados en profundidad en la GPF-OCEX 5340. Normalmente son **controles directos**.
- Los **controles generales de las tecnologías de la información (CGTI).**

  Son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI de la organización auditada y ayudan a asegurar su correcto funcionamiento. Son controles relacionados con el uso de las tecnologías de la información y las comunicaciones implantados en los distintos niveles de la estructura organizativa general de una entidad y en sus sistemas de información. Normalmente son **controles indirectos**.

4. Conocimiento del entorno de control

(Apartado 21 y A108 de NIA-ES 315R/GPF-OCEX 1315R)

El auditor obtendrá conocimiento del entorno de control (primer componente de un sistema de control interno) que sea relevante para la preparación de los estados financieros mediante la aplicación de PVR, tal como se señala en el apartado 24 de la GPF-OCEX 1316.

La evaluación por el auditor del entorno de control en relación con la **utilización de TI** por la entidad puede incluir cuestiones tales como:

- Si la **gobernanza sobre las TI** es acorde con la naturaleza y complejidad de la entidad y de sus operaciones de negocio/gestión realizadas a través de TI, incluida la complejidad o madurez de la plataforma o arquitectura tecnológicas de la entidad y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera.
- La **estructura organizativa de la dirección en relación con las TI y los recursos asignados**. Por ejemplo, si la entidad ha invertido en un entorno de TI adecuado y en las mejoras necesarias, o si se ha contratado al suficiente número de personas con la cualificación adecuada incluso cuando la entidad utiliza software comercial (con pocas o ninguna capacidad de modificación).

La nueva NIA-ES 315R enfatiza la importancia del entorno de control para el resto de los componentes del sistema de control interno. Por esta razón se incluyen aspectos relacionados con la gobernanza TI en la metodología para la revisión de los CGTI. Esta materia se ha desarrollado con detalle en las siguientes guías, a las que nos remitimos:

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría

El conocimiento y evaluación de estas materias están incluidos en la primera categoría de CGTI: "A. Gobernanza" (ver apartado 14.A).

[3] Ver definiciones en GPF-OCEX 5340.

5. Conocimiento del sistema de información y comunicación (SIC) y la utilización de las TI

5.1 Conocimiento del sistema de información y comunicación (SIC)

(Apartado 25.a de GPF-OCEX 1315R y 28-31 de la GPF-OCEX 1316R)

El auditor obtendrá conocimiento del SIC de la entidad que sea relevante para la preparación de los estados financieros, mediante la aplicación de PVR a través del conocimiento de las actividades de procesamiento de la información de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y las políticas que definen, para cada tipo de transacción, saldo contable e información a revelar significativa (TTSCIRS).

Este conocimiento incluirá:

i. **el modo en que la información fluye** por el sistema de información de la entidad, incluido el modo en que:
   a. las transacciones se inician y la información sobre ellas se registra, se procesa, se corrige si es necesario, se contabiliza y se incluye en los estados financieros; y
   b. la información sobre los hechos y condiciones, distintos de las transacciones, se captura, se procesa y se revela en los estados financieros;

ii. **los registros contables**, cuentas específicas de los estados financieros y otros registros de soporte relacionados con los flujos de información en el sistema de información;

iii. **el proceso de información financiera** utilizado para la preparación de los estados financieros de la entidad, incluida la información a revelar; y

iv. **los recursos de la entidad, incluido el entorno de TI**, relevantes para los apartados i a iii anteriores;

Como parte de la valoración del riesgo, la NIA-ES 315R requiere de forma explícita que el auditor obtenga un conocimiento de los sistemas de información relevantes para la preparación de las cuentas anuales y del sistema de control interno de la entidad con la finalidad de identificar y valorar los RIM. Esto incluye comprender el uso de las TI por parte de la entidad, conocer el entorno de TI e identificar los riesgos derivados del uso de las TI.

En términos generales, el auditor **debe conocer** los siguientes aspectos de TI del sistema de información[4]:

a) **El modelo de negocio de la entidad y el modo en que integra la utilización de TI** ya que pueden proporcionar información útil sobre la naturaleza y extensión de las TI en el sistema de información.

b) **La naturaleza y características de las aplicaciones de TI significativas, la infraestructura de TI en las que se apoyan y otros aspectos del entorno de TI**, a la vez que obtiene conocimiento del modo en que la información relativa a los TTSCIRS entra, fluye, se procesa y sale del sistema de información de la entidad.

Se debe conocer el **entorno de TI** relevante para los flujos de transacciones y el procesamiento de la información en el sistema de información de la entidad porque la utilización de aplicaciones de TI o los **otros aspectos del entorno de TI** pueden dar lugar a **riesgos derivados de la utilización de TI.**

5.2 El entorno de TI

(Apartado 12.(g) de la NIA-ES 315R/GPF-OCEX 1315R)

El entorno de TI está formado por:

- **Aplicaciones TI,** son programas que se utilizan para el inicio, procesamiento, registro y reporte de transacciones o información.
- La **infraestructura de TI** que da soporte a las TI comprende el hardware y software relacionados con:
  - ✓ la red,
  - ✓ los sistemas operativos y
  - ✓ las bases de datos.
- Los **procesos de TI** son los procesos de la entidad para la gestión del acceso al entorno de TI, la gestión de cambios en los programas o de los cambios al entorno de TI, y para la gestión de las operaciones TI.

[4] Apartados A140-A143 de la NIA-ES 315R/GPF-OCEX 1315R.

- El **personal de TI** involucrado en esos procesos que una entidad utiliza para respaldar las operaciones de negocio y para lograr la consecución de las estrategias de negocio. Esto incluye aspectos que pueden ser relevantes (como la competencia profesional de las personas que realizan el trabajo, si se dispone de los recursos adecuados y si existe una adecuada segregación de funciones).

A los efectos de esta guía, podemos representar el entorno de TI de una entidad mediante un modelo simplificado formado por varios niveles o capas tecnológicas superpuestas, tal como se muestra en la figura 1, en el que operan los procesos y las personas.

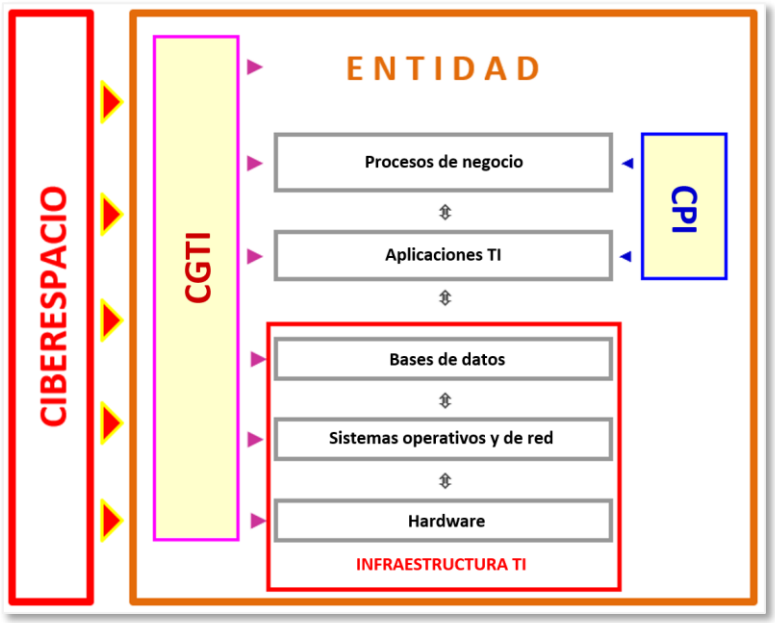

Figura 1

En general, conocer el entorno de TI será más fácil en **entidades menos complejas**, que utilicen una aplicación comercial ("estándar") y en las que la entidad, generalmente, no puede hacer cambios en la aplicación, por no tener acceso a su código fuente. El auditor puede considerar, entre otras, las siguientes cuestiones a la hora de obtener conocimiento de una aplicación comercial:

a) el grado en que la aplicación está bien implantada y tiene la reputación de ser fiable;

b) hasta qué punto puede la entidad modificar el código fuente para modificar la funcionalidad estándar o efectuar cambios directos a los datos;

c) la naturaleza y la extensión de las adaptaciones que se han hecho en la aplicación. Aunque una entidad, generalmente, no pueda modificar su código fuente, muchas aplicaciones permiten hacer cambios en su configuración (por ejemplo, establecer parámetros),

d) el grado en que se puede acceder directamente a los datos relacionados con la preparación de los estados financieros (es decir, acceso directo a la base de datos sin utilizar la aplicación) y el volumen de datos que se procesa. Cuanto mayor sea el volumen de datos, más probable será que la entidad pueda necesitar controles que mantengan la integridad de los datos, como los CGTI sobre el acceso no autorizado y cambios en los datos, y

e) si la entidad tiene una adecuada política de parcheado y tiene en cuenta los anuncios de los proveedores.

Los **entornos de TI complejos** pueden incluir aplicaciones de TI altamente personalizadas o integradas tipo ERP y se necesitará un mayor esfuerzo para su conocimiento. Los procesos de información financiera o las aplicaciones de TI pueden estar integradas con otras aplicaciones de TI que se utilizan en las actividades operativas de la entidad y que proporcionan información a las aplicaciones de TI relevantes para los flujos de transacciones y el procesamiento de la información en el sistema de información y la preparación de los estados financieros. Los entornos complejos pueden también requerir departamentos dedicados a TI que cuenten con procesos de TI estructurados sustentados por personal con habilidades en el desarrollo de software y en el

mantenimiento del entorno de TI. En otros casos, la entidad puede emplear proveedores de servicios para gestionar algunos aspectos de su entorno de TI o procesos de TI dentro del mismo (por ejemplo, alojamiento por terceros o proveedores de servicios en la nube).

En el Anexo 1 se recogen consideraciones para el conocimiento de la utilización de las TI realizadas en la NIA-ES 315R/GPF-OCEX 1315R.

5.3 Utilización de tecnologías de la información en los componentes del sistema de control interno

(Anexo 5 Consideraciones para el conocimiento de las tecnologías de la información de la NIA-ES 315R/GPF-OCEX 1315R y Apartado 60 de la GPF-OCEX 1316R.)

El sistema de control interno de la entidad contiene controles manuales y automatizados cuya combinación varía según la naturaleza y complejidad de la utilización de las TI por la entidad.

El apartado A94 de la NIA-ES 315R/GPF-OCEX 1315R señala que el objetivo global y el alcance de una auditoría no son diferentes si una entidad opera en un entorno mayoritariamente manual, un entorno totalmente automatizado o un entorno en el que se combinan elementos manuales y automatizados.

Sin embargo, aunque el objetivo y el alcance de una auditoría no sean diferentes, **el grado de digitalización de la entidad, además de a los riesgos inherentes, afecta a la forma en que debe realizarse el conocimiento del sistema de control interno y de sus componentes,** a la valoración de los riesgos de control y a los procedimientos posteriores de auditoría basados en dicha valoración.

La utilización por la entidad de las TI afecta al modo en que la información relevante para la preparación de los estados financieros se procesa, almacena y comunica y, en consecuencia, afecta al modo en que se diseña e implementa el sistema de control interno de la entidad.

Los controles automatizados pueden resultar **más fiables** que los manuales debido a que no pueden ser fácilmente evitados, ignorados o forzados y también a que están menos expuestos a simples errores. Los controles automatizados pueden ser **más eficaces** que los manuales en aquellas circunstancias en las que se produce un número elevado de transacciones recurrentes.

6. Conocimiento del componente de actividades de control

(Apartado 26 de GPF-OCEX 1315R y 32 de la GPF-OCEX 1316R)

De acuerdo con el apartado 26 de la GPF-OCEX 1315R el auditor debe obtener conocimiento del componente de actividades de control, en particular debe:

- Identificar los controles **(CPI)** que responden a los RIM en las afirmaciones. *(Ver GPF-OCEX 5340)*
- **Identificar las aplicaciones de TI y otros aspectos del entorno de TI que están sujetos a riesgos derivados de la utilización de TI** basándose en los CPI identificados. *(Ver apartado 7)*
- **Identificar los riesgos derivados de la utilización de TI en las aplicaciones TI y otros aspectos del entorno TI.** *(Ver apartado 8)*
- **Identificar los CGTI de la entidad que responden directamente a los riesgos derivados TI.** *(Ver apartado 9)*

En la presente guía nos centramos en los CGTI. Los CPI son analizados en profundidad en la GPF-OCEX 5340.

De forma gráfica, el conocimiento y la revisión de los CGTI en una auditoría financiera, de acuerdo con la NIA-ES 315R/ GPF-OCEX 1315R sigue el siguiente proceso que se muestra en la figura 2.

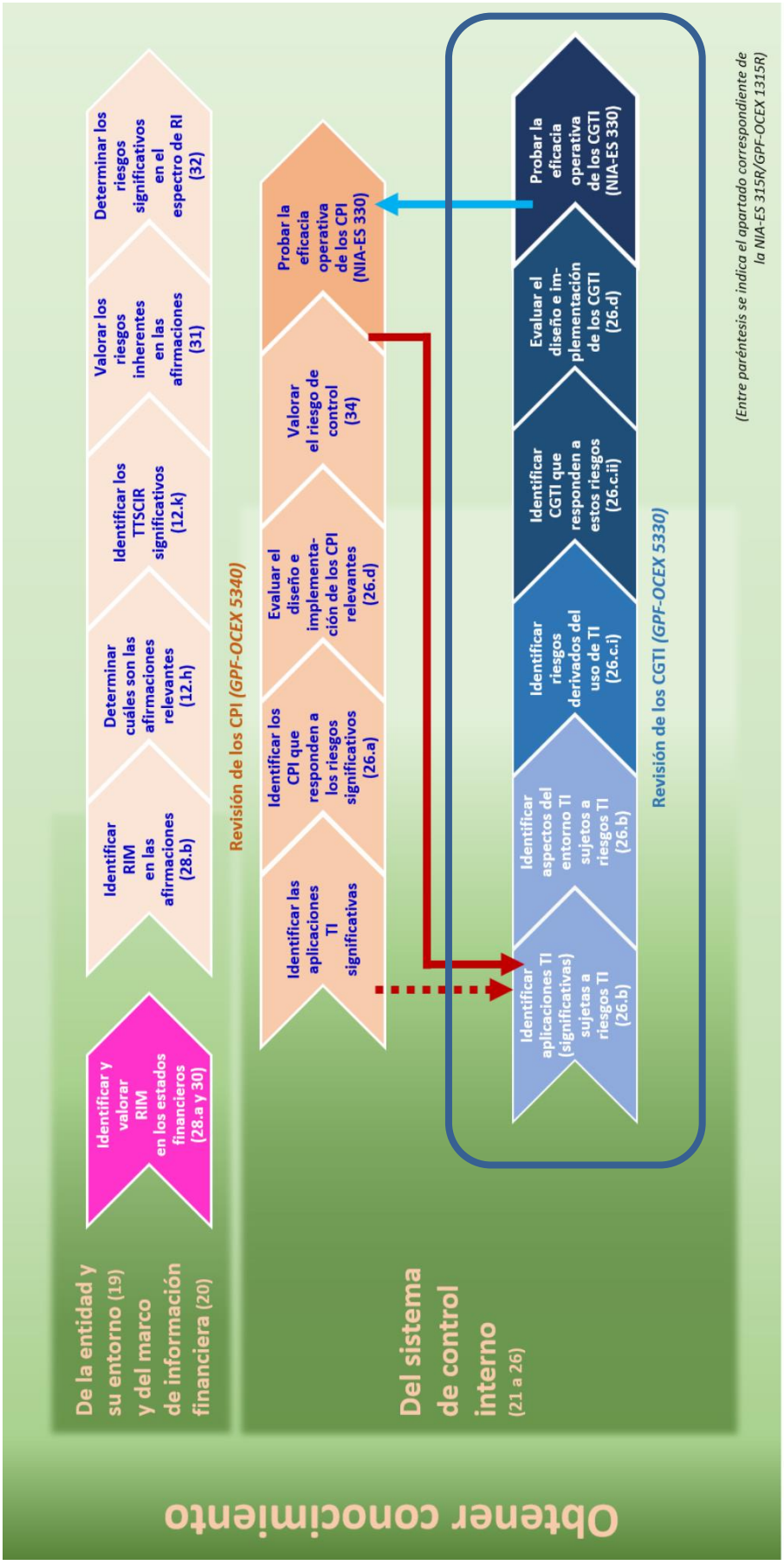
Obtener conocimiento
De la entidad y su entorno (19) y del marco de información financiera (20)
Identificar y valorar RIM en los estados financieros (28.a y 30)
Identificar RIM en las afirmaciones (28.b)
Determinar cuáles son las afirmaciones relevantes (12.h)
Identificar los TTSCIR significativos (12.k)
Valorar los riesgos inherentes en las afirmaciones (31)
Determinar los riesgos significativos en el espectro de RI (32)
Del sistema de control interno (21 a 26)
Revisión de los CPI (GPF-OCEX 5340)
Identificar las aplicaciones TI significativas
Identificar los CPI que responden a los riesgos significativos (26.a)
Evaluar el diseño e implementación de los CPI relevantes (26.d)
Valorar el riesgo de control (34)
Probar la eficacia operativa de los CPI (NIA-ES 330)
Revisión de los CGTI (GPF-OCEX 5330)
Identificar aplicaciones TI (significativas) sujetas a riesgos TI (26.b)
Identificar aspectos del entorno TI sujetos a riesgos TI (26.b)
Identificar riesgos derivados del uso de TI (26.c.i)
Identificar CGTI que responden a estos riesgos (26.c.ii)
Evaluar el diseño e implementación de los CGTI (26.d)
Probar la eficacia operativa de los CGTI (NIA-ES 330)
(Entre paréntesis se indica el apartado correspondiente de la NIA-ES 315R/GPF-OCEX 1315R)

Figura 2

7. Identificación de las aplicaciones de TI y otros aspectos del entorno de TI que están sujetos a riesgos derivados de la utilización de TI

(Apartado 26.b, A167-172 de NIA-ES 315R/GPF-OCEX 1315R y 36-37 de la GPF-OCEX 1316R)

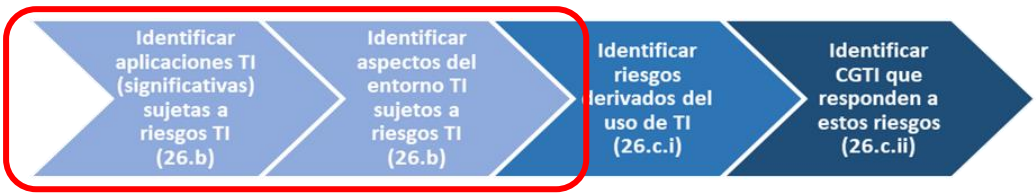

Figura 3

Como hemos visto, el auditor debe obtener conocimiento del componente de actividades de control mediante la aplicación de PVR a través de:

- **la identificación de las aplicaciones de TI significativas y otros aspectos del entorno de TI que están sujetos a riesgos derivados de la utilización de TI**;
- para dichas aplicaciones de TI y otros aspectos del entorno de TI identificados, la identificación de:
  i. los **riesgos derivados de la utilización de TI**; y
  ii. los **controles generales de TI** de la entidad que responden directamente a dichos riesgos.

7.1 Identificación de las aplicaciones TI significativas sujetas a riesgos derivados de la utilización de TI

Una vez identificadas las aplicaciones TI relevantes o significativas (de acuerdo con lo explicado en el apartado 7.2 de la GPF-OCEX 5340), que son aquellas aplicaciones TI relacionadas con procesos de negocio/gestión que soportan los TTSCIR significativos en las que se han identificado CPI, el auditor debe identificar las que están sujetas a riesgos derivados de la utilización de TI. En la práctica, normalmente, todas las aplicaciones TI significativas estarán sujetas, en mayor o menor grado, a riesgos derivados de la utilización de TI.[5]

El auditor también puede considerar el modo en que la información relativa a los TTSCIRS se almacena y procesa en el sistema de información y si la dirección confía en CGTI para mantener su integridad.

La amplitud del conocimiento de los procesos de TI y de los CGTI que necesita el auditor, variará según la naturaleza y las circunstancias de la entidad y de su entorno de TI, así como según la naturaleza y extensión de los controles identificados por el auditor. El número de aplicaciones de TI sujetas a riesgos derivados de la utilización de TI también variará en base a estos factores.

***Ejemplos** (A170):*

- *Es poco probable que una entidad que utiliza un software comercial y no tiene acceso al código fuente para realizar cambios en los programas tenga un proceso relativo a cambios en los programas, pero sí puede tener procedimientos para configurar el software (por ejemplo, el cuadro de cuentas, parámetros, etc.).*
- *Por el contrario, es posible que una entidad de gran dimensión confíe en mayor grado en las TI y el entorno de TI puede involucrar múltiples aplicaciones y los procesos de TI pueden ser complejos, incluido el que la entidad haya implementado CGTI formales sobre sus procesos.*
- *Cuando la dirección confíe en una aplicación de TI para el procesamiento o el mantenimiento de los datos y el volumen de datos sea significativo, y la aplicación de TI ejecute controles automatizados que el auditor también ha identificado, es probable que la aplicación de TI esté sujeta a riesgos por la utilización de TI.*

7.2 Identificación de otros aspectos del entorno de TI sujetos a riesgos derivados de la utilización de TI.

Cuando el auditor haya identificado aplicaciones de TI significativas sujetas a riesgos derivados de la utilización de TI, es muy probable que otros aspectos del entorno de TI estén sujetos a riesgos derivados de la utilización de TI (por ejemplo, bases de datos, sistema operativo, red y, en determinadas circunstancias, las comunicaciones mediante interfaces entre aplicaciones de TI y con la nube). Es importante tenerlos en cuenta porque esos aspectos de la infraestructura de TI dan apoyo e interactúan con las aplicaciones de TI.

[5] En el apartado 14 del Anexo 2 de la GPF-OCEX 5340 puede verse una serie factores de riesgo inherente relacionados con el uso de las TI.

Por lo general, no se identifican otros aspectos del entorno de TI cuando el auditor no identifica aplicaciones significativas sujetas a riesgos derivados de la utilización de TI.

Entre los riesgos derivados del uso de las TI en el entorno TI se pueden incluir los siguientes ejemplos:

- Las **bases de datos** almacenan los datos utilizados por las aplicaciones de TI y consisten en numerosas tablas de datos interrelacionadas. Se puede acceder a sus datos directamente mediante sistemas de gestión de bases de datos o mediante usuarios con permisos de administración de bases de datos. Cuando el auditor identifica aplicaciones de TI sujetas a riesgos derivados de la utilización de TI, también deben considerarse las bases de datos en las que se almacenan los datos procesados por esas aplicaciones.
- El **sistema operativo** (SO) es responsable de la gestión de las comunicaciones entre el hardware, las aplicaciones de TI y otro software utilizado en la red. Por tanto, debido a que la capacidad de funcionar de una aplicación de TI a menudo depende del SO y a que se puede acceder a las aplicaciones de TI y a las bases de datos desde el SO, el SO está habitualmente sujeto a riesgos derivados de la utilización de TI.
- Se utiliza una **red** en la infraestructura de TI para transmitir datos y compartir información, recursos y servicios a través de una conexión de comunicaciones común. La red también establece habitualmente una capa de seguridad lógica para el acceso a los recursos subyacentes. Se puede identificar la red como sujeta a riesgos TI cuando es un punto central de acceso a las TI y a las bases de datos, o cuando una aplicación de TI interactúa con proveedores o con terceros a través de internet.

8. Identificación de riesgos derivados de la utilización de TI

(Apartado 12.i, 26.c, A173-A174 y Anexo 5 de NIA-ES 315R/GPF-OCEX 1315R y 38 de la GPF-OCEX 1316R)

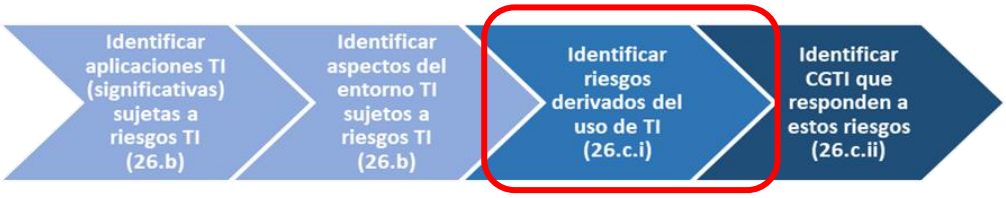

Figura 4

En la NIA-ES 315R se definen los **riesgos derivados de la utilización de TI** como la exposición de los CPI a un diseño o un funcionamiento ineficaces, o riesgos para la integridad de la información (es decir, la completitud, exactitud y validez de las transacciones y demás información) en el sistema de información de la entidad, **debido a un diseño o a un funcionamiento ineficaz de los procesos de TI de la entidad.**

En la identificación de riesgos derivados de la utilización de TI, el auditor puede considerar la naturaleza de la aplicación de TI identificada u otro aspecto del entorno de TI y los motivos por los que están sujetos a riesgos derivados de la utilización de TI.

Algunos **ejemplos de riesgos** derivados de la utilización de TI señalados en el Anexo 5 de la NIA-ES 315R:

- **Accesos no autorizados a los datos** que pueden producir su destrucción o su modificación indebida, incluido el registro de transacciones no autorizadas o inexistentes, o un registro inexacto de las transacciones.

  Puede haber riesgos relacionados con el acceso no autorizado de personal interno o de terceros (que, a menudo, se denominan riesgos de **ciberseguridad)**.

- Es importante recordar que los **ciber-incidentes** ocurren habitualmente en primer lugar a través de las capas del perímetro y de la red, que tienden a estar más alejadas de la aplicación de TI, de la base de datos y de los sistemas operativos que afectan a la preparación de los estados financieros. En consecuencia, si se ha identificado información acerca de un fallo de seguridad, el auditor, por lo general, considera hasta qué punto ese fallo tiene el potencial de afectar a la información financiera. Si puede haber sido afectada la información financiera, el auditor puede decidir profundizar en su conocimiento y comprobar los correspondientes controles para determinar el posible impacto o el alcance de incorrecciones potenciales materiales en los estados financieros.
- La posibilidad de que el personal del departamento de TI obtenga **permisos de acceso más allá de los necesarios** para realizar sus tareas, no existiendo así una segregación de funciones.

- **Cambios no autorizados en los datos de los ficheros maestros**.
- **Cambios no autorizados en aplicaciones de TI o en otros aspectos del entorno de TI.** Al considerar si las aplicaciones de TI para las que el auditor haya identificado controles automatizados están sujetas a riesgos derivados de la utilización de TI, es probable que el auditor considere si, y en qué grado, la entidad podría tener acceso al código fuente que permite realizar cambios en los programas o en las aplicaciones de TI. El grado en que la entidad realiza cambios en los programas o en la configuración y el grado en que los procesos de TI para esos cambios están formalizados también pueden ser consideraciones relevantes.
- No realizar cambios necesarios en las aplicaciones de TI o en otros aspectos del entorno de TI.
- Intervención manual inadecuada.
- **Pérdida potencial de datos** o incapacidad de acceder a los datos en tiempo y forma necesarios.
- El empleo de **proveedores de servicios** para algunos aspectos de su entorno de TI (p.e., subcontratando a un tercero para el alojamiento de su entorno de TI o utilizando un centro de servicios compartidos para la gestión centralizada de los procesos de TI en un grupo).
- Además, es posible que las disposiciones legales y reglamentarias que puedan tener un efecto directo o indirecto en los estados financieros de la entidad contengan **normas de protección de datos**. La consideración del cumplimiento por la entidad de las **disposiciones legales y reglamentarias**, de conformidad con la NIA 250 (Revisada) puede incluir la obtención de conocimiento de los procesos de TI de la entidad y de los controles de TI que la entidad ha implementado con fines de cumplimiento.

En el apartado 14 del Anexo 2 de la GPF-OCEX 5340 puede verse una serie factores de riesgo inherente relacionados con el uso de las TI.

La extensión y la naturaleza de los riesgos identificados derivados de la utilización de TI varían según la naturaleza y las características de las aplicaciones de TI y otros aspectos del entorno de TI. **Es más probable que haya más riesgos derivados de la utilización de TI cuanto mayor sea el volumen o la complejidad de los controles automatizados y la dirección otorgue una mayor confianza a dichos controles** para un procesamiento eficaz de las transacciones o el mantenimiento eficaz de la integridad de la información subyacente.

Es posible que el auditor haya identificado algún **riesgo para el cual los procedimientos sustantivos por sí solos no son suficientes** debido a la utilización por la entidad de un procesamiento de las transacciones **muy automatizado** y sin papel, lo que puede involucrar múltiples aplicaciones de TI integradas. En esas circunstancias, los controles identificados por el auditor probablemente incluyan controles automatizados que se deberán revisar.

9. Identificación de los CGTI que responden a los riesgos TI

(Apartado 26.c y A150, A166, Anexo 5 de NIA-ES 315R/GPF-OCEX 1315R y 39, 41 y 61 de la GPF-OCEX 1316R)

Los CGTI son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI de la organización auditada y ayudan a asegurar su correcto funcionamiento. Son controles relacionados con el uso de las tecnologías de la información y las comunicaciones implantados en los distintos niveles de la estructura organizativa general de una entidad y en sus sistemas de información. Normalmente son **controles indirectos**.

Los CGTI se implementan para responder a los riesgos derivados de la utilización de TI.

Figura 5

9.1 Finalidad de los CGTI

La **finalidad** de los CGTI en un entorno de administración electrónica es establecer un marco general de control y confianza sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno y posibilitar el correcto funcionamiento de los CPI.

Desde el punto de vista del auditor del sector público, los **objetivos de los CGTI** son proporcionar una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplen las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el ENS, de **obligado cumplimiento** en el sector público.

Objetivos de los CGTI	Descripción
Confidencialidad	Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Integridad	Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. *Según la NIA-ES 315R esta propiedad incluye la completitud, exactitud y validez de la información.*
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
Autenticidad	Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.[6]
Trazabilidad	Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Figura 6

Los CGTI deben diseñarse para cumplir uno o varios de los objetivos anteriores.

La importancia de los CGTI radica en que tienen un efecto generalizado, es decir, suelen afectar a más de una aplicación informática, y si no funcionan adecuadamente no se podrá confiar en los CPI y será necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos. Es decir, la eficacia de los CGTI afecta a la estrategia de auditoría que se debe adoptar. Para más detalles ver la GPF-OCEX 5340.

9.2 Identificar CGTI

El auditor utiliza el conocimiento obtenido de las aplicaciones de TI significativas identificadas y otros aspectos del entorno de TI y los correspondientes riesgos derivados de la utilización de TI para determinar qué CGTI identificar. En algunos casos, una entidad puede utilizar procesos de TI comunes en su entorno de TI o entre ciertas aplicaciones de TI, en cuyo caso se pueden identificar riesgos comunes derivados de la utilización de TI y CGTI también comunes.

Cuanto mayor sea la extensión de los CPI automatizados, o de los controles en los que participa algún proceso automatizado, que utilice la dirección y en los que confíe en relación con su información financiera, más importante será para la entidad implementar CGTI eficaces y para el auditor identificarlos y revisarlos.

Además, unos CGTI sólidos constituyen una buena línea de defensa para la ciberseguridad.

Hay que destacar que el auditor no es responsable de conocer todos los CGTI existentes en el entorno TI y realizar las pruebas subsiguientes. La responsabilidad del auditor se limita a los CGTI que respaldan CPI relevantes que tienen una relación directa con la preparación de los estados financieros o con los objetivos de una auditoría de cumplimiento o de otro tipo.

[6] En la literatura "no ENS", por ejemplo, el INCIBE o las normas ISO, se habla de las tres dimensiones de la seguridad, y la autenticidad y la trazabilidad se encuentran incluidas en "integridad".
También se encuentra incluida en la integridad el "no repudio" que es la cualidad que impide que un individuo niegue falsamente haber realizado una determinada acción y proporciona la capacidad de determinar si un determinado individuo realizó una determinada acción, como crear información, enviar un mensaje, aprobar una operación o recibir un mensaje.

Si no hay aplicaciones TI ni otros elementos del entorno TI sujetos a riesgos derivados de la utilización de TI, no se deben identificar ni revisar los CGTI.

En general, es probable que se identifique un mayor número de CGTI relacionados con aplicaciones TI y bases de datos que con otros aspectos del entorno de TI. Esto es así porque estos están más estrechamente relacionados con el procesamiento y almacenamiento de la información en el sistema de información de la entidad.

El auditor debe identificar los riesgos derivados de la utilización de TI y los CGTI relacionados con las aplicaciones relevantes identificadas y otros aspectos del entorno de TI implementados por la entidad para responder a esos riesgos ya que **su conocimiento puede afectar a:**

- La decisión del auditor sobre si probar la eficacia operativa de los CPI para responder a los RIM identificados en los estados financieros.

  Ejemplo: *Cuando los CGTI no están diseñados de un modo eficaz o no están debidamente implementados para responder a los riesgos derivados de la utilización de TI (por ejemplo, los controles no previenen o detectan cambios no autorizados en los programas o accesos no autorizados a aplicaciones de TI), esto puede influir en la decisión del auditor para no confiar en controles automatizados en la aplicación de TI afectada.*

- La valoración por el auditor del riesgo inherente en las afirmaciones.

  Ejemplo*: Cuando hay cambios significativos y extensos en los programas de una aplicación de TI para tratar nuevos requerimientos de información financiera, puede ser un indicio de la complejidad de estos y de su efecto en los estados financieros de la entidad. Cuando se producen tales cambios en los programas o en los datos, es probable que la aplicación de TI esté sujeta a riesgos derivados de la utilización de TI.*

- La valoración por el auditor del riesgo de control en las afirmaciones.

  Ejemplo: *La eficacia operativa de un CPI puede depender de determinados CGTI que previenen o detectan cambios no autorizados en la aplicación TI y en los CPI. En tales circunstancias, la esperada eficacia operativa del CGTI (o su ausencia) puede influir en la valoración por el auditor del riesgo de control (por ejemplo, el riesgo de control puede ser más elevado cuando se espera que dichos CGTI sean ineficaces o si el auditor no tiene previsto probar los CGTI).*

- La estrategia del auditor para probar la información producida por las aplicaciones de TI de la entidad o que involucra información originada por estas.

  Ejemplo: *Cuando la información producida por la entidad que vaya a ser utilizada como evidencia de auditoría sea generada por aplicaciones de TI, el auditor puede decidir probar controles sobre informes generados por el sistema, incluida la identificación y comprobación de los CGTI que responden a los riesgos de cambios inapropiados o no autorizados en los programas o cambios directos de datos en los informes.*

- El diseño de procedimientos posteriores de auditoría.

9.3 Determinar qué controles son relevantes

Aunque la nueva NIA-ES 315R omite la definición del concepto de control relevante para la auditoría, a efectos prácticos seguiremos utilizándolo, entendiendo como tales aquellos controles que se deben identificar de acuerdo con el apartado 26 de la NIA-ES 315R.

Un control será relevante cuando su ausencia o su mal funcionamiento representa una deficiencia significativa o una debilidad material de control interno. Por ejemplo, si su mal funcionamiento invalida la eficacia un CPI relevante.

Todos los controles no son iguales en su grado de eficacia a la hora de reducir los riesgos identificados y no será necesario evaluar todos los controles relacionados con un riesgo concreto. Por tanto, hay que focalizar el trabajo en aquellos controles que sean relevantes, es decir, aquellos que proporcionan una mayor seguridad de que el objetivo de control se ha alcanzado.

Al decidir si un control es relevante, debe aplicarse el juicio profesional, y se tendrá en cuenta lo siguiente:

- Los controles relevantes generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos significativos y alcanzar el objetivo de control relacionado.

- Los controles relevantes a menudo respaldan más de un objetivo de control.

***Por ejemplo**, los controles de acceso respaldan la integridad y validez de las transacciones financieras, las valoraciones contables, la segregación de tareas, etc.*

Puede resultar efectivo hacer una combinación de controles relevantes a fin de alcanzar un objetivo concreto o bien una serie de objetivos, para no depender demasiado de un solo control.

- Los controles que hacen frente directamente a los riesgos significativos son con frecuencia relevantes.

  ***Por ejemplo**, el riesgo de acceso no autorizado es un riesgo significativo para la mayoría de entidades; por tanto, los controles que previenen o detectan accesos no autorizados son importantes.*

- Los controles automatizados son más fiables que los controles manuales.

  ***Por ejemplo**, los controles automatizados que obligan a cambiar periódicamente de contraseña son más fiables que las normas genéricas que no son de uso forzoso. Los procesos manuales también están expuestos a errores humanos.*

- La ausencia de un control determinado no significa que el sistema de control interno de una entidad tenga un diseño inadecuado, ya que en muchos casos el riesgo provocado por aquella deficiencia puede ser mitigado por un **control compensatorio**. Situaciones de este tipo se presentan con frecuencia en las organizaciones pequeñas.

9.4 Tipos de controles

A la hora de analizar un control se debe tener presente sus características y tipología:

Tipo	Características	Ejemplos
Preventivo	Su finalidad es prevenir que ocurra un hecho que no es consistente con los objetivos de control. Detecta los problemas antes de que sucedan. Monitoriza las operaciones y los inputs y previene errores, omisiones o actos malintencionados.	Limitar el acceso a los sistemas TIC. Limitar el acceso mediante perfiles de usuario y contraseñas a cambiar programas reduce el riesgo de transacciones no autorizadas.
Detectivo	Detectan e informan de la ocurrencia de un error, omisión o acto malintencionado.	Un supervisor revisa todos los pases a producción de los cambios en las aplicaciones para verificar que están autorizados.
Compensatorio	Si es efectivo, puede limitar o mitigar la gravedad de una deficiencia de control interno. Limitan la gravedad de una deficiencia y sus consecuencias, pero no la eliminan.	En entidades de pequeñas los controles de segregación de funciones pueden ser difíciles de implantar y deben compensarse con otros que supongan una mayor supervisión.
Correctivo	Si han fallado los controles preventivos y ha sucedido un incidente o un desastre, permite recuperarse.	Copias de seguridad.

Figura 7

Los controles **preventivos** son por regla general más eficaces que los **detectivos** en tanto que previenen que se produzca el error en vez de detectarlo después de que éste ya se haya producido. Por lo tanto, los controles preventivos se consideran a menudo relevantes.

***Por ejemplo**, prevenir que se produzca un fraude es mejor que simplemente detectarlo después de que haya ocurrido.*

10. Evaluación del diseño e implementación (D+I) de los CGTI relevantes

(Apartado 26.d, A175 y 176 de NIA-ES 315R/GPF-OCEX 1315R y 40 de la GPF-OCEX 1316R)

Figura 8

Para cada uno de los controles identificados que sean relevantes o significativos el auditor debe:

a) **Evaluar si el control está diseñado (D) eficazmente** para responder al RIM en las afirmaciones (CPI) o si está diseñado eficazmente para sustentar el funcionamiento de otros controles (CGTI). Implica que el auditor considere si el control, de manera individual o en combinación con otros controles, es capaz de prevenir de modo eficaz, o de detectar y corregir, incorrecciones materiales (es decir, permite alcanzar el objetivo de control) o si es capaz de sustentar el funcionamiento de otros controles.

b) **Determinar si el control ha sido implementado (I)** estableciendo que el control existe y que la entidad lo está utilizando.

No tiene mucho sentido que el auditor evalúe la implementación de un control que no tenga un diseño eficaz. En consecuencia, el auditor evalúa en primer lugar el diseño del control. Un control incorrectamente diseñado o implementado puede representar una **deficiencia de control**.

Cuando el auditor haya comprobado el D+I de un CPI y vaya a confiar en su eficacia operativa como parte de su respuesta para abordar los RIM valorados y esos controles dependen de los CGTI, el auditor deberá comprobar también el D+I de esos CGTI y después probar la eficacia operativa de los CGTI.

Para cada CGTI que se identifique como relevante, el auditor debe aplicar PVR para **analizar la efectividad de su diseño para realizar la actividad de control y su implementación**, considerando el riesgo TI y los objetivos de la auditoría. Si se concluye que el diseño e implementación es eficaz se aplicarán procedimientos posteriores de auditoría para **verificar si está en funcionamiento durante todo el periodo auditado**.

Como ya se ha indicado, el alcance del trabajo de revisión de los CGTI es una cuestión de juicio profesional. El auditor **no** es responsable de identificar **todos** los CGTI del entorno de TI y revisará la eficacia operativa **solo** de los CGTI relevantes para los objetivos de la fiscalización.

El resto de CGTI no relevantes carece de interés para la auditoría financiera. Si se revisan los CGTI de algún sistema o subsistema que no tiene relación con la información de interés para la auditoría se estará haciendo un trabajo innecesario y por tanto ineficiente.

> ***Por ejemplo*** *si se está revisando una aplicación de gestión de nóminas por ser los gastos de personal un TTSCIRS, los procedimientos de revisión de los CGTI estarán focalizados en aquellos que afectan más directamente a esa aplicación; en este caso no tendría ningún interés revisar los controles relacionados con el desarrollo y mantenimiento de la aplicación de gestión del inmovilizado, tampoco se revisarían los controles de acceso o la gestión de usuarios de la aplicación de ingresos, ya que esos trabajos no nos permitirían reducir el riesgo de auditoría del área de gastos de personal. Se deberían revisar los CGTI relacionados con la aplicación de recursos humanos, con la de nóminas, las bases de datos de ambas aplicaciones, y con los sistemas operativos y servidores que soportan dichas aplicaciones y bases de datos.*

11. Revisión de la eficacia operativa de los CGTI relevantes

(Apartados 8-17 de la NIA-ES-SP 1330 y apartado 65 de la GPF-OCEX 1316R)

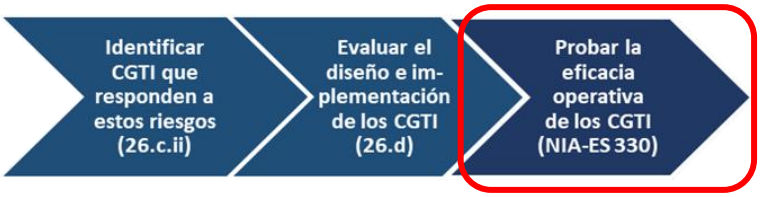

Figura 9

11.1 Pruebas de controles

Si el auditor planea probar la eficacia operativa de un CPI automatizado será necesario, además de evaluar el D+I de los CGTI, probar previamente la eficacia operativa de los CGTI relacionados que sustentan su funcionamiento continuo y eficaz. *(Apartados 26, A150 y A229 de la NIA-ES 315R)*

La NIA-ES-SP 1330 *(10.b)* establece que, al diseñar y ejecutar pruebas de controles, el auditor determinará si los controles a comprobar dependen a su vez de otros controles (controles indirectos) y, si es así, si es necesario obtener evidencia adicional de auditoría que acredite el funcionamiento efectivo de dichos controles indirectos.

> ***Por ejemplo****: una entidad puede tener correctamente configurada la segregación de funciones en el proceso de compras, contabilidad y pago; pero si no existe un CGTI que establezca mecanismos de identificación y autenticación de los usuarios que sea eficaz, todo el sistema de segregación de funciones devendrá a su vez en ineficaz y no confiable.*

La NIA-ES-SP 1330 también establece lo siguiente:

8. *El auditor diseñará y realizará **pruebas de controles** con el fin de obtener evidencia de auditoría suficiente y adecuada sobre la **eficacia operativa de los controles** relevantes si:*

   (a) la valoración de los riesgos de incorrección material en las afirmaciones realizada por el auditor comporta la expectativa de que los controles estén operando eficazmente (es decir, para la determinación de la naturaleza, momento de realización y extensión de los procedimientos sustantivos, el auditor tiene previsto confiar en la eficacia operativa de los controles); o

   (b) los procedimientos sustantivos por sí mismos no pueden proporcionar evidencia de auditoría suficiente y adecuada en las afirmaciones.

9. *En el diseño y aplicación de pruebas de controles, el auditor obtendrá evidencia de auditoría más convincente cuanto más confíe en la eficacia de un control.*

La obtención de evidencia de auditoría sobre la implementación de un **control manual** en un determinado momento **no proporciona evidencia** de auditoría sobre la eficacia operativa del control en otros momentos del periodo que comprende la auditoría.

En el caso de **CPI automatizados**, el auditor puede planificar comprobar su eficacia operativa mediante la identificación y comprobación de CGTI que aseguran el funcionamiento congruente del CPI automatizado (por ejemplo, auditando los controles de acceso y los controles de gestión de cambios) en vez de aplicar pruebas de eficacia operativa directamente sobre los CPI automatizados[7].

Si bien la razón más común por la que se prueba la eficacia operativa de un CGTI es apoyar la evaluación por parte del auditor de la eficacia operativa de un CPI automatizado, puede haber otros casos en los que las pruebas sobre la eficacia operativa de los CGTI sean pertinentes para otros procedimientos, que pueden incluir:

- Controles sobre los asientos de diario: el auditor puede confiar en los CGTI relativos a la administración de los permisos para registrar los asientos de diario no estándar y se deberán comprobar.
- Informes personalizados: cuando los procedimientos sustantivos del auditor utilizan informes generados por el sistema, el auditor probará la eficacia operativa de los CGTI que abordan el riesgo de cambios inapropiados, no autorizados o directos en el informe.
- Revisar aspectos específicos del control interno, adicionales a las necesidades de una auditoría financiera, por la exigencia superior de revisar el cumplimiento de los auditores públicos. Por ejemplo, los controles relacionados con la LOPD, la ciberseguridad o con el cumplimiento legal.

En la NIA-ES-SP 1330 se señalan diversos aspectos a tener en cuenta en las pruebas sobre la eficacia operativa de los controles, incluidas las pruebas de controles indirectos.

Aunque principalmente el auditor puede centrarse en los CGTI que apoyan los CPI integrados en las aplicaciones TI, ya que su impacto en la información financiera puede identificarse fácilmente, **también es muy importante que el auditor aborde los riesgos derivados del uso de TI identificados en otros elementos del entorno TI como los accesos a las bases de datos subyacentes**.

> ***Ejemplo:*** *Un auditor planea confiar en la eficacia operativa de un CPI de la aplicación de contabilidad de la entidad que requiere la triple coincidencia de una orden de compra, el albarán del proveedor y su factura para contabilizar la compra. El auditor ha evaluado el diseño, determinado que se ha implementado y probado la eficacia operativa del CPI y, como parte de esta prueba, también prueba el CGTI que evita cambios no autorizados en el CPI.*
>
> *Sin embargo, el auditor ha identificado que no existen controles que impidan el acceso no autorizado a la base de datos que almacena los nombres de usuario y contraseñas de personas autorizadas que pueden realizar cambios en el CPI. Esto ocasionará en que el auditor no podrá confiar en los resultados de las pruebas, incluso si el CGTI para evitar cambios no autorizados en el control estaba funcionando.*
>
> *El auditor puede ser capaz de realizar procedimientos alternativos, como revisar manualmente los registros para verificar si se realizaron cambios en la forma en que funcionaba el control.*

La realización de pruebas sobre la eficacia operativa de los controles no es lo mismo que la obtención de conocimiento y la evaluación de su diseño e implementación. Sin embargo, se utilizan los mismos tipos de

[7] Apartado A180 de la NIA-ES 315R/GPF-OCEX 1315R.

procedimientos de auditoría. En consecuencia, **es posible que el auditor decida que resulta eficiente probar la eficacia operativa de los controles al mismo tiempo que se evalúa su diseño y se determina si han sido implementados.** En este sentido, aunque algunos PVR no hayan sido específicamente diseñados como pruebas de controles, pueden, no obstante, proporcionar evidencia de auditoría sobre la eficacia operativa de los controles y, consecuentemente, ser utilizados como pruebas de controles. *(NIA-ES-SP 1330, A21 y A22)*

Al revisar los CGTI, **los auditores necesitarán conocimientos especializados** como los proporcionados por auditores de TI para ayudarlos a obtener suficiente evidencia de auditoría adecuada a medida que aumenta la complejidad del entorno de TI. Los especialistas en auditoría de sistemas de información **analizarán con los auditores financieros** aquellos controles que son relevantes para los objetivos de la auditoría financiera, ya que no todos los riesgos son iguales, ni en probabilidad, ni en su materialidad.

El OCEX debe garantizar que los miembros del equipo de fiscalización y, en su caso, los expertos externos que formen parte del equipo colectivamente tengan la competencia y las capacidades adecuadas para realizar la fiscalización.

11.2 ¿La eficacia operativa de los CGTI tiene que ser probada cada año?

En determinadas circunstancias, las normas de auditoría permiten a los auditores utilizar evidencia de auditoría sobre la eficacia operativa de los controles obtenida en auditorías anteriores. Los párrafos 13 y 14 de la NIA-ES-SP 1330 describen las consideraciones, restrictivas, para que el auditor determine si es apropiado utilizar evidencia de auditoría sobre la eficacia operativa de los controles obtenida en auditorías anteriores.

Destacaremos aquí que:

(a) **Si se han producido cambios** que afectan a la continuidad de la relevancia de la evidencia de auditoría procedente de la auditoría anterior, **el auditor realizará pruebas sobre los controles en la auditoría actual.**

(b) **Si no se han producido tales cambios, el auditor probará los controles al menos en una de cada tres auditorías,** realizando pruebas sobre algunos controles en cada auditoría para evitar la posibilidad de que se prueben en un solo periodo de auditoría todos los controles en los que tenga previsto confiar y no se realice prueba alguna en los dos periodos de auditoría subsiguientes.

Cuando se trate de controles sobre riesgos significativos no se confiará en el trabajo realizado en años anteriores y se deberán realizar pruebas sobre los controles en la auditoría actual *(apartados 15 y A37b de la NIA-ES-SP 1330).* Esto incluirá tanto CPI que abordan directamente esos riesgos significativos como los CGTI que los soportan.

Ejemplo: *Normalmente los controles de acceso deberán revisarse siempre.*

El auditor debe también considerar la eficacia de los CGTI al determinar si las pruebas de auditoría relativas a la eficacia de un CPI en particular de un período anterior pueden utilizarse en el período actual.

12. Qué sucede si los CGTI no se diseñan e implementan adecuadamente o no funcionan de manera efectiva

(Apartado 37 de NIA-ES 315R/GPF-OCEX 1315R)

Una vez que el auditor haya comprobado la eficacia operativa de los controles de conformidad con la NIA-ES-SP 1330, podrá confirmar su expectativa inicial acerca de la eficacia operativa de los controles. **Si los controles no están funcionando eficazmente según lo esperado, el auditor tendrá que revisar la valoración del riesgo de control** de conformidad con el apartado 37 de la NIA-ES 315R/GPF-OCEX 1315R.

Si el auditor espera que los correspondientes CGTI sean ineficaces, esta determinación puede afectar a su valoración del riesgo de control en las afirmaciones y sus procedimientos posteriores de auditoría probablemente tengan que incluir procedimientos sustantivos para responder a los riesgos derivados de la utilización de TI.

En el apartado A31 de la NIA-ES 330 (2024) se señala que **cuando el auditor determina que un CGTI es deficiente**, puede tener en cuenta la naturaleza del riesgo o los riesgos identificados relacionados derivados de la utilización de TI, para sustentar el diseño de los procedimientos adicionales para responder al riesgo valorado de incorrección material. Esos procedimientos pueden tratar la determinación de si:

- El riesgo o los riesgos derivados de la utilización de TI se han materializado.

  ***Por ejemplo**, si los usuarios tienen un acceso no autorizado a una aplicación de TI (pero no pueden acceder a modificar los registros del sistema que rastrean los accesos), el auditor puede examinar los registros del sistema para obtener evidencia de auditoría de que dichos usuarios no accedieron a la aplicación de TI durante el periodo*.

- Existen otros CGTI alternativos, o cualquier otro control, que responden al riesgo o a los correspondientes riesgos derivados de la utilización de TI. En ese caso, el auditor puede identificar esos controles (si no han sido aún identificados) y, en consecuencia, evaluar su diseño, determinar que han sido implementados y realizar pruebas de su eficacia operativa.

  ***Por ejemplo**, si un CGTI relacionado con el acceso de usuarios es deficiente, es posible que la entidad disponga de un control alternativo (compensatorio) mediante el cual la dirección revisa de manera oportuna los informes de acceso de los usuarios finales.*

Cuando **no existan CGTI alternativos o el auditor no pueda diseñar procedimientos sustantivos adecuados** para hacer frente a los riesgos existentes derivados del uso de TI, el auditor **no podrá confiar** en:

- La eficacia operativa de los CPI automatizados dentro de las aplicaciones TI afectadas (ya que los controles no pueden prevenir o detectar adecuadamente cambios no autorizados de programas o el acceso a aplicaciones informáticas).
- La integridad, exactitud y validez de los informes generados por el sistema utilizados para en la auditoría, u otros informes elaborados internamente por el ente auditado y los controles manuales dependientes de TI que se basan en dichos informes (ya que es posible que no esté garantizada la integridad de la información de dichos informes).
- La eficacia operativa de los controles de entrada (CPI) que proporcionan garantías sobre los datos introducidos en el sistema (ya que la aplicación informática puede no reducir suficientemente el riesgo de cambios intencionados o involuntarios erróneos en los datos una vez introducidos en el sistema). Esto también puede afectar a cualquier procedimiento analítico sustantivo que el auditor haya planeado realizar y que se base en esos datos.

En circunstancias en las que el auditor haya determinado, de conformidad con el párrafo 33 la NIA-ES 315R / GPF-OCEX 1315R que los procedimientos sustantivos por sí solos no pueden proporcionar suficiente evidencia de auditoría adecuada para hacer frente a un riesgo y no se pueden llevar a cabo procedimientos alternativos, habrá un impacto en la capacidad del auditor para obtener suficiente evidencia de auditoría adecuada **y en su opinión de auditoría**.

13. Los CGTI en el entorno TI

Los CGTI se pueden establecer en los siguientes niveles (ver figura 1):

a) Nivel de la entidad

Los controles a este nivel se reflejan en la forma de funcionar de una organización, e incluyen políticas, procedimientos y otras prácticas de alto nivel que marcan las pautas de la organización incluyendo las materias relacionadas con las TI. Forman el entorno de control de una entidad, uno de los cinco componentes del sistema de control interno. Ver apartado 4 de esta guía.

El entorno de control y el compromiso con comportamientos éticos es una "filosofía" de trabajo que debe emanar de arriba hacia abajo, desde los altos puestos directivos hacia el resto de la organización. Es esencial que un tono de control adecuado sea marcado por los máximos responsables de la entidad; y que se envíe un mensaje a toda la organización de que los controles deben ser tomados en serio.

Los controles a nivel de entidad tienen influencia significativa sobre el rigor con el que el sistema de control interno es diseñado y opera en el conjunto de los procesos. La existencia de unos CGTI rigurosos a este nivel, como son, por ejemplo, unas políticas y procedimientos bien definidos y comunicados, con frecuencia sugieren un entorno operativo TI más fiable.

En sentido contrario, las organizaciones con unos controles débiles a este nivel es más probable que tengan dificultades a la hora de realizar actividades de control regularmente. La capacidad de la dirección para eludir

controles y un pobre tono de control (que se manifiesta a nivel de la entidad) son dos aspectos comunes en un mal comportamiento corporativo.

Estos controles se recogen en la categoría A. Gobernanza de la figura 10.

b) Nivel de procesos/aplicaciones de gestión/aplicaciones de TI

Los procesos de gestión (o procesos de negocio) son los mecanismos que emplea una entidad para desarrollar su actividad y prestar un servicio a sus destinatarios o usuarios y normalmente estarán soportados por aplicaciones de TI.

Los CGTI a este nivel consisten en las políticas y procedimientos establecidos para controlar determinados aspectos relacionados con la gestión de la seguridad, controles de acceso lógico, gestión de la configuración y de los usuarios en las aplicaciones de TI. Estarán también relacionados con su naturaleza y complejidad.

> ***Por ejemplo**, los CGTI garantizarán razonablemente que los cambios en el software de las aplicaciones son verificados totalmente y están autorizados.*
>
> ***Por ejemplo**, serán relevantes más controles en el caso de aplicaciones de TI altamente integradas con opciones de seguridad complejas que en una aplicación de TI heredada (obsoleta) que soporta un número reducido de saldos contables con métodos de acceso únicamente a través de transacciones.*

Cuando son examinados los CGTI a nivel de aplicación, el auditor financiero y el auditor de sistemas evalúan los controles de acceso lógico que limitan o restringen el acceso a determinadas aplicaciones y ficheros relacionados (como, por ejemplo, el fichero maestro de empleados) a usuarios autorizados bajo los principios de necesidad de saber, de mínimo privilegio y de segregación de funciones.

> ***Por ejemplo**, un empleado de la función de nóminas puede tener acceso a las aplicaciones sobre nóminas, pero puede tener restringido el acceso a una determinada tarea, como puede ser la revisión o actualización de datos de las nóminas sobre los empleados del propio departamento de nóminas o sobre los datos del maestro de empleados.*

c) Nivel de la infraestructura TI

La infraestructura TI incluye la gestión de redes y comunicaciones, la gestión de bases de datos, la gestión de sistemas operativos, la gestión de almacenamiento, la gestión de las instalaciones y sus servicios y la administración de seguridad. Todo ello está gestionado, normalmente, por un departamento TI.

El auditor debe evaluar separadamente los distintos subniveles o capas tecnológicas:

- ✓ **Bases de datos**

  Los CGTI en la capa de base de datos normalmente responden a los riesgos derivados de modificaciones no autorizadas de la información financiera mediante el acceso directo a las bases de datos o la ejecución de una secuencia de comandos (script) o de un programa.

- ✓ **Sistemas operativos (SO)**

  Es el software que controla la ejecución de otros programas de ordenador, programa tareas, distribuye el almacenamiento, gestiona las interfaces y muestra la interfaz por defecto con el usuario cuando no hay funcionando ningún otro programa. También se incluye en este apartado el middleware, los sistemas de virtualización, utilidades diversas y aplicaciones no relacionadas con los procesos de gestión de la actividad de la entidad.

  Es muy importante realizar determinados procedimientos de auditoría para analizar los controles existentes a este nivel, ya que vulnerabilidades en los SO tienen un impacto potencial en todo el sistema de información. Aunque las aplicaciones y las bases de datos tengan buenos controles, si un intruso pudiera penetrar sin restricciones en el sistema operativo y su sistema de carpetas, podría provocar graves daños en los datos y sistemas de la entidad.

- ✓ **Redes**

  Los CGTI en la capa de red normalmente responden a los riesgos TI relacionados con la segmentación de la red, el acceso remoto y la autenticación. Los controles a este nivel son más relevantes cuando la entidad dispone de aplicaciones web para procesos que gestionan información financiera. También son importantes cuando existen accesos o intercambios de información con proveedores o existen servicios externalizados que requieren mayor volumen de transmisión de datos y/o accesos remotos.

✓ **Infraestructura física**

Son todos los elementos físicos, el *hardware* y las instalaciones.

Cuando los CPDs no están protegidos físicamente, pueden surgir diversos riesgos y consecuencias, que pueden conducir a accesos no autorizados, violaciones de datos, interrupción de los servicios, daños a la reputación y consecuencias legales. Los riesgos físicos más habituales se refieren a incendios, inundaciones, vandalismo, etc., que pueden derivar en la discontinuidad del servicio.

14. Categorías de controles generales

A los efectos de esta guía, los CGTI se han agrupado en **cinco** categorías, de acuerdo con el siguiente esquema.

Categorías de controles	Controles principales	Medidas del ENS
A. Gobernanza	A.1 Gobernanza sobre las TI	org, mp.per
	A.2 Cumplimiento normativo	
	A.3 Gobernanza de la ciberseguridad	org, mp.per
B. Gestión de cambios en aplicaciones y sistemas	B.1 Adquisición de aplicaciones y sistemas	op.pl.3 y 4
	B.2 Desarrollo de aplicaciones	mp.sw.1 y 2
	B.3 Gestión de cambios	op.exp.5, op.acc.3
C. Operaciones de los sistemas de información	C.1 Inventario de hardware y software	op.exp.1
	C.2 Gestión de vulnerabilidades	op.exp. 3 y 4
	C.3 Configuraciones seguras	op.exp.2, 3 y 4
	C.4 Registro de eventos y de la actividad de los usuarios	op.exp.8
	C.5 Servicios externos	op.ext.1 y 2 y nub.1
	C.6 Protección del entorno de TI	op.exp.6, mp.s, mp.eq
	C.7 Protección de las instalaciones e infraestructuras	mp.if
	C.8 Gestión de incidentes	op.exp.7 y 9
	C.9 Monitorización del sistema y su seguridad	op.mon
	C.10 Protección de las comunicaciones	op.pl.2, mp.com, op.ext.4
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios de administración	op.acc.
	D.2 Gestión de usuarios	
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas	mp.info.6
	E.2 Plan de continuidad	op.cont.2 y 3 op.ext.3
	E.3 Alta disponibilidad	op.cont.4

Figura 10

Existen diversas clasificaciones de CGTI según el marco conceptual[8] que se consulte y de cuáles sean los objetivos de la auditoría, aunque los controles detallados que forman los controles principales son básicamente coincidentes en todos los casos.

Los controles descritos en esta guía están totalmente alineados con el ENS, que es de aplicación obligatoria en el sector público.

[8] Por ejemplo: INTOSAI/WIGITA, COBIT, FISCAM de la GAO, o la NIA-ES 315R que agrupa los CGTI en tres tipos: a) Procesos para gestionar el acceso, b) Procesos para la gestión de cambios en los programas o al entorno de TI y c) Procesos para la gestión de las operaciones de TI, que incluye los controles relacionados con la continuidad del servicio.

A. Gobernanza

Por qué son importantes estos controles

Ya se ha destacado en el apartado 4 anterior la importancia que la NIA-ES 315R/GPF-OCEX 1315R concede al conocimiento y evaluación del entorno de control, y como parte fundamental de este, al conocimiento y evaluación de la gobernanza sobre las TI (véase la GPF-OCEX 5331) y de su componente más importante en relación con los CGTI, la gobernanza de la ciberseguridad (véase la GPF-OCEX 5314).

Con estos controles se pretende asegurar que se cumplen diversas normas relevantes para mantener un adecuado control sobre la gestión de la seguridad de los sistemas de información y las comunicaciones (ENS), la privacidad de la información (LOPD) y el esquema nacional de interoperabilidad (ENI).

Es muy importante verificar que los entes auditados dan el debido cumplimiento a lo dispuesto por el Esquema Nacional de Seguridad, ya que su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designe a las unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización. La importancia de la gobernanza en la gestión de la ciberseguridad ha sido objeto de diversos documentos del Centro Criptológico Nacional (CCN), por ejemplo: *Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022*, la *Guía de Seguridad de las TIC CCN-STIC 201 Organización y Gestión para la Seguridad de las TIC* y la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*.

https://ens.ccn.cni.es/es/

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

Programa de auditoría del área

La revisión de esta área o categoría A está cubierta por las siguientes guías:

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría

B. Gestión de cambios en aplicaciones y sistemas

Por qué son importantes estos controles

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 son importantes porque 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.

Además, la gestión sistemática de los cambios en el entorno TI incluye la notificación de las actuaciones a las partes interesadas, permitiendo la programación de las actuaciones conforme a las circunstancias concretas de la entidad.

En general, estos controles se refieren a controles sobre el proceso para diseñar, programar, probar y migrar los cambios a un entorno de producción (es decir, de usuario final) y a controles que segregan el acceso para ejecutar y migrar los cambios a un entorno de producción.

Ejemplos[9]

Ejemplos de riesgos TI	Ejemplos de CGTI
Cambios en las aplicaciones: Se realizan cambios inapropiados en los sistemas o aplicaciones que contienen CPI relevantes (es decir, parámetros configurables, algoritmos automatizados, cálculos automatizados y extracción de datos automatizada) o lógica de informes.	*Pruebas de aceptación* Los cambios en las aplicaciones se prueban adecuadamente antes de incorporarse al entorno de producción
	Segregación de entornos El acceso para realizar cambios en el entorno de producción de la aplicación está adecuadamente restringido y separado del entorno de desarrollo.
Cambios en las bases de datos: Se realizan cambios inapropiados en la estructura de las bases de datos y en las relaciones entre los datos, lo que puede provocar su pérdida o el deterioro de la calidad de los datos.	*Pruebas de aceptación* Se realizan pruebas de los cambios planificados. Estas pruebas se realizan únicamente sobre datos de prueba en entornos de preproducción.
Cambios en el software de sistemas: Se realizan cambios inapropiados en el software de sistemas (por ejemplo, sistema operativo, redes, software de gestión del cambio, software de control de accesos), lo que puede provocar el mal funcionamiento de las aplicaciones, de sus controles, pérdida de datos y afectación de la normal operativa de la entidad.	*Autorización de cambios* Previamente a la aplicación de cambios sobre sistemas que soportan procesos críticos de la organización, se informa y se solicita autorización del cambio a los responsables de estos procesos y servicios críticos. Se coordina con estos responsables la aplicación de los cambios en las ventanas temporales sin afección sobre el negocio.

Figura 11

Programa de auditoría del área

La revisión de esta área o categoría B está cubierta por la siguiente guía:

GPF-OCEX 5332 Gestión de cambios en aplicaciones y sistemas

[9] En este apartado 14, se presentan algunos ejemplos de riesgos derivados de la utilización de las TI y posibles CGTI, parcialmente extraídos de la NIA-ES 315R/GPF-OCEX 1315R (anexo 6), junto con otros de elaboración propia.

C. Operaciones de los sistemas de información

Por qué son importantes estos controles

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.

Ejemplos

Ejemplos de riesgos TI	Ejemplos de CGTI
Activos de sistemas de información: Se desconoce los activos a los que se debe proteger.	*Inventario de dispositivos físicos y lógicos* Existe un control activo del software y hardware de la organización que debe ser debidamente protegido.
	Control de acceso de dispositivos físicos El acceso a la red se limita mediante sistemas específicos de control de acceso, permitiendo la conexión únicamente a aquellos dispositivos, pertenecientes a la organización, que cumplen con las políticas de seguridad.
Red: La red no impide el acceso a los sistemas de la organización a usuarios no autorizados.	*Segmentación de redes* La red está estructurada para separar las aplicaciones orientadas a la web de la red interna, en la que se encuentran las aplicaciones TI significativas.
	Detección de intrusiones Se dispone de herramientas de detección y/o prevención de intrusiones que generan alertas de seguridad basadas en la verificación de reglas sobre el tráfico de red. Se dispone de procedimientos de respuesta a las alertas generadas por el sistema de detección y/o *prevención* de intrusiones, que inician acciones de contención sobre las amenazas materializadas.

Figura 12

Programa de auditoría del área

La revisión de esta área o categoría C está cubierta por la siguiente guía:

GPF-OCEX 5333 Operaciones de los sistemas de información

D. Controles de acceso a datos y programas

Por qué son importantes estos controles

Esta área incluye todos aquellos controles relativos a la gestión de usuarios, sus privilegios y los mecanismos de identificación y autenticación. Estos controles son principalmente organizativos y de gestión, y por su especial relevancia deben encontrarse expresamente recogidos en las políticas y normas de seguridad de la organización.

Los controles de acceso son importantes por dos motivos principales.

El primero motivo es que los usuarios son, probablemente, el vector de ataque[10] más importante de las amenazas existentes y su acceso y gestión deben encontrarse especialmente protegidos. Las amenazas sobre los usuarios pueden ser de naturaleza fortuita, por un uso inadecuado de sistemas o privilegios por parte de usuarios legítimos. O intencional, debido a amenazas externas que explotan la configuración inadecuada de los mecanismos de acceso, identificación y gestión de usuarios y privilegios de los sistemas.

El segundo motivo es el especial impacto de estos controles sobre los CPI. Los controles de acceso son condición indispensable para permitir el adecuado funcionamiento de CPI relevantes, como por ejemplo los controles de segregación de funciones.

[10] Ruta o método que utiliza un ciberdelincuente al intentar obtener acceso ilegítimo a un sistema de TI, siendo el usuario el receptor del ataque.

Ejemplos

Ejemplos de riesgos TI	Ejemplos de CGTI
Identificación y autenticación: El acceso a los sistemas no está adecuadamente restringido al personal autorizado para ello y no se puede mantener la trazabilidad de las acciones realizadas sobre la información financiera.	*Identificación* El acceso a los sistemas se realiza con un nombre de usuario unívoco, no compartido, lo que permite mantener la trazabilidad de las acciones realizadas por la persona responsable de dicha cuenta de usuario.
	Autenticación El acceso se autentica mediante contraseñas u otros métodos que garantizan que únicamente los usuarios autorizados pueden acceder. Los parámetros de las contraseñas cumplen los estándares de la entidad o del sector (por ejemplo, longitud y complejidad mínimas de la contraseña, periodo de validez, bloqueo de la cuenta).
Permisos de acceso excesivos: Los usuarios tienen permisos de acceso más allá de los necesarios para realizar sus tareas. Esto puede dar lugar a una incorrecta segregación de funciones.	*Asignación de permisos* y *autorización* La dirección aprueba la naturaleza y la extensión de los permisos de acceso de usuarios para nuevos usuarios o modificaciones de los permisos existentes, incluidos perfiles/funciones estándar por aplicaciones, transacciones críticas de información financiera y segregación de funciones.
	Eliminación de permisos El acceso para usuarios que dejan la entidad o son transferidos a otro departamento se elimina o modifica de manera oportuna.
	Revisiones de acceso de usuarios Se realizan revisiones periódicas que permiten comprobar si los permisos de acceso existentes están justificados y responden a las necesidades de la entidad.
	Segregación de funciones Se realiza un seguimiento de la segregación de funciones y los conflictos se eliminan o se asocian con controles mitigantes, los cuales se documentan y comprueban
	Acceso privilegiado El acceso privilegiado (por ejemplo, administradores de configuración, de datos y de seguridad) se autoriza y se restringe adecuadamente
Acceso directo a los datos: Se realizan directamente cambios inapropiados a los datos financieros por medios distintos a los de las transacciones de la aplicación.	*Asignación de permisos* y *autorización* El acceso a los archivos de datos o a los objetos/tablas/datos de las bases de datos se restringe al personal autorizado, en base a las responsabilidades de su puesto y a la función asignada, y dicho acceso es aprobado por la dirección.

Figura 13

Programa de auditoría del área

La revisión de esta área o categoría D está cubierta por la siguiente guía:

GPF-OCEX 5334 Controles de acceso a datos y programas

E. Continuidad del servicio

Por qué son importantes estos controles

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.

Ejemplos

Ejemplos de riesgos TI	Ejemplos de CGTI
Copias de seguridad de datos y recuperación: No se puede recuperar o acceder de modo oportuno a los datos financieros cuando se produce una pérdida de datos (frente a un ataque de *ransomware* o un incendio, por ejemplo).	*Copias de seguridad* Controles para asegurar que las copias de seguridad de los datos de información financiera se ejecutan de acuerdo con lo previsto.
	Copias de seguridad desconectadas y en ubicaciones diferentes Controles para asegurar que las copias de seguridad se preservan de aquellos riesgos que afectan a la información original.
	Pruebas de recuperación de las copias de seguridad realizadas Controles para asegurar que las copias de seguridad permiten recuperar la información en caso de ser necesario.

Figura 14

Programa de auditoría del área

La revisión de esta área o categoría E está cubierta por la siguiente guía:

GPF-OCEX 5335 Continuidad del servicio

15. Procedimientos de auditoría en fiscalizaciones financieras o de cumplimiento

El primer paso, en cualquier auditoría, es obtener un conocimiento adecuado de lo que se va a auditar, en particular del sistema de control interno, incluyendo el entorno de TI (ver apartado 3 y siguientes de esta guía).

Los procedimientos de auditoría a ejecutar para conocer el entorno tecnológico y los CGTI dependerán del tipo de auditoría que se vaya a realizar, de los objetivos de esta y de su alcance. Un resumen de estas cuestiones se incluirá en el Documento de inicio de la auditoría (DIA) y remitirá a la entidad. También podrá incluirse una primera solicitud de información.

Se mantendrá una reunión inicial con el responsable de sistemas y/o el coordinador de la fiscalización para, entre otras cuestiones:

- Informar sobre cuál es el objetivo general del trabajo, calendario e información que se les va a solicitar.
- Obtener información general sobre los sistemas de información de la entidad fiscalizada y de los CGTI.
- Ayudar a identificar la existencia de deficiencias en esos controles que puedan derivar en riesgos significativos de auditoría.

Para ello se cumplimentarán las tablas A y B que hay en el programa del anexo 2. Este trabajo se hará **en todas las fiscalizacione**s.

El equipo de auditoría debe garantizar la seguridad en el envío y recepción de la información del ente auditado ya que, en general, se trata de información confidencial que podría ser utilizada por personas mal intencionadas para vulnerar los sistemas de información auditados. Toda la información sensible en tránsito (ordenadores portátiles, lápices de memoria o a través de internet) deber estar cifrada.

En aquellas fiscalizaciones de seguridad razonable en entidades de **tamaño y complejidad media o alta**, además, se cumplimentarán las fichas de revisión de las GPF-OCEX 5331 a 5335, que se estructuran en las áreas vistas en el apartado 14. Estos programas de trabajo o fichas de revisión están diseñados para ayudar a:

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

Estas fichas/programas modelo deben adaptarse en cada caso a las características del ente auditado, de su entorno TI, y del objetivo y alcance de la auditoría, que como se ha visto en el apartado 2 pueden ser muy variables. La concreción del alcance de la revisión se realizará por el auditor financiero, de acuerdo con las necesidades de su auditoría, con la asistencia del auditor de sistemas de información.

Estos procedimientos son de ejecución necesaria en aquellas auditorías en las que se deba emitir una opinión de auditoría de seguridad razonable sobre las cuentas anuales o un componente significativo de las mismas o auditorías de cumplimiento, en entidades en las que su actividad se apoye en sistemas TI o bien en aquellas auditorías específicas de los CGTI.

Las fichas/programa han sido diseñadas para ser completados por personal con conocimientos sobre los CGTI. En general se realizará por un especialista en auditoría de sistemas de información.

Una vez cumplimentado el trabajo de revisión **se concluirá**:

- Formulando conclusiones generales sobre los controles revisados.
- Identificando y documentando las deficiencias de control detectadas.
- Identificando y documentando riesgos de incorrección material sobre los estados financieros.
- Formulando recomendaciones para la mejora de los CGTI.
- Determinando en su caso la necesidad de trabajo adicional.

La información obtenida, las evidencias y las conclusiones sobre las mismas se documentarán en el archivo de papeles de trabajo electrónicos creado para la fiscalización dentro de un área específica para la revisión de los CGTI.

En el Anexo 2 se adjunta un modelo de programa general para incluir en los programas de trabajo de todas las auditorías financieras.

16. Evaluación de las deficiencias de control interno detectadas

Todas las comprobaciones tienen por finalidad contrastar la situación real de los CGTI en la entidad con las buenas prácticas recogidas en las GPF-OCEX 5330 a 5335, en las que se especifican con el máximo detalle los aspectos a comprobar en cada control.

Los resultados del trabajo se analizarán y evaluarán a dos niveles: controles detallados y controles principales.

16.1 Evaluación de los controles detallados

Los CGTI principales de la figura 10 están compuestos por varios controles detallados, de los que se debe revisar su diseño e implementación y su eficacia operativa.

El trabajo de auditoría consistirá básicamente en evaluar cada uno de los controles detallados revisados en función de los resultados de las pruebas realizadas y las evidencias obtenidas.

Cada control detallado se evalúa según la escala mostrada en el siguiente cuadro:

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

Figura 15. Evaluación de los controles detallados

16.2 Nivel de madurez de los controles principales

Además, cada **control principal** (compuesto por varios controles detallados) se evaluará utilizando el modelo de **nivel de madurez**.

El modelo de nivel de madurez de los procesos de control está basado en el anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y en la *Guía de seguridad CCN-STIC 804* del CCN. Se utiliza la escala de la figura 16.

La evaluación sobre el nivel de madurez de los controles no debe basarse únicamente en los procesos teóricos o en los procedimientos formalmente aprobados, debe efectuarse tras la **verificación de su diseño, implementación** y **eficacia operativa.**

Para evaluar el nivel de madurez de cada control se tienen en cuenta los resultados obtenidos en la revisión de los controles detallados que lo forman y considerando la ponderación o importancia relativa que se les asigna para el cumplimiento del objetivo de control.

Este modelo proporciona una base sólida para formarse una idea general de la situación de los CGTI en la entidad revisada. También permite comparar resultados entre distintos entes y entre distintos momentos en el tiempo.

También se calculará el índice de madurez para cada categoría de CGTI.

Nivel	Índice	Descripción
N0 Inexistente	0-9	Esta medida/control no está siendo aplicada en este momento.
N1 Inicial / *ad hoc*	10-49	Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes. Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.
N2 Repetible, pero intuitivo	50-79	En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.
N3 Proceso definido	80-89	Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados. Los procedimientos se comunican con acciones formativas. *Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.* *Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.*
N4 Gestionado y medible	90-99	Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad. La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere.
N5 Optimizado	100	La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación. *El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.*

Figura 16. Niveles de madurez

16.3 Indicador global

A efectos del ENS, la guía CCN-STIC-824 contempla una serie de indicadores agregados capaces de aportar información resumida sobre el estado de la seguridad en los organismos públicos. En particular el **índice de madurez general** sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de controles de ciberseguridad.

17. Importancia relativa de las deficiencias de control a efectos de la auditoría

Al evaluar las deficiencias de control interno detectadas se debe considerar la significatividad de estas. En este contexto el concepto "significativo" no puede ser definido de forma exacta, ya que una misma cuestión puede ser significativa, o no, dependiendo de los objetivos de la auditoría y de las circunstancias. *(GPF-OCEX 1735; P11)*

Las deficiencias de control interno se clasifican en tres niveles de importancia relativa, que vienen definidos en la GPF-OCEX 1265 (apartado 6):

- Deficiencia de control interno
- Deficiencia significativa de control
- Debilidad material

Para evaluar la importancia relativa o significatividad de las deficiencias de control interno se tendrán en consideración los criterios señalados en el apartado 8 de la **GPF-OCEX 1265**, que debe leerse con carácter previo a la presente guía y damos por reproducido.

Si las deficiencias de control constituyen debilidades materiales, el auditor concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoría, es decir, la combinación adecuada de pruebas de cumplimiento y de pruebas sustantivas, dando mayor énfasis a estas últimas para intentar minimizar el riesgo final de auditoría.

La evaluación de la importancia relativa o significatividad de las deficiencias incluye consideraciones sobre los siguientes factores de carácter general: *(GPF-OCEX 1735; P12)*

a) La **magnitud del impacto** se refiere al efecto probable que la deficiencia pudiera tener en el logro de los objetivos de la entidad y se ve afectado por factores como el tamaño, el ritmo y la duración del impacto de la deficiencia. Una deficiencia puede ser más significativa para un objetivo que para otro.

b) La **probabilidad de ocurrencia** se refiere a la posibilidad de que una deficiencia afecte a la capacidad de una entidad para alcanzar sus objetivos.

c) La **naturaleza de la deficiencia** implica factores tales como el grado de subjetividad implicado con la deficiencia y si la deficiencia surge del fraude o de una conducta indebida.

Al evaluar las deficiencias de un CGTI para determinar si una deficiencia de control, individualmente o junto con otras, constituye una deficiencia significativa o una debilidad material, el auditor puede considerar, entre otros, los siguientes factores:

- Perjudica o puede perjudicar el cumplimiento de los objetivos de la entidad.
- Ocasiona un aumento significativo del riesgo de auditoría.
- La probabilidad de que una persona pueda obtener acceso no autorizado o ejecutar actividades no autorizadas o inapropiadas en sistemas críticos de la entidad o archivos que puedan afectar a la información con impacto en las cuentas anuales. Esto puede incluir:

  a) la habilidad para tener acceso a sistemas en los que residen aplicaciones críticas y que posibilita a usuarios no autorizados a leer, añadir, borrar, modificar o extraer información financiera, bien directamente o a través de la utilización de software no autorizado;

  b) la habilidad para acceder directamente y modificar ficheros que contengan información financiera; o

  c) la habilidad para asignar derechos de acceso a las aplicaciones a usuarios no autorizados, con la finalidad de procesar transacciones no autorizadas.
- La naturaleza de los accesos no autorizados que pueden conseguirse (por ejemplo: limitados a programadores del sistema o de las aplicaciones o a administradores del sistema; a todos los usuarios; a alguien externo a través de acceso no autorizados por Internet) o la naturaleza de las actividades no autorizadas o inadecuadas que pueden llevarse a cabo.
- La probabilidad de que importes de las cuentas anuales estén afectados de forma significativa.
- La probabilidad de que otros controles puedan prevenir o detectar accesos no autorizados.
- El riesgo de que la dirección de la entidad pueda burlar los controles (por ejemplo, mediante derechos de acceso excesivos).
- **Efecto en los CPI**

  La importancia de una deficiencia en un CGTI debe ser evaluada en relación con su efecto en los CPI, es decir, si provoca que los CPI sean ineficaces. Si la deficiencia de la aplicación es provocada por el CGTI ambas deficiencias deben ser consideradas de la misma forma (como deficiencias significativas o como debilidades materiales).

- **Efecto en el entorno de control**

  Después de que una deficiencia de un CGTI haya sido evaluada en relación con los CPI, también debe ser evaluada considerando el conjunto de las deficiencias de control y su efecto agregado.

Por ejemplo, *debe considerarse la decisión de la gerencia de no subsanar una deficiencia de CGTI y reflexionar sobre su relación con el entorno de control; al considerarla agregada a otras deficiencias que afectan al entorno de control puede llevar a la conclusión de que existe una debilidad material o una deficiencia significativa en el entorno de control.*

- **Análisis del efecto agregado de las deficiencias de control**

  Algunas deficiencias de control pueden ser consideradas no significativas individualmente, pero consideradas junto con otras deficiencias similares, el efecto combinado puede ser más significativo.

  Por ejemplo*, en una entidad que no realiza revisiones periódicas de las listas de usuarios con acceso a su aplicación de contabilidad se considerará que tiene una deficiencia en el diseño de un control. Por un lado, puede que no se considere significativa, especialmente si existen controles compensatorios. Pero si se ha detectado que el procedimiento de autorización de nuevos usuarios a esa aplicación es inadecuado, entonces el efecto agregado de las dos deficiencias puede resultar en una deficiencia significativa o en una debilidad material. Es decir, el efecto combinado de las deficiencias de control relacionadas con las solicitudes de nuevos accesos y las revisiones de los derechos de acceso en una aplicación contable cuestiona la validez de los permisos de acceso en esa aplicación y en consecuencia plantea dudas sobre la validez de las transacciones dentro del sistema de información.*

Basándose en las consideraciones reseñadas el auditor determinará si las deficiencias de control son, individualmente o en conjunto, debilidades materiales o deficiencias significativas.

Se considerará que tienen un impacto significativo aquellas deficiencias de control que potencialmente podrían permitir un incidente de seguridad clasificado en los niveles “Alto”, “Muy alto” y “Crítico” de los recogidos en la tabla de “Criterios de determinación del nivel de impacto de los ciberincidentes” de la guía CCN-STIC 817.

Si las deficiencias de control constituyen debilidades materiales, el auditor concluirá que los CGTI no son eficaces y deberá replantearse su estrategia de auditoría, pudiendo omitir la revisión de los CPI puesto que no van a ser eficaces, dando mayor énfasis a los procedimientos sustantivos, de forma que se intentará minimizar el riesgo final de auditoría.

Las debilidades materiales deben ser incluidas en el informe de auditoría como una salvedad o como una conclusión, según el tipo de informe.

18. Recomendaciones

Si se efectúan **recomendaciones**, existirá una relación directa entre el tipo de deficiencia de control (según su importancia relativa), el riesgo de auditoría que representa, y la prioridad que se conceda a cada recomendación. La prioridad también estará matizada por consideraciones coste/beneficio.

En el cuadro siguiente se resume la relación existente entre los tres tipos de deficiencias de control según su significatividad o importancia relativa, el riesgo que representan y la prioridad de las recomendaciones correspondientes: *(GPF-OCEX 1735)*

Tipo de deficiencia según su importancia relativa	Riesgo	Prioridad de una recomendación	
Debilidad material	**Alto**	**Alta**	**Se requiere atención urgente de la dirección para implantar controles/procedimientos que mitiguen los riesgos identificados.**
Deficiencia significativa	**Medio**	**Media**	**La dirección debería establecer un plan de acción concreto para resolver la deficiencia observada en un plazo razonable.**
Deficiencia de control interno	**Bajo**	**Baja**	

Figura 17

Los hallazgos de auditoría que las soportan deberán documentarse en los papeles de trabajo e incluir: *(GPF-OCEX 1735; P9)*

Criterio (de auditoría)

Hecho o condición

Causa

Efecto

Recomendación

Para elaborar las recomendaciones a realizar se tendrán en consideración los criterios señalados en la **GPF-OCEX 1735**, que debe leerse con carácter previo a la presente guía que damos por conocidos.

19. Documentación del trabajo

El trabajo de auditoría de los CGTI se documentará cumplimentando los programas y fichas de revisión de las guías GPF-OCEX 5331 a 5335 y 5314.

En cada auditoría se explicará en la memoria de planificación el alcance de la revisión, los controles seleccionados y las razones para ello en función de las circunstancias y objetivos de la auditoría.

Anexo 1 Consideraciones para el conocimiento de la utilización de TI por la entidad

(Anexo 5 de la NIA-ES 315 Revisada)

En este anexo se proporcionan cuestiones adicionales que el auditor puede considerar para el conocimiento de la utilización de las TI en un sistema de control interno.

El sistema de control interno de la entidad puede incluir la utilización de elementos manuales y automatizados que afectan al modo en que se inician, registran y procesan las transacciones y se informa sobre ellas.

En la obtención de conocimiento del entorno de TI relevante para los flujos de transacciones y el procesamiento de la información en el sistema de información, el auditor obtiene información acerca de la naturaleza y las características de las aplicaciones de TI que se utilizan, así como acerca de la infraestructura de TI en las que se sustentan. Para sintetizar esta información se podrá utilizar, por ejemplo, la tabla A siguiente.

El siguiente cuadro incluye ejemplos de cuestiones que el auditor puede considerar en la obtención de conocimiento del entorno de TI e incluye ejemplos de características habituales de entornos de TI basadas en la complejidad de las aplicaciones de TI utilizadas en el sistema de información de la entidad. No obstante, dichas características son indicativas y pueden diferir dependiendo de la naturaleza de las aplicaciones específicas de TI utilizadas por la entidad.

	Ejemplos de características habituales de:		
	Software comercial no complejo	**Software comercial o aplicaciones de TI de tamaño medio y moderadamente complejos**	**Aplicaciones grandes o complejas (por ejemplo, sistemas de planificación de recursos (ERP))**
Cuestiones relacionadas con el grado de automatización y la utilización de datos:			
Extensión de los procedimientos automatizados para el procesamiento y su complejidad, incluido, si existe procesamiento altamente automatizado, sin soporte papel.	N/A	N/A	Procedimientos automatizados extensos y a menudo complejos
Grado en que la entidad confía en informes generados por el sistema en el procesamiento de la información.	Lógica para la generación automatizada de información sencilla	Lógica para la generación automatizada de informes relevantes sencilla	Lógica para la generación automatizada de informes compleja; Software de redacción de informes
Forma en que se introducen los datos (es decir, introducción manual, introducción por el cliente o por el proveedor, descarga de archivos)	Introducción manual de datos	Número reducido de introducciones de datos o comunicaciones automatizadas sencillas	Elevado número de introducciones de datos o comunicaciones automatizadas complejas
Modo en que las TI facilitan las comunicaciones entre aplicaciones, bases de datos u otros aspectos del entorno de TI, interna y externamente, según corresponda, mediante comunicaciones automatizadas entre sistemas.	No existen comunicaciones automatizadas (solo introducciones manuales)	Número reducido de introducciones de datos o comunicaciones automatizadas sencillas	Elevado número de introducciones de datos o comunicaciones automatizadas complejas
El volumen y la complejidad de datos en formato digital que son procesados por el sistema de información, incluido si los registros contables u otra información se almacenan en formato digital y la ubicación de los datos almacenados.	Volumen de datos reducido o datos sencillos que se pueden verificar manualmente; datos disponibles localmente	Volumen de datos reducido o datos sencillos	Gran volumen de datos o datos complejos; almacenes de datos;[11] utilización de proveedores de servicios de TI (p.e, almacenamiento por terceros o alojamiento de datos)

[11] Un almacén de datos (Data Warehouse) se describe, por lo general, como un depósito central de datos integrados procedentes de una o varias fuentes (tal como múltiples bases de datos) a partir de los que se pueden generar informes o que pueden ser utilizados por la entidad para otras actividades de análisis de datos. Un redactor de informes es una aplicación de TI que se utiliza para extraerdatos de una o de varias fuentes (como de un almacén de datos, de una base de datos o de una aplicación de TI) y presentar los datos en un formato determinado.

	Ejemplos de características habituales de:		
	Software comercial no complejo	**Software comercial o aplicaciones de TI de tamaño medio y moderadamente complejos**	**Aplicaciones grandes o complejas (por ejemplo, sistemas de planificación de recursos (ERP))**
Cuestiones relacionadas con las aplicaciones y con la infraestructura de TI:			
El tipo de aplicación	Aplicación adquirida poco o nada personalizada	Aplicación adquirida o aplicaciones ERP sencillas heredadas o de gama baja poco o nada personalizadas	Aplicaciones a medida o ERP más complejas significativamente personalizadas o altamente integradas que pueden haber sido adquiridas y personalizadas o desarrolladas internamente
La complejidad de la naturaleza de las aplicaciones de TI y la infraestructura de TI subyacente.	Soluciones pequeñas, para ordenador portátil o basadas en una arquitectura cliente servidor	Ordenador central maduro y estable, arquitectura cliente-servidor pequeña o sencilla, software en la **nube**	Ordenador central complejo, arquitectura cliente- servidor de gran dimensión o compleja, orientado a la web, infraestructura de servicios en la **nube**
Si se acude a un tercero para el alojamiento o si se subcontratan las TI	Si las TI se subcontratan, proveedor de servicios competente, maduro y probado (p.e., proveedor de servicios en la **nube**)	Si las TI se subcontratan, proveedor de servicios competente, maduro y probado (por ejemplo, proveedor de servicios en la **nube**)	Proveedor de servicios competente, maduro y probado para determinadas aplicaciones y proveedor nuevo o emergente para otras
Si la entidad está utilizando tecnologías emergentes que afectan a su información financiera	No se utilizan tecnologías emergentes	Se utilizan tecnologías emergentes de modo limitado en algunas aplicaciones	Utilización mixta de tecnologías emergentes entre plataformas
Cuestiones relacionadas con los procesos de TI:			
El personal que participa en el mantenimiento del entorno de TI (número y grado de cualificación de los recursos de soporte a las TI que gestionan la seguridad y los cambios al entorno de las TI).	Poco personal, con conocimientos limitados de TI para procesar las actualizaciones del proveedor y gestionar el acceso	Número limitado de personas con cualificaciones en TI/dedicado a las TI	Departamentos destinados a TI con personal cualificado, incluidas habilidades de programación
La complejidad de los procesos para gestionar los derechos de acceso.	Una sola persona con acceso administrativo gestiona los derechos de acceso	Pocas personas con acceso administrativo gestionan los derechos de acceso	Procesos complejos gestionados por el departamento de TI para los derechos de acceso
La complejidad de la seguridad sobre el entorno de las TI, incluida la vulnerabilidad de las aplicaciones de TI, bases de datos y otros aspectos del entorno de TI a los riesgos informáticos, especialmente cuando existen transacciones por la web o transacciones en las que intervienen comunicaciones (interfaces) automatizadas externas.	Acceso sencillo en las propias oficinas sin elementos orientados a la web externos	Algunas aplicaciones basadas en la web con una seguridad principalmente sencilla, basada en funciones	Numerosas plataformas con acceso basado en la web y modelos de seguridad complejos
Si se han realizado cambios en los programas relativos al modo en que se procesa la información y la extensión de dichos cambios durante el periodo	Software comercial sin ningún código fuente instalado	Algunas aplicaciones comerciales sin código fuente y otras aplicaciones maduras con un número reducido de cambios o con cambios sencillos; desarrollo de sistemas tradicionales a lo largo de su vida útil	Cambios nuevos, numerosos o complejos, varios ciclos de desarrollo cada año
La extensión del cambio en el entorno de TI (p.e., nuevos aspectos del entorno de TI o cambios significativos en las aplicaciones de TI o en la infraestructura de TI subyacente).	Cambios limitados a actualizaciones de versiones de software comercial	Los cambios consisten en actualizaciones de versiones de software comercial, o mejoras en sistemas heredados	Cambios nuevos, numerosos o complejos, varios ciclos de desarrollo cada año, importante personalización de ERP

	Ejemplos de características habituales de:		
	Software comercial no complejo	**Software comercial o aplicaciones de TI de tamaño medio y moderadamente complejos**	**Aplicaciones grandes o complejas (por ejemplo, sistemas de planificación de recursos (ERP))**
Si se ha realizado una importante conversión de datos durante el periodo y, en su caso, la naturaleza y significatividad de los cambios realizados, y el modo se ha efectuado la conversión.	Actualizaciones de software proporcionadas por el proveedor; La actualización no cuenta con posibilidades de conversión de datos	Actualizaciones menores para aplicaciones de software comercial con una conversión limitada de datos	Actualización importante de la versión, nuevo lanzamiento, cambio de plataforma

Graduación

La capacidad de la entidad para mantener la integridad de la información almacenada y procesada en el sistema de información puede variar en función de la complejidad y del volumen de las correspondientes transacciones y demás información.

Cuanto mayor sea la complejidad y el volumen de datos que sustenta un tipo de transacciones, saldo contable o información a revelar significativos, menos probable será que la entidad mantenga la integridad de esa información sólo a través de controles de procesamiento de la información (por ejemplo, controles de entradas y salidas o controles de revisión). También se vuelve menos probable que el auditor pueda obtener evidencia de auditoría sobre la completitud y exactitud de esa información sólo a través de procedimientos sustantivos cuando se utiliza como evidencia de auditoría. En algunas circunstancias, cuando es menor el volumen y la complejidad de las transacciones, es posible que la dirección disponga de un control de procesamiento de la información suficiente para verificar la exactitud y completitud de los datos (por ejemplo, se pueden conciliar órdenes de venta individuales procesadas y facturadas con la copia impresa introducida originariamente en la aplicación de TI). Cuando la entidad confía en CGTI para mantener la integridad de cierta información utilizada por las aplicaciones de TI, el auditor puede determinar que las aplicaciones de TI que mantienen esa integridad están sujetas a riesgos derivados de la utilización de TI.

Ejemplos de características de una aplicación de TI que probablemente no esté sujeta a riesgos derivados de la utilización de TI	**Ejemplos de características de una aplicación de TI que probablemente esté sujeta a riesgos derivados de la utilización de TI**
• Aplicaciones independientes. • El volumen de datos (transacciones) no es significativo. • La funcionalidad de la aplicación no es compleja. • Cada transacción está soportada por documentación impresa original.	• Las aplicaciones están intercomunicadas. • El volumen de datos (transacciones) es significativo. • La funcionalidad de la aplicación es compleja porque: – la aplicación inicia automáticamente las transacciones y – hay una gran variedad de cálculos complejos que subyacen a las entradas automatizadas.
Es probable que la aplicación de TI no esté sujeta a riesgos derivados de la utilización de TI porque: • El volumen de datos no es significativo y, en consecuencia, la dirección no confía en CGTI para procesar o mantener los datos. • La dirección no confía en controles automatizados o en otra funcionalidad automatizada. El auditor no ha identificado controles automatizados de conformidad con el apartado 26(a). • Aunque la dirección utiliza informes generados por el sistema en sus controles, no confía en esos informes. Por el contrario, concilia los informes con la documentación impresa y verifica los cálculos incluidos en los informes. • El auditor comprobará directamente la información, producida por la entidad, que vaya a ser utilizada como evidencia de auditoría.	La aplicación de TI está sujeta a riesgos derivados de la utilización de TI porque: • La dirección confía en un sistema de aplicaciones para el procesamiento o el mantenimiento de los datos porque el volumen de datos es significativo. • La dirección confía en el sistema de aplicaciones para ejecutar ciertos controles automatizados que el auditor también ha identificado.

Anexo 2-Programa de auditoría financiera para la revisión de los CGTI

1. Análisis de las cuentas anuales

Información complementaria: *Ver GPF-OCEX-1315*

Trabajo a realizar*:*

1. Identificar los epígrafes del balance, de la cuenta de resultados y/o del presupuesto sobre los que focalizar el esfuerzo de la auditoría.
2. Hacer una **revisión analítica** de las cuentas del ejercicio fiscalizado comparándolas con las del ejercicio anterior y analizar las desviaciones más significativas. Las desviaciones analizadas se referenciarán al trabajo efectuado en el área correspondiente.
3. Identificar los TTSCIR materiales.
4. Identificar los procesos de gestión significativos.

2. Identificación y valoración de los RIM

Información complementaria: *Ver GPF-OCEX 5340 y GPF-OCEX 1513 Cómo realizar y documentar la reunión del equipo de auditoría para discutir sobre los RIM*

Trabajo a realizar*:*

5. Seguir los procedimientos descritos en GPF-OCEX 5340 para identificar los riesgos significativos.
6. Debe celebrarse una reunión del equipo de auditoría para discutir sobre los riesgos de auditoría previsibles y documentarla de acuerdo con la *GPF-OCEX 1513*.

3. Revisión de los Controles Generales de TI (CGTI) –Nivel básico

(Este trabajo se realizará en todas las auditorías)
Información complementaria: *Ver GPF-OCEX 5331 y 5314*

Trabajo a realizar*:*

7. Mantener una reunión con el auditor de sistemas para abordar el análisis de los controles generales de la entidad y planificar, en su caso, su colaboración.
8. Mantener una reunión con el coordinador y con el responsable de sistemas de la entidad para explicar el objetivo de nuestra revisión y la petición que se les va a realizar.

   Deben cumplimentar las tablas A y B adjuntas. Se les explicará su contenido.

   Esta entrevista la mantendrá el auditor financiero solo o con la asistencia del auditor de sistemas. Se comentará, en su caso, el trabajo a realizar de acuerdo con el apartado 4 del programa.
9. En caso de que la entidad haya sido fiscalizada en el ejercicio anterior, actualizar con el responsable de sistemas los datos correspondientes de la tabla A.
10. Recibidos los cuestionarios cumplimentados (tablas A y B), el equipo de auditoría analizará la información contenida en los mismos, indicando en un p/t las conclusiones para comentarlas oportunamente con el auditor de sistemas.
11. El auditor considerará si es necesaria o no la intervención de personal especializado para completar el análisis y/o realizar actividades adicionales

4. Revisión de los Controles Generales de TI (CGTI) –Nivel general

(Este trabajo solo se realizará cuando se haya establecido así en la memoria de planificación)
Información complementaria: *Ver GPF-OCEX 5330 a GPF-OCEX 5335*

Trabajo a realizar*:*

12. Revisar la valoración del riesgo realizada según GPF-OCEX 5340 y las observaciones surgidas tras analizar las tablas A y B.
13. Mantener una reunión con el auditor de sistemas para analizar la información obtenida, determinar y programar el trabajo requerido sobre los CGTI. El auditor de sistemas seleccionará el trabajo a realizar de las GPF-OCEX 5331 a 5335.
14. Entregar el cuestionario seleccionado de GPF-OCEX 5331 a 5335 al responsable del departamento de sistemas de información de la entidad auditada, con copia al coordinador, para que lo completen con la información solicitada y lo devuelvan firmado en soporte informático mediante procedimiento cifrado.
15. Identificar los riesgos TI significativos y los CGTI relevantes y diseñar pruebas sobre el D+I que van a realizarse en colaboración con el auditor de sistemas.
16. El auditor de sistemas realizará las pruebas de eficacia operativa de los CGTI.
17. Comentar las conclusiones y recomendaciones preliminares con el responsable de sistemas y de seguridad de la entidad
18. Concluir sobre la eficacia operativa de los CGTI para respaldar el adecuado funcionamiento de los CPI y la adecuación de la estrategia prevista de auditoría en cuanto a procedimientos sustantivos y alcance.
19. Formular las recomendaciones definitivas.

Tabla A para documentar el conocimiento del entorno TI

ENTORNO TI DE: _____*Entidad*_____

FECHA: xx/xx/xx

Cuentas anuales		**Aplicaciones (1)**					**Bases de datos**		**Sistemas operativos**		**Plataforma hardware**	**Observaciones**
Epígrafe	Importe gestionado 2024 (euros)	Proceso	Aplicación utilizada	Tipo de aplicación **(2)**	Puesto y nombre de los responsables funcional/técnico	Control acceso (SO/aplicación) **(3)**	Marca y versión	Administrador	Marca y Versión	Puesto y nombre del responsable	Identificación marca. Denominación de los servidores	
Contabilidad												
Personal												
Compras-contratación												
Tributos												
Subvenciones												
Añadir si existen otras aplicaciones relevantes para la gestión económica de la entidad												

(1) Si alguno de estos procesos/aplicaciones es mantenido por un proveedor de servicios externo, indicarlo en el apartado de observaciones, señalando el nombre del proveedor y la fecha del contrato.

(2) Adquirida o de desarrollo propio.

(3) Entorno que ofrece el control en el acceso lógico a la aplicación: delegada en el sistema operativo (SO) u otro sistema o de la propia aplicación.

Nota: En el caso de aplicaciones que soportan procesos que se van a auditar, adjuntar el modelo de datos de la base de datos o la documentación existente sobre el modelo de datos, los manuales de usuario de la aplicación y los informes de auditoría de sistemas de información sobre la aplicación realizados en el último año. Solo se aportará la información que se disponga, no es necesario elaborar documentación ad hoc. Si no se dispone de documentación, señalarlo.

Tabla B para la revisión preliminar de los CGTI en una auditoría financiera

Subcontrol	Referencia	Objetivo de control	Cumplimiento	Observaciones/Plan de acción
A. Gobernanza				
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un plan estratégico de TI	a) Sí b) Parcial c) No	
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un comité de gobierno de las TI con un funcionamiento efectivo.	a) Sí b) Parcial c) No	
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un sistema de gestión de riesgos de TI.	a) Sí b) Parcial c) No	
Cumplimiento normativo	GPF-OCEX 5331	Se dispone de la certificación de cumplimiento del ENS o del plan de adecuación correspondiente.	a) Sí b) Parcial c) No	
Cumplimiento normativo	GPF-OCEX 5331	Se ha nombrado un DPD.	a) Sí b) Parcial c) No	
Cumplimiento normativo	GPF-OCEX 5331	Se dispone de un plan de adecuación al ENI.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un plan estratégico de ciberseguridad o de seguridad de la información.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de una Política de Seguridad de la Información (PSI) formalmente aprobada.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un comité de seguridad de la información, formalmente aprobado y con un funcionamiento efectivo.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un sistema de gestión de riesgos de seguridad de la información.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se ha nombrado un responsable de seguridad.	a) Sí b) Parcial c) No	

Subcontrol	Referencia	Objetivo de control	Cumplimiento	Observaciones/Plan de acción
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Existe un plan de concienciación y de formación en ciberseguridad.	a) Sí b) Parcial c) No	
Gobernanza de la ciberseguridad	GPF-OCEX 5314	El personal y los recursos económicos asignados a las TI y a la seguridad de la información se considera adecuado.	a) Sí b) Parcial c) No	
B. Gestión de cambios en aplicaciones y sistemas				
Procedimientos para la gestión de cambios	GPF-OCEX 5332: B.3.1	La entidad dispone de un procedimiento para la gestión de los cambios en los sistemas y aplicaciones y en sus configuraciones.	a) Sí b) Parcial c) No	
Responsabilidades para la gestión de cambios de aplicaciones o sistemas	GPF-OCEX 5332: B.3.2	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.)	a) Sí b) Parcial c) No	
Entornos para pruebas separados de producción	GPF-OCEX 5332: B.3.3	Se han separado el entorno de desarrollo del de producción, realizándose el desarrollo sobre sistemas diferenciados de los productivos.	a) Sí b) Parcial c) No	
Segregación de funciones	GPF-OCEX 5332: B.3.5	Se segregan aquellas funciones que, ante determinadas circunstancias, podrían culminar en conflicto de interés como, por ejemplo, desarrollo y operación. Se evita, siempre que sea posible, que las capacidades de desarrollo y operación recaigan en la misma persona o en el mismo equipo	a) Sí b) Parcial c) No	
Pruebas de aceptación	GPF-OCEX 5332: B.3.6	Una vez implementados cambios en aplicaciones y sistemas, se realizan las pruebas de aceptación convenientes.	a) Sí b) Parcial c) No	
C. Operaciones de los sistemas de información				
Inventario de activos HW	GPF-OCEX 5333: C.1.1	Se dispone de un inventario de activos hardware actualizado. Es admisible el concepto de inventario federado, que consiste en la suma de varios inventarios independientes que en su conjunto constituyen el inventario completo.	a) Sí b) Parcial c) No	
Inventario de activos SW	GPF-OCEX 5333: C.1.2	Se dispone de un inventario actualizado de todos los activos software del sistema, incluyendo software de endpoint, software de servidores, y software proporcionado por terceros.	a) Sí b) Parcial c) No	
Control de SW no autorizados	GPF-OCEX 5333: C.1.4	Se dispone de una lista de software autorizado y de medidas que permitan detectar el uso de software no autorizado.	a) Sí b) Parcial c) No	
Gestión de vulnerabilidades	GPF-OCEX 5333: C.2.1	Se dispone de procesos para identificar, analizar y priorizar la resolución de las vulnerabilidades.	a) Sí b) Parcial c) No	

Subcontrol	Referencia	Objetivo de control	Cumplimiento	Observaciones/Plan de acción
Software soportado por el fabricante	GPF-OCEX 5333: C.2.3	Se dispone de un plan de mantenimiento del software y se controlan las fechas de fin de soporte del software.	a) Sí b) Parcial c) No	
Configuración de seguridad	GPF-OCEX 5333: C.3.1	Se realiza una configuración de seguridad (bastionado) a los equipos, previamente a su puesta en producción.	a) Sí b) Parcial c) No	
Activación de logs de auditoría	GPF-OCEX 5333: C.4.1	Se registran los eventos y actividades de usuarios y entidades que acceden a los sistemas.	a) Sí b) Parcial c) No	
Centralización y revisión de logs	GPF-OCEX 5333: C.4.4	Se realizan revisiones de los logs y se dispone de herramientas para apoyar la revisión.	a) Sí b) Parcial c) No	
Requisitos de seguridad de los servicios externos	GPF-OCEX 5333: C.5.2	Se han establecido contractualmente los requisitos de seguridad que deben cumplir los proveedores de servicio, como el certificado de conformidad respecto al ENS.	a) Sí b) Parcial c) No	
Áreas separadas con control de acceso	GPF-OCEX 5333: C.7.1	Las instalaciones de los CPD están dotadas de adecuadas medidas de seguridad.	a) Sí b) Parcial c) No	
Procedimiento, notificación, detección y respuesta de incidentes	GPF-OCEX 5333: C.8.1	Se dispone de un proceso integral para tratar los incidentes que puedan tener un impacto en la seguridad del sistema.	a) Sí b) Parcial c) No	
Segmentación de Redes	GPF-OCEX 5333: C.10.4	Se ha segmentado la red, segregando el tráfico de modo que cada grupo de usuarios únicamente tenga acceso a la información que necesita. Los segmentos de red se han implementado por medio de redes de área local virtuales (VLANs), redes privadas virtuales (VPNs), o con medios físicos separados	a) Sí b) Parcial c) No	
D. Controles de acceso a datos y programas				
Inventario y control de cuentas de administración	GPF-OCEX 5334: D.1.1	Está adecuadamente controlada la asignación del privilegio de administración.	a) Sí b) Parcial c) No	
Uso dedicado de cuentas de administración	GPF-OCEX 5334: D.1.2	Cuando el usuario tiene diferentes roles frente al sistema (por ejemplo, usuario y administrador) se le asignan identificadores singulares para cada perfil.	a) Sí b) Parcial c) No	
Procedimiento de gestión de usuarios	GPF-OCEX 5334: D.2.1	La entidad dispone de un proceso formalmente establecido de solicitud y alta de nuevos usuarios en los sistemas. La entidad dispone de un proceso formalmente establecido para la gestión de las bajas de cuentas de usuarios en el sistema que garantice que no existen cuentas no necesarias.	a) Sí b) Parcial c) No	

Subcontrol	Referencia	Objetivo de control	Cumplimiento	Observaciones/Plan de acción
Identificación	GPF-OCEX 5334: D.2.2	Cada entidad (usuario o proceso) que accede al sistema cuenta con un identificador singular que permite reconocerlo y asignarle los derechos de acceso que le corresponden.	a) Sí b) Parcial c) No	
Mecanismos de autenticación	GPF-OCEX 5334: D.2.3	La política de autenticación se considera robusta y adecuada para reducir el riesgo de accesos no autorizados. *Posibles mecanismos de autenticación contemplados en el ENS son: contraseñas, certificados y certificados cualificados. Una medida que incrementa su robustez es el doble factor de autenticación.*	a) Sí b) Parcial c) No	
Gestión de derechos de acceso	GPF-OCEX 5334: D.2.5	Los derechos de acceso de cada recurso TI se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema. Se gestionan los derechos de acceso en base al principio de mínimo privilegio.	a) Sí b) Parcial c) No	
E. Continuidad del servicio				
Realización de copias de seguridad	GPF-OCEX 5335: E.1.1	Se realizan copias de seguridad que permitan recuperar los datos perdidos accidental o intencionadamente.	a) Sí b) Parcial c) No	
Realización de pruebas de recuperación	GPF-OCEX 5335: E.1.2	La organización ha establecido y aprobado procedimientos formales de restauración de datos y sistemas desde las copias de seguridad. Las pruebas de recuperación de copias se realizan regularmente, con una periodicidad dependiente de la criticidad de los datos y del impacto que causaría la falta de disponibilidad.	a) Sí b) Parcial c) No	
Protección de las copias de seguridad	GPF-OCEX 5335: E.1.3	Las copias de seguridad se preservan de aquellos riesgos que también podrían afectar a la información original. Por ejemplo copias en distintas ubicaciones y copias desconectadas.	a) Sí b) Parcial c) No	
Identificación de elementos críticos del negocio	GPF-OCEX 5335: E.2.1	Se ha realizado un análisis de impacto (BIA) en los servicios en el ámbito del ENS.	a) Sí b) Parcial c) No	
Plan de recuperación de desastres (DRP)	GPF-OCEX 5335: E.2.2	Existen definidos planes de emergencia, contingencia o recuperación, en consonancia con el Plan de Continuidad general.	a) Sí b) Parcial c) No	
Plan de continuidad	GPF-OCEX 5335: E.2.3	Se dispone de un Plan de Continuidad documentado, coherente con los resultados del BIA.	a) Sí b) Parcial c) No	