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

Referencia: ISSAI 5300, GPF-OCEX 5300, GPF-OCEX 1315 y GPF-OCEX 1316

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 12/11/2018

1. Introducción

El enfoque de auditoría basado en el análisis del riesgo es el fundamento central de la actividad auditora desarrollada bajo las Normas Internacionales de Auditoría (NIA-ES) y las ISSAI-ES. Tal como señala la GPF-OCEX 1315, "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 la mayor 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."

Actualmente, en una auditoría financiera basada en el análisis de los riesgos realizada de acuerdo con la ISSAI-ES 200, el estudio y revisión de los sistemas de información en los que se sustenta la gestión de una entidad (empresa o fundación pública, ayuntamiento, administración de la comunidad autónoma, etc.) se ha convertido en una actividad de importancia creciente, 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) que deben ser considerados en la estrategia de auditoría.

Para orientar y facilitar a los auditores de los OCEX la aplicación del enfoque de riesgo y la auditoría en entornos de administración electrónica se han desarrollado las Guías Prácticas de Fiscalización (GPF-OCEX).

De acuerdo con las ISSAI-ES/NIA-ES, una vez adquirido un conocimiento general de la entidad, incluyendo sus sistemas de información y de control interno, y antes de iniciar la revisión de los procesos y aplicaciones de gestión significativos a los efectos de la auditoría financiera y de sus controles, se debe revisar la situación de los controles generales, ya que el grado de confianza en los mismos determinará la posterior estrategia de auditoría.

En un entorno informatizado de complejidad media o alta, la revisión de los controles generales de tecnologías de la información (CGTI) requerirá, normalmente, la colaboración de un experto en auditoría de sistemas de información y la aplicación de una metodología específica. En estas circunstancias la revisión de los CGTI (y de los controles de aplicación) es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.

Muy esquemáticamente, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son (ver GPF-OCEX 1315) las que se muestran en la figura 1.

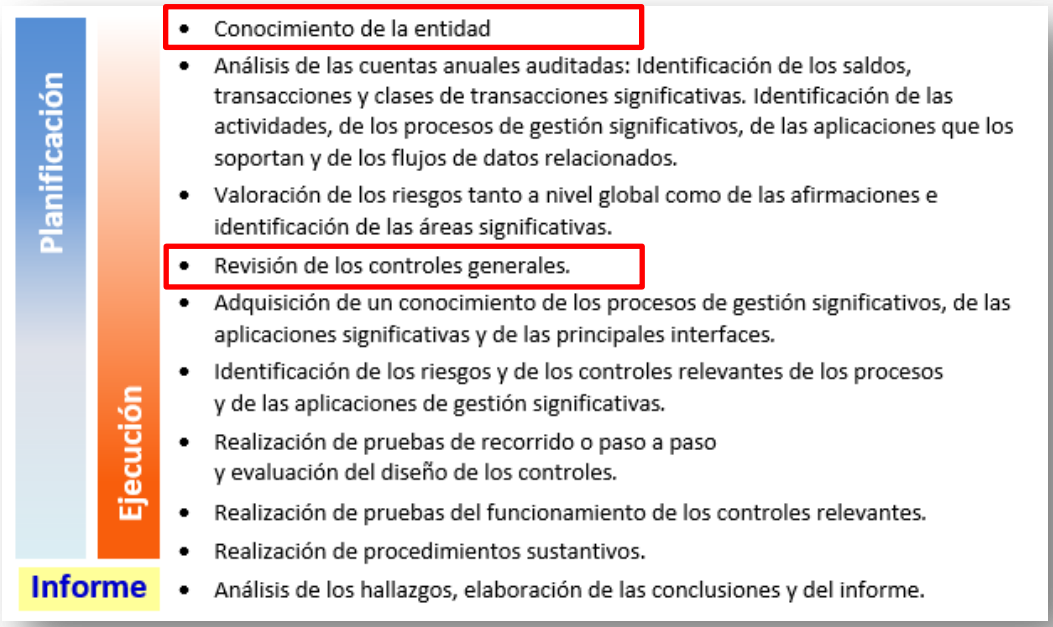

Figura 1

En el Anexo 4 de la GPF-OCEX 1315 puede verse un flujograma de la actividad típica en una auditoría financiera.

Las normas reguladoras de la auditoría pública más recientes recogen la necesidad de los auditores revisen la fiabilidad de los sistemas de información, de los controles internos y de la seguridad de la información[1].

Para la adecuada comprensión de esta guía debe leerse previamente la GPF-OCEX 1315 y la GPF-OCEX 1316.

Para revisar los CGTI será indispensable que el equipo de fiscalización cuente con la colaboración de especialistas en auditoría de sistemas de información, bien personal propio del OCEX o bien expertos externos contratados.

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

[1] A modo de ejemplo:

a) La Ley 16/2017 que modifica 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:

"CAPÍTULO III De la auditoría pública

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."*

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

2. Objetivos de esta etapa de la auditoría

La revisión de los controles generales TI como finalidad:

- 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 significativos que van a ser revisados.
- Identificar, analizar y comprobar el adecuado funcionamiento de los controles generales.
- Confirmar si la estrategia de auditoría adoptada en la planificación es válida.
- Reducir el riesgo de auditoría a un nivel aceptable.

El **objetivo de la auditoria** de los CGTI será obtener una seguridad razonable de que el sistema de control interno proporciona una seguridad razonable sobre la confidencialidad, integridad, autenticidad, disponibilidad, y trazabilidad de los datos, la información y los activos de los sistemas de información.

3. Concepto de control general

3.1 Los controles generales 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.

Los controles generales de tecnologías de la información (CGTI) son aquellos controles relacionados con el uso de las tecnologías de la información y las comunicaciones (TIC) implantados en los distintos niveles de la estructura organizativa general de una institución y en sus sistemas de información, que establecen un marco general de confianza respecto del funcionamiento del resto de controles implantados en los procedimientos y aplicaciones informáticas de gestión.

Su importancia radica en que tienen un efecto generalizado, es decir, suelen afectar a más de una aplicación informática, y si los CGTI no funcionan adecuadamente se imposibilita que se pueda confiar en los controles de los procedimientos y aplicaciones de gestión.

3.2 La finalidad de los controles generales de un entorno informatizado 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 el correcto funcionamiento de los controles de aplicación.

3.3 Desde el punto de vista del auditor **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 Esquema Nacional de Seguridad**:**

- **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.
- **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.
- **Trazabilidad**, es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3.4 La finalidad de la auditoría de los CGTI es verificar su eficacia, es decir que garantizan razonablemente estas propiedades. Para poder confiar en los controles implantados en las aplicaciones informáticas es requisito fundamental que los controles generales del entorno de TI sean efectivos y, por tanto, permitan garantizar el buen funcionamiento de aquellos. En caso contrario, no se podrá confiar en los controles automáticos embebidos en las mismas.

Tomando en consideración los diferentes niveles que conforman los sistemas de información, la revisión de los CGTI se estructura en las áreas que se detallan en el apartado 5 siguiente.

3.5 A los efectos de esta guía, podemos representar el sistema de información de una entidad mediante un modelo simplificado formado por cinco niveles o capas tecnológicas superpuestas, tal como se muestra en la figura 2.

Debemos hacer una primera distinción muy importante entre[2]:

- Los **controles generales de las tecnologías de la información (CGTI).** Afectan a todos los niveles de los sistemas de información, si bien están relacionados con mucha mayor intensidad con aquellos niveles de carácter general que afectan a toda la organización y a los sistemas TI. Son políticas y procedimientos vinculados a muchas aplicaciones y favorecen un funcionamiento eficaz de los controles de las aplicaciones.
- Los **controles de aplicación.** Operan al nivel de los procesos de gestión y que se aplican al procesamiento de las transacciones mediante aplicaciones informáticas específicas. Son analizados en la GPF-OCEX 5340.

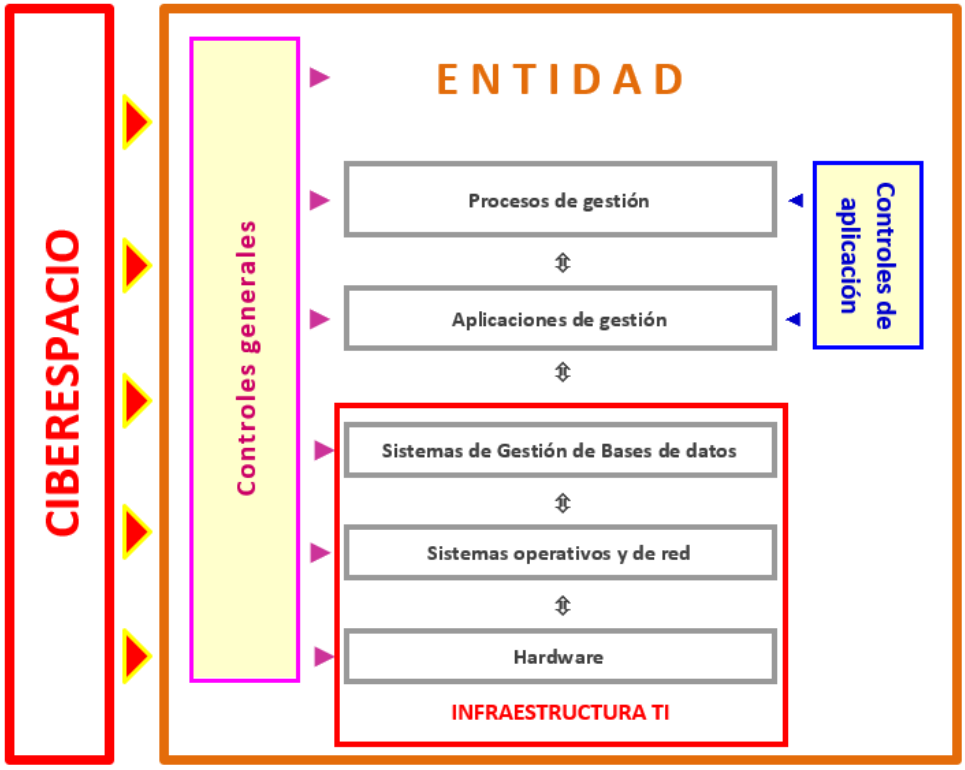

Figura 2

[2] Véase GPF-OCEX 1316; apartado 9.2.

3.6 Los CGTI pueden establecerse en los siguientes niveles:

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 TIC. Forman el entorno o ambiente de control de una entidad y son un componente fundamental del modelo COSO[3].

El ambiente o 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 el tono adecuado de control sea marcado por los máximos responsables de la entidad, 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. Por consiguiente, la fortaleza o debilidad de los controles a nivel de entidad tendrá su efecto en la naturaleza, extensión y momento en que se realicen las pruebas de auditoría.

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.

Una sólida comprensión de los controles a este nivel por parte del auditor, proporciona una buena base para evaluar los controles relevantes relacionados con la información contable y financiera en el nivel de los procesos de gestión.

b) Nivel de procesos/aplicaciones de gestión

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.

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. *Por ejemplo, los procedimientos de gestión de la configuración garantizarán razonablemente que los cambios en el software de las aplicaciones son verificados totalmente y están autorizados.*

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 y los ficheros de transacciones de nóminas) a usuarios autorizados bajo los principios de necesidad de saber y de mínimo privilegio.

También se puede evaluar la seguridad establecida en la propia aplicación para restringir el acceso en mayor medida, normalmente mediante creación de usuarios con palabra clave de acceso y otras restricciones programadas en el software de la aplicación mediante una adecuada gestión de los perfiles de usuario y sus privilegios. Así, 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.

[3] Committee of Sponsoring Organizations of the Treadway Commission

c) Nivel de la infraestructura TI

La infraestructura TI constituye la base de las operaciones de la entidad y normalmente incluyen 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 por un departamento TI.

Los controles en este nivel están formados por los procesos que gestionan los recursos específicos del sistema TI relacionados con su soporte general; son más específicos que los establecidos al nivel de entidad y normalmente están relacionados con un tipo determinado de tecnología.

Dentro de este nivel hay varios subniveles o capas tecnológicas que el auditor debe evaluar separadamente:

- ✓ Sistemas de gestión de bases de datos

  Los CGTI en el nivel de la base de datos hacen frente habitualmente a los riesgos derivados de la utilización de las TI para realizar modificaciones no autorizadas de la información financiera de las bases datos mediante el acceso directo a las mismas o mediante la ejecución de scripts.

- ✓ 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.

  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).

  También se incluye el middleware[4], los sistemas de virtualización, utilidades diversas, correo electrónico y aplicaciones no relacionadas con los procesos de gestión de la actividad de la entidad.

- ✓ Sistemas de virtualización

  La tecnología actual ha generalizado el uso de aplicaciones que permiten crear "máquinas virtuales" para realizar las funciones de servidores de sistemas operativos y de soporte a otras aplicaciones o bases de datos y que mejoran la eficiencia en la gestión de los sistemas de información, permitiendo ahorros de espacio y de personal significativos.

  El uso de estas aplicaciones se encuentra presente en la mayor parte de los sistemas de información actuales y representan un nuevo riesgo a considerar, ya que es frecuente que la mayoría de los procesos críticos de una entidad dependan del adecuado funcionamiento de la virtualización. En estos casos será necesario revisar su adecuada configuración para garantizar los controles del resto de sistemas dependientes.

- ✓ Redes

  Los CGTI a nivel de capa de red cubren los riesgos derivados del uso de técnicas de segmentación de red, acceso remoto y 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*. Incluye las comunicaciones.

[4] *Middleware* es software que permite la compatibilidad entre los distintos sistemas TI, SGBD y las aplicaciones de negocio.

3.7 Los controles pueden clasificarse en tres tipos:

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 passwords 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 semanalmente todos los pases a producción de las modificaciones en las aplicaciones para verificar que están debidamente autorizadas.
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 reducida dimensión los controles de segregación de funciones pueden ser difíciles de implantar y deben compensarse con controles que impliquen una mayor supervisión o control gerencial.

Figura 3

4. Interrelación de los controles generales con los controles de aplicación

4.1 Los CGTI ayudan a asegurar el correcto funcionamiento de los sistemas de información mediante la creación de un entorno adecuado para el correcto funcionamiento de los controles de aplicación.

Una evaluación favorable de los CGTI da confianza al auditor sobre los controles de aplicación automatizados integrados en las aplicaciones de gestión. Si no existieran controles generales o no fueran efectivos, no se podría confiar en los controles de aplicación y sería necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos. Es decir, la eficacia de los CGTI afecta a la estrategia de auditoria que se debe adoptar.

Para más detalles ver apartado 5 en la FGPF-OCEX 5340.

5. Categorías de controles generales

5.1 Existen diversas clasificaciones de CGTI según el marco conceptual[5] que se adopte y de cuáles sean los objetivos de la auditoria, aunque las subcategorías y controles son básicamente coincidentes en todos los casos. A los efectos de esta guía, los CGTI se han agrupado en **cinco** categorías, de acuerdo con el esquema básico mostrado en la Figura 4.

[5] Por ejemplo: INTOSAI/WIGITA, COBIT, FISCAM de la GAO, NIA-ES 315.

Categorías de controles	Controles principales	Medidas del ENS
A. Marco organizativo	A.1 Cumplimiento de legalidad (CBCS.8)	org.1
	A.2 Estrategia de seguridad	org.2
	A.3 Organización y personal de TI	
	A.4 Marco normativo y procedimental de seguridad	mp.per
B. Gestión de cambios en aplicaciones y sistemas	B.1 Adquisición de aplicaciones y sistemas	
	B.2 Desarrollo de aplicaciones	mp.sw.1 y 2
	B.3 Gestión de cambios	op.exp.5
C. Operaciones de los sistemas de información	C.1 Inventario de hardware y software (CBCS 1 y 2)	op.exp.1
	C.2 Gestión de vulnerabilidades (CBCS.3)	op.exp.3 y 4
	C.3 Configuraciones seguras (CBCS.5)	op.exp.2 y 3
	C.4 Registro de la actividad de los usuarios (CBCS.6)	op.exp.8 y 10
	C.5 Servicios externos	op.ext.1 y 2
	C.6 Protección frente a malware	op.exp.6
	C.7 Protección de las instalaciones e infraestructuras	mp.if
	C.8 Gestión de incidentes	op.exp.7 y 9
	C.9 Monitorización	
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS.4)	op.acc.4
	D.2 Mecanismos de identificación y autenticación	op.acc.1 y 5
	D.3 Gestión de derechos de acceso	op.acc.4
	D.4 Gestión de usuarios	op.acc
	D.5 Protección de las redes y comunicaciones	mp.com
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS.7)	mp.info.9
	E.2 Plan de continuidad	op.cont.2 y 3
	E.3 Alta disponibilidad	mp.if.9

Códigos de colores: Controles básicos de ciberseguridad (*son controles mínimos a revisar en cualquier fiscalización*)

Figura 4

5.2 La ausencia de una actividad de control determinada o la ineficacia de su diseño, 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.

6. Identificar qué CGTI son relevantes para revisar en una auditoría

6.1 En una entidad mediana o grande se pueden identificar, en conjunto, numerosos CGTI que:

- Resulta materialmente imposible revisarlos en su totalidad.
- Gran parte de ellos no tienen interés para los objetivos de la auditoria.
- Sólo un pequeño subconjunto tiene impacto en el riesgo de auditoria.

A estos últimos los denominaremos controles relevantes y en ellos deberá centrar la atención y trabajo el auditor. Para ello se aplicará la metodología descrita en el anexo 2 de la GPF-OCEX 1315, según la cual el análisis de las cuentas a auditar conduce a identificar las aplicaciones de gestión significativas en las que debe centrar el esfuerzo el auditor.

A continuación, el enfoque de riesgo requiere que para cada área o aplicación significativa:

- Se valoren los RIM relacionados.
- Se revise la eficacia del control interno:
  1º los CGTI relacionados, y
  2º los controles de procesos /aplicación de gestión
- Se realicen las pruebas sustantivas.

La importancia de los CGTI es tal que del resultado de su revisión dependerá la naturaleza, extensión y momento de realización de las pruebas sobre los controles de procesos/aplicación y de las pruebas sustantivas.

6.2 Debido al gran número de CGTI que existen en una entidad mediana o grande, el enfoque de riesgo brevemente descrito nos permite centrarnos solo en los controles que están relacionados con los sistemas y las aplicaciones significativas a efectos de la información contable, financiera o presupuestaria auditada, de acuerdo con los objetivos y alcance de la auditoría que se esté realizando. Es decir, aquellos cuyo buen funcionamiento afecta a las aplicaciones identificadas cómo significativas, el resto carece de interés para la auditoría financiera.

Si el número de aplicaciones significativas es elevado, tal como sucede por ejemplo en la auditoría de las cuentas de una comunidad autónoma, será imposible revisar todos los controles de aplicación y CGTI relacionados. En estos casos se deberá establecer un plan de auditoria plurianual que establezca un calendario para la revisión de los controles automatizados, tanto de aplicación cómo generales, que sea realizable con los recursos del OCEX.

Si se revisan los CGTI de algún sistema o subsistema que no tiene relación con la información contable, financiera o presupuestaria auditada 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 área significativa, los procedimientos de revisión de los controles generales 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 inventario de 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.

Es decir, los CGTI deben evaluarse en relación con su efecto en las aplicaciones significativas y en los datos relacionados con las cuentas anuales auditadas. *Por ejemplo, si no se han implementado nuevos sistemas durante el periodo auditado, las debilidades en los CGTI sobre el desarrollo de sistemas pueden no ser relevantes respecto de las cuentas anuales auditadas.*

6.3 Si se realiza una auditoría informática no integrada en una auditoría financiera, generalmente todas las categorías de controles y todos los CGTI pueden ser relevantes excepto que expresamente se excluyan del alcance de la auditoría.

Pero si la auditoría de los sistemas de información forma parte de una auditoría financiera (o de una auditoría operativa) **se analizará con los auditores financieros** aquellos controles que son relevantes para los objetivos de la auditoría financiera (u operativa), ya que no todos los riesgos son iguales, ni en probabilidad, ni en su materialidad. Se deberá adoptar un enfoque basado en el análisis del riesgo.

Por otra parte, todos los controles tampoco son iguales en su grado de eficacia a la hora de reducir los riesgos identificados; por tanto no será necesario evaluar todas las actividades de control relacionadas con un riesgo concreto, hay que ceñirse únicamente a aquellos controles que sean relevantes, es decir, aquellos que proporcionan una mayor seguridad de que el objetivo de control se ha alcanzado.

Un control será relevante cuando su ausencia o su mal funcionamiento representa una deficiencia significativa o una debilidad material de control interno. En otras palabras es aquel que proporciona una seguridad razonable de que incorrecciones materiales serán prevenidas o detectadas

oportunamente. En consecuencia, el auditor seleccionará para revisar solo los controles relevantes, es decir aquellos que le permitan mitigar determinados riesgos de incorrección material.

6.4 A la hora de 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.

  En la mayoría de los casos, resulta 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 de seguridad que previenen o detectan accesos no autorizados son importantes.
- Los controles preventivos son por regla general más eficientes que los detectivos. Por lo tanto, los controles preventivos se consideran a menudo relevantes.

  Por ejemplo, prevenir que se produzca un fraude es mucho mejor que simplemente detectarlo después de que haya ocurrido.
- Los controles automatizados son más fiables que los controles manuales.

  Por ejemplo, los controles automatizados que obligan al usuario 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.

6.5 Para cada CGTI que se haya identificado como relevante, el auditor debe aplicar **procedimientos** para **analizar la efectividad de su diseño para realizar la actividad de control**, considerando el riesgo TI y los objetivos de la auditoría.

Si se concluye que el diseño es eficaz se aplicarán procedimientos de auditoría para **verificar si está implementado y en funcionamiento durante todo el periodo auditado**.

7. Procedimientos de auditoria

7.1 El primer paso, en cualquier auditoria, es obtener un conocimiento adecuado de lo que se va a auditar, en este caso del sistema de información y de los controles generales.

Los procedimientos de auditoria a ejecutar para conocer el entorno tecnológico y los CGTI dependerán del tipo de auditoria que se vaya a realizar, de los objetivos de la misma y de la profundidad requerida.

7.2 Se tendrá una reunión en la que se explicará personalmente al responsable de TI y al coordinador cuál es el objetivo general del trabajo, calendario e información que se les va a solicitar.

La solicitud de la información podrá realizarse por escrito o correo electrónico dirigido al coordinador de la fiscalización o al responsable del departamento de TI (si se acuerda este procedimiento con el coordinador y el responsable de TI) al iniciarse la fiscalización.

El equipo de auditoría debe asegurar la seguridad en el envío y recepción de la información sobre los sistemas de 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.

7.3 Sin ánimo de ser exhaustivo pueden presentarse las siguientes situaciones:

a) Auditorias operativas o específicas de sistemas de información:

- Auditorias de los controles de ciberseguridad.
- Auditoria de sistemas de los registros contables de facturas.
- Auditoría de los sistemas de control interno.
- Auditoría de seguridad.
- Etc.

En estas auditorías se requerirán procedimientos específicamente diseñados, que normalmente incluirán o estarán basados en el cuestionario del Anexo 3 y el trabajo se documentará en las fichas del Anexo 4.

b) Auditoria de sistemas de información en apoyo de auditorías financieras o de cumplimiento.

- Auditorias con alcances limitados.

  En cualquier auditoria que requiera un conocimiento básico de la entidad y de su sistema de control interno, se revisarán los CBCS (véase la GPF-OCEX 5313), que están incluidos en el programa del Anexo 4.

- Auditorias financieras de cuentas anuales o de elementos de las cuentas anuales.

  Por ejemplo: de la cuenta general de un ayuntamiento, de la liquidación del presupuesto, de los gastos de personal, de los ingresos tributarios.

  En estas auditorías junto con la petición inicial de información se solicitará que se cumplimente el cuestionario del Anexo 3 (ajustado al alcance de controles que se determine), se obtendrán evidencias adicionales y se documentará el trabajo realizado y las conclusiones con las fichas del Anexo 4.

  Los CBCS tendrán carácter de revisión mínima y están incluidos en el programa del Anexo 4.

  Los controles a revisar serán los del apartado 5.

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

7.5 El cuestionario que se adjunta como Anexo 3 está diseñado para:

- 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.

El cuestionario se estructura en las 5 áreas vistas en el apartado cinco.

7.6 Tras recibir el cuestionario cumplimentado, el equipo de auditoría analizará la información contenida en el mismo, que se utilizará para realizar el trabajo previsto en el Anexo 4.

Estas fichas están diseñadas para:

- Ayudar a obtener información avanzada sobre los sistemas de información de la entidad fiscalizada y de los CGTI.
- Ayudar a identificar actividades y objetivos de control relacionadas con los CGTI.
- Ayudar a evaluar el diseño y eficacia de los CGTI de la entidad auditada.

- Ayudar a 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 a la eficacia e implementación de los CGTI.

Estas fichas/programa estándar debe adaptarse en cada caso a las características del ente auditado, de sus sistemas de información, y del objetivo y alcance de la auditoría. Los objetivos de control son invariables, pero el diseño de los controles y las características de su implementación son específicos de cada entidad.

Estos procedimientos se ejecutarán en aquellas fiscalizaciones en la que se deba emitir una opinión de auditoría de seguridad razonable sobre las cuentas anuales o un componente significativo de las mismas en entidades en la que su actividad se apoye en sistemas TIC o en aquellas auditorías específicas de los CGTI.

Este procedimiento ha sido diseñado para ser completado por personal con conocimientos sobre los CGTI. En general se realizará por un especialista en auditoría de sistemas de información.

Las fichas se estructuran en las 5 áreas vistas en el apartado cinco.

7.7 Una vez cumplimentado el Anexo 4, **se concluirá** indicando:

- Conclusiones generales sobre los controles revisados.
- Identificar y evidenciar las deficiencias de control detectadas.
- Identificar y documentar riesgos incorrección material sobre los estados financieros.
- Necesidad de trabajo adicional.

7.8 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 sistemas de información.

8. Evaluación de las deficiencias de control interno detectadas

8.1 Cada uno de los controles principales señalados en la Figura 4 está compuesto por una serie de **subcontroles o controles detallados**, que son detallados en la fichas de revisión del Anexo 4. En estas fichas se debe documentar el trabajo realizado y concluir para cada subcontrol, en base a las evidencias, sobre su **eficacia** pudiendo encontrarse cada uno de ellos en alguna de las siguientes situaciones:

Control efectivo

Control bastante efectivo

Control poco efectivo

Control no efectivo

8.2 Además cada **control principal** (compuesto por subcontroles) se evaluará utilizando el modelo de **nivel de madurez** (ver Anexo 1) y se deberá concluir en las mismas FICHAS DE REVISIÓN. Para evaluar el nivel de madurez se tendrá en cuenta los resultados obtenidos en los subcontroles que lo forman y la importancia relativa de estos para el cumplimiento del objetivo de control.

8.3 Tras analizar los resultados de la revisión de cada control se extraerán las deficiencias de control interno observadas y las recomendaciones que se deriven de las mismas, que deben estar bien soportadas en los papeles de trabajo. Los hallazgos de auditoría que las soportan deben incluir: *(GPF-OCEX 1735; P9)*

Criterio (de auditoría): la referencia o norma con la que se compara o evalúa el hecho observado; lo que debería ser.

En las auditorías de sistemas de información (CGTI, controles de aplicación y cibercontroles) los criterios de auditorías son los establecidos con carácter general en la GPF-OCEX relacionadas, que están basadas en el ENS, NIA-ES, ISSAI, etc.

Hecho o condición: la situación observada y documentada en la auditoría.

Están basados en evidencia de auditoría. Pueden ser deficiencias de control, problemas operacionales o incumplimiento de requerimientos legales o administrativos.

Causa: las razones que dan lugar al hecho observado.

Puede servir como base para proponer acciones correctoras en las recomendaciones. Se debe identificar la unidad o departamento responsable de la deficiencia.

Las causas más comunes incluyen políticas, procedimientos o criterios mal diseñados, o aplicados de forma inconsistente, incompleta o incorrecta; o factores más allá del control de los gestores. Los auditores pueden evaluar si la evidencia proporciona un argumento razonable y convincente de por qué la causa indicada es el factor clave que contribuye a la diferencia entre la condición y los criterios.

Efecto: qué consecuencia negativa tiene lugar o podría tener lugar, provocada por la diferencia entre el hecho observado y el criterio.

Explica el impacto adverso al objetivo operacional u objetivo del control. Al articular el impacto y el riesgo, el elemento del efecto real o potencial es muy importante para ayudar a convencer a la administración del auditado de la necesidad de tomar acciones correctoras en respuesta a los problemas y/o riesgos significativos identificados.

Recomendación: acciones correctoras sugeridas.

Las recomendaciones deben redactarse de forma que se aborde la corrección de las causas que originan el hecho o condición observado.

8.4 Al evaluar las deficiencias de control interno detectadas se deben 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; P10)*

8.5 Las deficiencias de control interno se clasifican en tres niveles de importancia relativa al examinar el control interno: *(GPF-OCEX 1735; P11)*

- Una **deficiencia de control interno** existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable. Pueden ser *deficiencia de diseño* del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o *deficiencias de funcionamiento* (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).
- Una **deficiencia significativa** es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera o presupuestaria de forma fiable, de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota, de que una manifestación errónea en las cuentas anuales, o un incumplimiento, que no es claramente trivial, no sea prevenida o detectada en plazo oportuno.
- Una **debilidad material** es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una manifestación errónea significativa en las cuentas anuales o un incumplimiento de carácter grave no sea prevenida o detectada y corregida en plazo oportuno.

8.6 La evaluación de importancia relativa o significatividad de las deficiencias incluye consideraciones sobre los siguientes factores de carácter general: la magnitud del impacto, la probabilidad de que ocurra y la naturaleza de la deficiencia. *(GPF-OCEX 1735; P12)*

Implica evaluar, en el contexto de los objetivos de la auditoría, los siguientes factores:

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.

8.7 En particular, 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.
- Es una deficiencia de control interno que ocasiona un aumento significativo del riesgo de auditoria.
- 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:

  (1) 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;
  (2) la habilidad para acceder directamente y modificar ficheros que contengan información financiera; o
  (3) 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).

8.8 Además al evaluar las deficiencias de un CGTI deben hacerse otras consideraciones adicionales:

- **Efecto en los controles de las aplicaciones**.

  La importancia de una deficiencia en un CGTI debe ser evaluada en relación con su efecto en los controles de aplicación, es decir, si provoca que los controles de aplicación 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 controles de aplicación, 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 conjuntamente 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.

8.9 Basándose en las consideraciones reseñadas el auditor financiero y el auditor informático, conjuntamente, determinarán si las deficiencias de control son, individualmente o en conjunto, debilidades materiales o deficiencias significativas.

Si las deficiencias de control constituyen debilidades materiales, el auditor concluirá que los CGTI no son eficaces y deberá replantearse su estrategia de auditoria, omitiendo revisar los controles de aplicación puesto que no van a ser eficaces, dando mayor énfasis a los procedimientos sustantivos, de forma que se intentará minimizar el riesgo final de auditoria.

8.10 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; P13)*

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 6

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

Anexo 1. Niveles de madurez de los procesos según la Guía de seguridad CCN-STIC 804

Para evaluar los resultados generales por cada uno de los CGTI se utilizará el modelo de nivel de madurez de los procesos[6] usando una escala entre 0 y 5. Este modelo proporciona una base para comparar resultados entre distintos entes y entre distintos periodos para un ente determinado.

Nivel	Descripción
0 - Inexistente.	Esta medida no está siendo aplicada en este momento.
1 - Inicial / ad hoc	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. *La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.*
2 - Repetible, pero intuitivo.	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas, sin procedimientos escritos ni actividades formativas. *La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.*
3 - Proceso definido	Los procesos están estandarizados, documentados y comunicados con acciones formativas. *Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.* *Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.*
4 - Gestionado y medible.	La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere. *Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.* *En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.*
5 - Optimizado.	Se siguen buenas prácticas en un ciclo de mejora continua. *El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.* *En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.*

[6] Basado en la Guía de seguridad CCN-STIC 804.