Guía práctica de fiscalización de los OCEX

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

Referencia: GPF-OCEX 1315 (Revisada) y GPF-OCEX 5330

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 19/10/2023.

1. Gobernanza y normas de auditoría

Uno de los primeros pasos que el auditor debe dar en una auditoría, de acuerdo con el requerimiento 19.a.i de la GPF-OCEX 1315R/NIA-ES 315R, consiste en aplicar procedimientos de valoración del riesgo para obtener conocimiento de la entidad y su entorno, y en particular de la estructura organizativa, de propiedad y de **gobierno de la entidad** y de su modelo de negocio, **incluido el grado en que el modelo de negocio integra el uso de TI.**

Posteriormente se deberá obtener conocimiento del **sistema de control interno**, que la GPF-OCEX 1315R/NIA-ES 315R define (apartado 11.m) como el sistema diseñado, implementado y mantenido por los **responsables del gobierno de la entidad**, la **dirección** y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad relativos a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables.

A los efectos de las NIA, el sistema de control interno comprende cinco componentes interrelacionados:

a) el entorno de control;

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 y

e) las actividades de control.

Además, en referencia al sistema de control interno, también se requiere (apartado 21.a de la GPF-OCEX 1315R/NIA-ES 315R) que el auditor obtenga conocimiento del primer componente del *entorno de control*, es decir, del conjunto de controles, procesos y estructuras que tratan:

a) el modo en que la dirección ejerce las **responsabilidades de supervisión**, tales como la cultura de la entidad y el compromiso de la dirección con la integridad y los valores éticos;

b) **la independencia de los responsables del gobierno de la entidad y su supervisión del sistema de control interno** de la entidad cuando estos sean distintos de la dirección;

c) la asignación de **autoridad y responsabilidad** en la entidad.

Interesa destacar cómo las NIA-ES distinguen claramente entre gobierno corporativo y dirección, con diferentes responsabilidades y funciones,.

Continúa la nueva GPF-OCEX 1315R/NIA-ES 315R señalando (apartado A108) que 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 realizadas a través de TI, incluida la complejidad o madurez de la plataforma o arquitectura tecnológica 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 modificación.

2. Porqué es importante para el auditor conocer la estructura de gobierno y dirección de la entidad, incluida la gobernanza sobre las TI

Como ya se ha señalado, el auditor debe adquirir un conocimiento del entorno de control del sistema de control interno de la entidad[1] que incluye las **funciones de gobierno y de dirección**, así como las actitudes, grado de percepción y actuaciones de los **responsables del gobierno de la entidad y de la dirección** en relación con el sistema de control interno de la entidad.

Es importante conocerlo, ya que el entorno de control establece el tono directivo (tone at the top) de una organización, influye en la conciencia de control de sus miembros y proporciona un fundamento general para el funcionamiento de los demás componentes del sistema control interno de la entidad.

El grado de conocimiento de estas importantes cuestiones que deberá adquirir el auditor será acorde con el tamaño y complejidad de la entidad auditada. **Cuanto mayor y más compleja sea la entidad mayor importancia le deberá dar el auditor a esta cuestión.**

Los responsables del gobierno ejercen una influencia importante sobre la conciencia de control de una entidad, sobre su "cultura" de control. En consecuencia, las siguientes cuestiones influyen en la valoración de la eficacia del diseño del entorno de control relativo a la participación de los responsables del gobierno de la entidad:

- Su independencia con respecto a la dirección y su capacidad para evaluar las acciones de la dirección.
- Si comprenden cómo desarrolla su actividad o las transacciones comerciales de la entidad.
- La medida en que evalúan si los estados financieros se preparan de conformidad con el marco de información financiera aplicable, y si incluyen la información a revelar adecuada.

Hemos visto al principio que la nueva GPF-OCEX 1315R/NIA-ES 315R establece que la evaluación del entorno de control es un aspecto clave del conocimiento y revisión del sistema de control interno de la entidad auditada, y en aquellas entidades que operen en un entorno de administración electrónica avanzada, será preciso analizar si la **gobernanza sobre las TI** es acorde con la naturaleza y complejidad de la entidad y de sus operaciones de negocio realizadas a través de TI, incluida la complejidad o madurez de la plataforma o arquitectura tecnológica de la entidad y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera. También se analizará la **estructura organizativa de la dirección en relación con las TI y los recursos asignados.**

El auditor debe obtener un conocimiento suficiente del diseño y la implementación de las prácticas de gobernanza sobre las TI en la entidad auditada durante la planificación y la fase inicial del trabajo. Un buen conocimiento de los posibles riesgos a los que se enfrenta la entidad cuando estas prácticas son inadecuadas es un requisito previo para cualquier trabajo de auditoría de TI. Incluso si los objetivos de la auditoría no cubren expresamente la gobernanza de TI, **muchas debilidades de control en cualquier dominio pueden estar relacionadas con mecanismos de gobernanza inadecuados**.

[1] Véanse los puntos 4 y 5 del Anexo 3, de la GPF-OCEX 1315 Revisada.

Resulta ilustrativo revisar los **riesgos** asociados a una gobernanza sobre las TI inadecuada que se detallan en el apartado 6 siguiente.

Un auditor de los OCEX puede necesitar analizar la situación de la gobernanza sobre las TI por alguno de estos motivos:

a) En una auditoría financiera, de acuerdo con lo establecido en las GPF-OCEX 1315R/NIA-ES 315R.

b) En una auditoría de CGTI, tal como establece la GPF-OCEX 5330.

c) En una auditoría específica sobre gobernanza de las TI.

La auditoría puede desempeñar un papel importante en la mejora de la gobernanza sobre las TI en una entidad pública al proporcionar recomendaciones que mitiguen los riesgos asociados con uno o más elementos de la gobernanza sobre las TI. El auditor de TI debe conocer los riesgos derivados de la falta de una gobernanza adecuada sobre las TI, identificar los elementos clave que son inadecuados y hacer recomendaciones pertinentes para su subsanación.

Un componente muy importante de la gobernanza sobre las TI es la gobernanza de la seguridad de la información que afecta de forma directa a la valoración de los riesgos de auditoría derivados del uso de las TI, que se comentará más adelante. Esta materia se trata en profundidad en la *GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría*.

3. Qué debe entenderse por gobierno de la entidad o gobernanza corporativa

Aclaremos en primer lugar qué debe entenderse por **gobierno de la entidad**, término utilizado por las NIA, a los efectos de las auditorías realizadas en el sector público. Este término es equivalente al de **gobernanza corporativa** utilizado por otros marcos normativos como las normas UNE-ISO.

En la GPF-OCEX 1315 (versión 18/11/2015) se definía **gobierno de la entidad como la función de la persona o personas u organizaciones responsables de la supervisión de la dirección estratégica de la entidad y de las obligaciones relacionadas con la rendición de cuentas de la entidad**. Esta definición sigue siendo totalmente válida en la actualidad.

En la Nota explicativa de la NIA-ES-SP 1315 se señala que, en relación con la denominación en el derecho mercantil y público de los **órganos de dirección y gobierno de las entidades auditadas**, habrá que tener en cuenta, en particular, la correspondiente norma de creación de la organización auditada, y en general, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En tal sentido, generalmente hay que entender como "**Dirección**" a aquellas personas que tienen la responsabilidad ejecutiva y esta responsabilidad ejecutiva tendrá que determinarla el auditor público en función de la legalidad aplicable y el diseño de la estructura de la organización auditada; por otra parte, se entiende como "**Gobierno de la entidad auditada**" u órgano superior de la entidad auditada a aquella persona o conjunto de personas que tiene la facultad de supervisar a la "Dirección" y de formular las cuentas anuales. En referencia a las Entidades Locales, habrá que estar a lo previsto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

Atendiendo a la definición dada en la UNE-ISO/IEC 38500[2] la "**gobernanza corporativa**" es el sistema por el cual se dirigen y controlan las organizaciones. Y la distingue de la "**gestión**" que define como el sistema de controles y los procesos necesarios para alcanzar los objetivos estratégicos establecidos por el **órgano de gobierno de la entidad**. La gestión está sujeta a la dirección marcada por la política y seguimiento establecidos por medio de la gobernanza corporativa.

[2] UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información.

Debemos distinguir entre la función y el órgano responsable de ejecutarla:

Función	Definición	Órgano	
Gobierno de la entidad o gobernanza corporativa	El sistema por el cual se dirigen y controlan las organizaciones. Función de la persona o personas u órganos superiores responsables de la supervisión de la dirección estratégica de la entidad y de las obligaciones relacionadas con la formulación y rendición de cuentas de la entidad.	Órgano de gobierno de la entidad	Aquella persona o conjunto de personas que tiene la facultad de supervisar a la "Dirección" y de formular las cuentas anuales
Gestión o dirección	Sistema de controles y los procesos necesarios para alcanzar los objetivos estratégicos establecidos por el órgano de gobierno de la entidad.	Dirección	Aquellas personas que tienen la responsabilidad ejecutiva

En las sociedades mercantiles resulta sencillo identificar su órgano de gobierno ya que coincidirá con el consejo de administración. En el resto de entes instrumentales del sector público, normalmente, revisando sus estatutos también será sencillo identificar y distinguir sus órganos de gobierno de sus órganos ejecutivos o dirección ejecutiva al máximo nivel o alta dirección.

Sin embargo, en las administraciones públicas esta cuestión no siempre es evidente por la confusión existente entre los órganos de gobierno corporativos (consejos de gobierno en las comunidades autónomas y juntas de gobierno en las entidades locales) y la alta dirección (que son los mismos órganos).

Partiendo del apartado 55 de la *GPF-OCEX 1730 Preparación de informes de auditoría sobre los estados financieros*, se pueden poner los siguientes ejemplos orientativos:

Entidad	Responsables del gobierno de la entidad	Dirección de la entidad
Sociedad mercantil	Administradores.	Directores ejecutivos (incluye administradores únicos, consejero delegado…).
Ayuntamiento	Alcalde, Junta de Gobierno Local y Pleno.	Alcalde, Tenientes de Alcalde, Directores y responsables de área.
Comunidad Autónoma	Consejo de Gobierno (Presidente y Consejeros).	Presidente, Consejeros, secretarios, subsecretarios y directores generales.
Fundación	Patronato.	Consejo ejecutivo o de dirección. Director, administrador o gerente. Directores funcionales.
Consorcio	Órganos de gobierno.	Órganos ejecutivos y de dirección.
Diputación provincial	Presidente, Vicepresidente/s, Pleno de Diputación y Junta de Gobierno.	Presidente, Junta de Gobierno, diputados y personal directivo.
Universidad	Consejo de gobierno, Rector.	Rector y equipo de gobierno.

4. Qué es la gobernanza sobre las TI

La implantación plena de la administración electrónica avanzada, tras un proceso de transformación digital y de hiperconexión de sistemas a través de internet, ha ocasionado que las entidades públicas sean totalmente dependientes de las TI lo que a su vez ha provocado que sea mucho más importante la existencia de una adecuada gobernanza TI.

L**a gobernanza sobre las TI es un componente clave de la gobernanza corporativa en general**. Debe ser considerada como la forma en la que las TI crean valor para adaptarse a la estrategia de gobernanza corporativa de la entidad y nunca debe ser considerada como una disciplina por sí sola. Al adoptar este enfoque, se requerirá que todas las partes interesadas participen en el proceso de toma de decisiones. Esto crea una aceptación compartida de la responsabilidad para los sistemas críticos y garantiza que las decisiones relacionadas con TI sean tomadas y conducidas por la organización y no a la inversa.[3] Según COBIT 2019, el gobierno de las TI se interesa por la entrega de valor derivada de la transformación digital y la mitigación del riesgo de negocio que resulta de dicha transformación digital.

Para profundizar sobre lo qué debemos entender por gobernanza sobre las TI conviene acudir de nuevo a la norma *UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información (TI)*, que define (apartado 1.6.3) la gobernanza corporativa de la TI como **el sistema por el cual se dirige y controla el uso, actual y futuro, de la TI**. Implica evaluar y dirigir la utilización de la TI para dar soporte a la organización y la monitorización de ese uso para lograr la consecución de los planes. Incluye la estrategia y políticas para la utilización de las TI en la organización.

Continuando con la *UNE-ISO/IEC 38500,* en su apartado 2.2, señala que se debería "gobernar" las TI a través de tres tareas principales:

a) **evaluar** el uso actual y futuro de la TI;

b) **dirigir** la preparación y ejecución de planes y políticas para asegurar que el uso de la TI satisface los objetivos de la organización;

c) **monitorizar** el cumplimiento de las políticas y el desempeño con relación a lo planificado.

Por tanto, entenderemos por gobierno corporativo de las TIC o gobernanza sobre las TI, el conjunto de mecanismos para la toma de decisiones estratégicas con relación al uso y la gestión de las TIC en un determinado contexto organizativo[4]. Se refiere, por tanto, a:

a) qué tipo de decisiones estratégicas requieren del gobierno corporativo,

b) quién las debe tomar,

c) cómo se deben tomar y

d) cómo se mide y se hace un seguimiento de su ejecución.

La gobernanza sobre las TI constituye una parte esencial del gobierno de la entidad en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que las TIC respaldan y facilitan el desarrollo de los objetivos estratégicos definidos. Esto garantiza que:

- Las TI están alineadas con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros, incluyendo los relacionados con la ciberseguridad mediante la coordinación con el CSI.

[3] Apartado 1.1 de IT Audit Handbook, INTOSAI, 2014.

[4] Rodríguez y Palao, COBIT y el gobierno corporativo de las TIC (https://blogs.uoc.edu/informatica/cobit-y-gobierno-corporativo-tic/)

Como se ha señalado previamente, la gobernanza sobre las TI es una parte integral de la gobernanza corporativa de una entidad, y comprende el liderazgo organizacional, las estructuras institucionales, los procesos, y otros mecanismos (reporting y retroalimentación, cumplimiento, recursos, etc.) que garantizan que los sistemas de TI alcancen los objetivos y la estrategia de la organización, compensen los riesgos y administren eficazmente los recursos. Los beneficios obtenidos por una entidad pública de una práctica de gobernanza sobre las TI diseñada adecuadamente incluyen la entrega de valor, la gestión de riesgos y recursos, la alineación estratégica de TI con los objetivos de servicio de la entidad y el seguimiento y medición oportunos de los objetivos estratégicos de TI.

Una entidad pública, por lo tanto, debe diseñar e implementar la gobernanza sobre las TI de una manera que satisfaga las necesidades de las partes interesadas[5], garantice que los servicios de TI existentes y las posibles opciones tecnológicas se evalúen para adaptarse mejor a los objetivos generales de la entidad; garantice que se tomen decisiones oportunas para dirigir el gasto en TI; y garantice que el rendimiento y el cumplimiento se contrastan con los objetivos establecidos.

El mensaje importante es que **las decisiones críticas sobre la informática no corresponden al departamento de TI, sino al órgano de gobierno de la entidad** y que se debe encontrar un equilibrio adecuado entre los diferentes interesados y sus objetivos. El conjunto de acciones las debe realizar el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

El diseño de la gobernanza sobre las TI en una entidad pública varía en función de su tamaño, naturaleza y de la dependencia estratégica de las TI para el desarrollo de su actividad. En la mayoría de las entidades, la gobernanza es responsabilidad de un conjunto de altos directivos bajo la dirección del máximo responsable de la entidad. En las entidades públicas más pequeñas, es posible que no se definan claramente funciones distintas para la gobernanza y la gestión de las TI.

En la práctica, no obstante, muchas entidades del sector público no tienen mecanismos formales de decisión sobre la informática residenciados en los órganos de gobierno y muchas de estas decisiones se toman en el marco de la gestión (la dirección de TI, la dirección financiera, el director general o el comité de dirección).

Sin embargo, es importante que exista una capa superior de gobernanza que supervise las funciones de gestión de las TI, evaluando propuestas, considerando opciones y dirigiendo el camino estratégico y los recursos para TI, para que la entidad pública cumpla mejor con sus funciones.

5. Elementos clave de la gobernanza sobre las TI[6]

Los auditores deben comprender y evaluar los diferentes componentes de la gobernanza sobre las TI para determinar con mayor probabilidad si las decisiones de TI, los recursos y el seguimiento del desempeño respaldan las estrategias y objetivos de la organización.

Para llevar a cabo la evaluación, el auditor debe ser consciente de los riesgos asociados a la insuficiencia de cada componente en una entidad (ver apartado 6).

5.1 Estrategia de TI

Un objetivo común a muchas entidades públicas es introducir o ampliar los servicios ofrecidos a través de Internet. La infraestructura y la arquitectura de TI heredada (legacy)[7] de la entidad pueden no ser adecuadas

[5] A los efectos de este documento consideraremos partes interesadas a los empleados, proveedores TI, clientes o destinatarios de los servicios, dirección y órganos de gobierno, y en general cualquier tercero afectado por el uso de las TI por la entidad.

[6] Los apartados 5, 6, 7 y 8 están basados, fundamentalmente, en Guidance on Audit of IT Management functions: IT Governance, Contracts & Sustainability de INTOSAI Working Group on IT Audit, publicado en 2022.

[7] Los sistemas legacy son sistemas anticuados que siguen siendo utilizados por las entidades y que no se quiere o no se puede reemplazar o actualizar de forma sencilla. Se caracterizan por basarse en tecnología fuera de soporte, estar afectados por vulnerabilidades conocidas, pero en los que la aplicación de parches es dificultosa y, en definitiva, constituyen un riesgo para la seguridad no solo del propio sistema sino del entorno TI en el que operan.

para hacer esta transición. Este escenario de negocio requeriría una estrategia de TI claramente documentada que establezca un plan que tenga en cuenta la arquitectura tecnológica, la planificación de la capacidad futura, las inversiones, el modelo de entrega de los servicios, así como la necesidad de recursos.

El auditor debe examinar si existe un documento de estrategia TI o sus componentes equivalentes y si satisface adecuadamente la necesidad de alinear las decisiones de TI, la continuidad de las operaciones de TI y el objetivo de servicio de la entidad pública.

5.2 Estructura de la gobernanza sobre las TI

Un auditor debe examinar si las funciones de los distintos órganos de gobernanza y gestión dentro de la entidad están claramente definidas y apoyadas con procesos que faciliten la toma de decisiones.

Toda entidad de tamaño mediano o grande debería crear un ***Comité de gobernanza sobre las TI*** o cualquier órgano equivalente que incluya miembros de los órganos superiores, de la alta dirección, de la dirección ejecutiva, así como los responsables de TI. El órgano debe tener la responsabilidad de examinar los casos de negocio/estudios de viabilidad para los servicios de TI, decidir sobre las opciones tecnológicas más convenientes para apoyar las decisiones empresariales clave, revisar la disponibilidad de fondos, tomar decisiones de inversión en TI comprometiendo los recursos necesarios y supervisar el rendimiento a nivel estratégico.

Es la pieza central de la estructura organizativa de las TI. Será el órgano colegiado encargado de la definición y supervisión de la estrategia sobre las TIC en una entidad. La definición de la composición y funciones de este comité corresponde al órgano superior de la entidad. Normalmente, estará compuesto por miembros de la alta dirección y gerencia senior que tienen la responsabilidad de revisar, aprobar y comprometer fondos para inversiones en TI.

El Comité de gobernanza sobre las TI debe ser determinante en la elaboración de las decisiones organizativas en las que se debe proporcionar tecnología a fin de respaldar las inversiones, así como en la aprobación de la forma para adquirir esta tecnología. Las decisiones de inversión que involucran las soluciones de desarrollo vs. compra son responsabilidad del comité de gobernanza sobre las TI, y generalmente se toman después de efectuadas las recomendaciones pertinentes por parte de los grupos o comités designados.[8]

Un órgano legalmente obligatorio en el sector público por el Esquema Nacional de Seguridad (ENS) es el **Comité de gobernanza de la ciberseguridad o Comité de seguridad de la información** (ver GPF-OCEX 5314). En las entidades de pequeño tamaño el Comité de gobernanza sobre las TI y el de ciberseguridad pueden confluir en uno único. Ejemplo de esto es la Sindicatura de Cuentas de la Comunidad Valenciana que en sus *Políticas generales de gestión y seguridad de los SI*[9] configura la Comisión de Informática y Gestión de la Seguridad de la Información como órgano con ambas funciones, entre cuyas competencias figura la "Propuesta y análisis de los proyectos y planes de inversión en materia de SI que garanticen la alineación de la organización y medios de los SI con los objetivos generales de la Sindicatura de Comptes". Esta comisión se reúne mensualmente analizando y realizando propuestas coherentes con la estrategia general de la Sindicatura para trasladarlas para su aprobación al órgano de gobierno de la Sindicatura.

Un órgano separado de **Gobernanza de proyectos TI** puede encargarse de supervisar los procesos de preparación de casos de negocio, petición de ofertas y compromiso con los proveedores. De acuerdo con el Observatorio de Administración Electrónica del Ministerio de Hacienda y Función Pública "no nos debemos olvidar que una parte importante del éxito o del fracaso de todos y cada uno de los proyectos es, por un lado, un buen soporte legal y jurídico asociado y, por otro lado, un sistema de gobernanza que permita que todo este tipo de innovaciones pueda acabar en buen puerto y no se quede completamente bloqueado por la resistencia al cambio."[10]

[8] IT Audit Handbook, INTOSAI, 2014.

[9] https://www.sindicom.gva.es/politicas-ssii

[10] Gobernanza para facilitar la innovación en la administración digital, Observatorio de Administración Electrónica, Ministerio de Hacienda y Función Pública, 30 de abril de 2018.

La frecuencia de las reuniones de estos órganos, el tipo de información de referencia examinada, los registros de las decisiones adoptadas (actas) y las respuestas a las preguntas planteadas pueden ayudar al auditor a evaluar la adecuación del funcionamiento de las estructuras de gobernanza sobre las TI.

La ausencia de estos órganos tiene un impacto crítico en muchos aspectos, entre ellos, en la transparencia y rendición de cuentas sobre la toma de decisiones de TI en una entidad pública.

Exponiendo de una forma gráfica cómo podría estar configurada la estructura de gobernanza en una entidad:

5.3 Políticas, normas y procedimientos

El auditor necesita revisar las políticas de TI y verificar si están aprobadas por el comité de gobernanza sobre las TI, si cumplen con la normativa sobre seguridad, con las normas sobre protección de datos, si consideran los servicios en la nube y facilitan el logro de los objetivos de servicio de la entidad. Estas políticas deben estar soportadas por normas y procedimientos detallados que definan cómo se llevará a cabo el trabajo y se aplicarán las políticas.

Es importante diferenciar entre norma y procedimiento. Una norma indica "qué debe hacerse". Los procedimientos detallarán de forma clara y precisa cómo llevar a cabo las tareas y quién debe hacer cada tarea.

Las áreas que necesitan procedimientos bien documentados incluyen:

- Control interno: se puede realizar su seguimiento a través de cuadros de mando, informes de gestión, registros, actualizaciones de proyectos y requisitos de auditoría.
- Identificación, gestión y revisión continua de los riesgos de TI por parte de las principales partes interesadas y existencia de un sistema adecuado de comunicación con los órganos de gobernanza para garantizar la transparencia.
- Acceso a los datos, tratamiento y almacenamiento, con disposiciones específicas sobre el tratamiento de datos sensibles que se hayan recopilado para facilitar la prestación de un servicio público, por ejemplo, los registros de pacientes recopilados por un centro sanitario público.
- Prácticas de gestión de personal que soportan la estrategia TI.
- Procedimientos de seguridad de los sistemas de información de acuerdo con el ENS.

El auditor debe verificar si la política, las normas y los procedimientos están bien comunicados y entendidos por las partes interesadas, incluido el personal y los proveedores para su adecuado cumplimiento.

Por otra parte, la entidad deberá comprometer los recursos necesarios en la formación del personal y en desplegar los recursos TI necesarios para maximizar el valor de los servicios prestados.

Además, el auditor verificará si la política, las normas y los procedimientos se revisan y actualizan periódicamente para seguir siendo efectivos.

5.4 Estructura de control y dirección de la infraestructura de TI, los servicios y componentes organizativos

Al auditar una entidad pública grande y compleja, con distintas ubicaciones geográficas, se puede encontrar que las responsabilidades de gobierno y gestión de los sistemas de información (comunicaciones, sistemas, aplicaciones, copia de seguridad y continuidad de los servicios, etc.) puede estar muy fragmentada, recayendo en órganos diferentes, con poca o ninguna coordinación y cohesión entre ellos.

En estos trabajos, un auditor necesita evaluar cómo las complejas subestructuras están alineadas para optimizar los recursos dentro de la entidad. A tal fin, la auditoría debe examinar los requisitos de presentación de informes, los cuadros de mando y la información que cada uno de los sub-órganos de gobierno y dirección envía periódicamente al nivel de gobernanza apropiado y entrevistar al personal adecuado.

5.5 Personas, habilidades y competencias

Volviendo al ejemplo de una entidad pública que comienza el desarrollo de sistemas que permitan ofrecer a los ciudadanos servicios de administración electrónica avanzada o que trabaja para ampliar el catálogo de este tipo de servicios, un requisito importante para alinear la infraestructura y los servicios de TI con los nuevos objetivos de servicio es identificar las **brechas de competencias** y tomar las medidas adecuadas para abordar las necesidades de personal.

A menudo se subestiman las brechas de competencias y no se comprometen los recursos necesarios para gestionar nuevos proyectos.

Cuando se implementan planes de formación, el auditor de TI debe evaluar la adecuación del diseño, la entrega y la cobertura de los programas de formación para la fuerza laboral existente a la hora de utilizar los nuevos sistemas de TI y los procesos de negocio rediseñados.

Una entidad pública a menudo carece de la disposición o la capacidad para crear **nuevos perfiles** laborales y contratar a personas de acuerdo con planes preestablecidos, incluso cuando se reconocen las limitaciones de habilidades. Estas limitaciones podrían estar fuera del control de la entidad debido a la normativa existente o a la dependencia de entidades que tengan otras prioridades.

El auditor debe sopesar adecuadamente las circunstancias en las que opera la entidad, examinar qué medidas estratégicas han adoptado los órganos de gobierno de TI de la entidad para resolver esas limitaciones, y evaluar las mejores prácticas que han adoptado otras entidades similares en parecidas circunstancias, como contratar a un proveedor con habilidades tecnológicas adecuadas para un objetivo determinado, y si serían aplicables en la entidad auditada.

Conviene recordar que la nueva GPF-OCEX 1315R/NIA-ES 315R, requiere que el auditor conozca entorno de TI relevante para los flujos de transacciones y el procesamiento de la información en el SI de la entidad porque la utilización de aplicaciones de TI u otros aspectos del entorno de TI pueden dar lugar a **riesgos derivados de la utilización de TI**. Y que como componente fundamental del entorno TI está 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.[11]

De acuerdo con la GPF-OCEX 1315R/NIA-ES 315R (apartado A133), conocer el sistema de información de la entidad también incluye conocer los recursos que la entidad va a utilizar en las actividades de procesamiento de la información. La información acerca de los recursos humanos que participan, que puede ser relevante para el conocimiento de los riesgos para la integridad del sistema de información, incluye:

a) la competencia profesional de las personas que realizan el trabajo;

b) si se dispone de los recursos adecuados y

c) si hay una adecuada segregación de funciones.

[11] Ver apartado 31 de la GPF-OCEX 1316 Revisada.

5.6 Monitorización/seguimiento del desempeño/rendimiento

Como parte de sus responsabilidades, el órgano de gobierno corporativo debe llevar a cabo un seguimiento del rendimiento con arreglo a las metas de rendimiento interno, los objetivos de control interno y los requisitos externos.

Estas actividades de supervisión del rendimiento pueden ser llevadas a cabo por el grupo de auditoría interna o de garantía de la calidad, que comunicaría periódicamente sus resultados a la dirección, que a su vez informa a los órganos de gobierno corporativo.

La función del auditor podría ser evaluar si se establecen indicadores de rendimiento apropiados, y si la presentación de informes periódicos da a los órganos de gobierno una visión clara de la naturaleza de la alineación de las actividades de TI con los objetivos de servicio de la entidad pública.

6. Riesgos asociados a una gobernanza sobre las TI inadecuada

El seguimiento continuo, el análisis y la evaluación de las métricas asociadas con las iniciativas de gobernanza sobre las TI requieren una visión independiente y equilibrada para facilitar la mejora de los procesos de TI. Las decisiones, aparentemente adecuadas, de TI tomadas por una entidad pública para mejorar sus servicios a menudo no ofrecen los beneficios esperados debido a las deficiencias en la estructura o los elementos de la gobernanza sobre las TI vistos en la sección anterior.

El auditor puede observar que los recursos comprometidos no se han proporcionado de acuerdo con el calendario previsto de un proyecto, que los órganos superiores de la entidad se desentienden de la toma de decisiones en materia de TI, que los datos de referencia utilizados por la entidad pública son inadecuados y conducen a que los proyectos de TI incumplan o incurran en sobrecostes y desvíos de calendario, al tiempo que contribuyen poco a los resultados relacionados con la misión de la entidad, etc.

La auditoría puede desempeñar un papel importante en la mejora de la gobernanza sobre las TI en una entidad pública al proporcionar recomendaciones que mitiguen los riesgos asociados con uno o más elementos de la gobernanza sobre las TI.

El auditor de TI debe conocer los riesgos derivados de la falta de una gobernanza adecuada sobre las TI, identificar los elementos clave que son inadecuados y hacer recomendaciones pertinentes para su subsanación.

Los escenarios habituales en los que se presentan estos riesgos incluirían:

6.1 Estructuras informáticas fragmentadas y duplicadas

El auditor puede encontrar que en las grandes entidades públicas que proporcionan un amplio conjunto de diferentes servicios, la infraestructura de TI puede haber evolucionado de una manera que está fragmentada en varias divisiones y ubicaciones que atienden a necesidades distintas.

Gran parte de la infraestructura y las aplicaciones informáticas pueden haberse implantado en diferentes períodos a lo largo del tiempo y gran parte del gasto descentralizado se dedica ahora al mantenimiento y la continuidad de las operaciones de estos sistemas, que funcionan en silos con poco margen para compartir información o infraestructura operativa.

Por ejemplo, una aplicación de propósito específico como la compra de material sanitario puede no tener ninguna interfaz con la aplicación de contabilidad, de forma que no es posible consultar el crédito disponible y contabilizar de manera automática los pedidos y pagos realizados.

El auditor examinará cómo, sin una autoridad y supervisión centralizada, la entidad garantiza que las inversiones en TI se están coordinando en toda la organización y que proporcionan una combinación adecuada de capacidades que apoyan las necesidades operativas, al tiempo que van eliminando los sistemas que trabajan en modo silo y evitan la fragmentación, superposición y duplicación innecesarias.

6.2 Las TI proporcionan una baja contribución al valor del servicio

El auditor puede identificar situaciones en las que las TI aportan poco o ningún valor a la consecución de los objetivos de la entidad a partir de la revisión de informes internos, documentación de lecciones aprendidas, actualizaciones del estado de proyectos, etc.

El siguiente paso sería tratar de identificar las principales condiciones que dieron lugar a tal escenario. En caso de nuevas adquisiciones, entrevistar a los jefes de TI en la entidad puede apuntar a deficiencias en la calidad del trabajo realizado por proveedores, incluso cuando la debilidad real puede haber sido una mala gobernanza del proyecto.

El auditor debe verificar la participación de las partes interesadas en la toma de decisiones en materia de TI, la calidad y puntualidad de la presentación de informes de gestión al comité de gobernanza sobre las TI y/o al comité de gobernanza de proyectos TI, la adecuación del personal cualificado comprometido con la estructura de gestión del proyecto, las propuestas tecnológicas presentadas al órgano de gobierno, o la adecuación de los datos de referencia para identificar las principales causas del bajo valor aportado por las TI.

6.3 Sistemas informáticos ineficaces o poco fáciles de usar

Los auditores pueden encontrar que las aplicaciones informáticas recién implantadas no cumplen con los requisitos funcionales de la entidad y provocan continuas peticiones para el desarrollo de nuevas funcionalidades en el sistema recién implantado, de alto coste y fuera del alcance previsto, para cubrir necesidades que los sistemas previos ya tenían satisfactoriamente cubiertas.

Esto podría ocurrir ya sea debido a la participación limitada de los responsables funcionales de los procesos de negocio y los usuarios en la definición de los requisitos, en el diseño de la experiencia del usuario, o en la etapa UAT[12]; también puede deberse a aspectos relacionados con la gestión y gobernanza del proyecto, por ejemplo, la presentación de informes inadecuados de problemas críticos por parte del equipo de gobierno del proyecto al comité de gobernanza sobre las TI con objeto de cumplir los hitos previstos en el proyecto o debido a la mala supervisión del proveedor.

6.4 Gestión ineficaz de los recursos de TI

El auditor puede encontrar que la entidad pública no es capaz de priorizar eficazmente el gasto en TI y tomar buenas decisiones de inversión.

Por ejemplo, la entidad auditada puede no hacer un uso coherente de las soluciones TI de gestión y ocasionar costes adicionales. El auditor también puede observar que algunas entidades públicas no optan por plataformas públicas desarrolladas para optimizar el gasto público en TI, aunque los documentos de política pueden prever tales estrategias de reutilización.

Las entidades individuales pueden verse limitadas por sus requisitos operativos o por la falta de recursos humanos adecuadamente capacitados en TI para poder realizar esta transición a las plataformas comunes y continúan trabajando con sistemas TI heredados.

Estos escenarios de utilización subóptima de recursos de TI pueden ser comunes en los servicios públicos, y pueden abordarse mediante los compromisos apropiados de las partes interesadas, la planificación adecuada de necesidades de personal y la reutilización de los recursos de TI existentes.

6.5 Proyectos fracasados

Los proyectos de TI públicos a menudo no ofrecen las funcionalidades necesarias, no están alineados con los objetivos de servicio de las entidades, se enfrentan a problemas contractuales, a problemas de gestión de alcances y de gestión del cambio que amplían indebidamente las fases de desarrollo o no cumplen con los estándares mínimos de seguridad y arquitectura que son cada vez más importantes en un escenario de servicios basados en la web en las entidades públicas.

[12] Prueba de aceptación del usuario.

Además, estos proyectos pueden incurrir en costes adicionales para mantener y administrar sistemas y aplicaciones no estándar.

Algunas entidades reducen el riesgo de fracaso en nuevos proyectos mediante la realización de amplias consultas con la industria, la metodología de desarrollo ágil, el aplazamiento de la adquisición de hardware y la puesta en marcha de proyectos piloto en ubicaciones seleccionadas.

Para evaluar las causas del fracaso en los proyectos de TI o para obtener garantías sobre los proyectos de TI bien gobernados en una entidad pública, el auditor necesita acceder a casos de negocio e informes de proyectos detallados para comprender lo que el proyecto pretende ofrecer.

El siguiente requisito es evaluar la calidad de la **gobernanza del proyecto**: en términos de recursos comprometidos, elaboración de hitos realistas, estimación de los requisitos de recursos técnicos, compromiso de los usuarios finales para elaborar requisitos funcionales y reingeniería de procesos empresariales, si los hay. El auditor debe evaluar la calidad y la frecuencia del seguimiento del progreso, la identificación de problemas críticos, sus propuestas de resolución y lo que el equipo de gobernanza del proyecto informa al Comité de gobernanza sobre las TI o al órgano de gobernanza equivalente.

6.6 Gasto en TI que es desconocido, excesivamente alto o insuficiente

Estas situaciones se producen cuando una gran entidad pública o varias entidades tienen múltiples centros de costes responsables del gasto en necesidades específicas de TI o mantenimiento, sin una estructura central de gobierno que apruebe todos los gastos de TI o porque las unidades de negocio dentro de la entidad no están clasificando adecuadamente los costes relacionados con TI.

El auditor de TI que se enfrenta a este escenario debe evaluar el papel desempeñado por el mecanismo de gobernanza existente en la entidad y la adecuación de los informes de gestión para permitir una mejor visibilidad de las inversiones en TI.

En estas situaciones, sería importante que la entidad restableciera sus prioridades de TI, identificara proyectos o sistemas de TI heredados que no están contribuyendo de manera eficiente a cumplir los objetivos y que la alta dirección tome decisiones basadas en la cartera de TI en su conjunto.

6.7 Exposición a riesgos de ciberseguridad y privacidad, como la pérdida de datos y las violaciones de seguridad

Una organización que no tiene controles, estructuras, procesos y políticas de ciberseguridad adecuados corre un mayor riesgo de incidentes y brechas de ciberseguridad y privacidad. Estos riesgos incluyen, entre otros, la apropiación indebida de activos, la divulgación no autorizada de información, el acceso no autorizado, la vulnerabilidad a ataques lógicos y físicos, la interrupción y la indisponibilidad de la información, el uso indebido de la información, el incumplimiento de las leyes y regulaciones sobre protección de datos personales y la incapacidad de recuperarse ante desastres que afecten al entorno TI.

Los ciudadanos requieren una mayor garantía de que las entidades públicas implementan controles adecuados para garantizar la protección de los datos personales, los datos de gestión y cumplen con las prácticas de buena gobernanza en su entorno operativo.

Las estructuras de gobernanza de ciberseguridad de una organización deben incluir políticas, normas y procedimientos para administrar y monitorizar las medidas de ciberseguridad y privacidad de la organización. Estos documentos deben comunicar las prioridades, los recursos disponibles, la tolerancia general a los riesgos de ciberseguridad e incluir información sobre el marco de gestión de riesgos de ciberseguridad de la entidad.

El auditor debe revisar los documentos de políticas, normas, procedimientos, matrices de privilegios de usuario, registros de acceso (logs), informes de revisión de registros, informes de respuesta a incidentes y arquitectura de seguridad para obtener garantías sobre la naturaleza del liderazgo que proporciona el comité de seguridad de la información para hacer cumplir los controles relacionados con la ciberseguridad en un entorno de aumento de los servicios basados en la web prestados por entidades públicas.

El auditor debe examinar si las políticas de seguridad, las prácticas y los manuales de formación comunican

claramente las prioridades de protección de datos, la tolerancia general a los riesgos de ciberseguridad y los mecanismos de seguimiento. Estas políticas, entre otras cosas, deben incluir planes y procedimientos de continuidad de las actividades en caso de un ataque disruptivo de ciberseguridad. El auditor también debe verificar si la entidad compromete recursos adecuados para implementar estas políticas.

En esta materia se atenderá a lo contenido en la GPF-OCEX 5313, 5314 y el ENS.

6.8 Deficiente prestación de servicios públicos

El auditor puede encontrar que la entidad pública no ha hecho el mejor uso de la tecnología para la prestación de sus servicios. Si bien la alta dirección puede aludir a la falta de fondos, este escenario a menudo se desencadena por una cultura de planificación de TI inadecuada. Como resultado, los servicios públicos prestados por la entidad no cumplen con las expectativas de los ciudadanos.

El auditor puede examinar si la entidad ha actualizado periódicamente su estrategia de TI, si ha considerado opciones tecnológicas y ha creado casos de negocio /estudios de viabilidad apropiados para apoyar la toma de decisiones de TI. También puede examinar si la calidad de los servicios prestados se ha visto limitada por la falta de recursos informáticos o la incapacidad de la entidad para reutilizar los recursos existentes.

Una forma de mitigar este riesgo es tener una estrategia de TI y actualizarla periódicamente, que identifique recursos y planes para satisfacer las necesidades futuras de la organización.

6.9 Dependencia de terceros (proveedores)

Si las políticas que rigen el proceso de adquisición y externalización de TI son inadecuadas, la organización podría enfrentar una situación en la que depende completamente de un proveedor o contratista.

7. Cómo puede el auditor evaluar si existe una adecuada gobernanza sobre las TI

Tal como requiere el apartado 21.a) de la GPF-OCEX 1315R/NIA-ES 315R uno de los primeros pasos que el auditor debe dar en una auditoría consiste en aplicar procedimientos de valoración del riesgo para obtener **conocimiento del entorno de control** de la entidad auditada y de su estructura de gobierno, uno de cuyos elementos principales según el apartado A108 de la misma norma es la gobernanza sobre las TI.

Para ello el auditor revisará la situación de una serie de componentes clave de la gobernanza de TI de interés para la auditoría. Son aquellos factores que determinan la alineación estratégica y operativa de TI con los objetivos de negocio o de servicio de la entidad y que se deben conocer y evaluar para determinar si las decisiones de TI, los recursos y el seguimiento del desempeño respaldan las estrategias y objetivos de la organización.

Para llevar a cabo la evaluación de la gobernanza sobre las TI el auditor debe ser consciente de los riesgos asociados a la insuficiencia de cada uno de sus componentes en la entidad auditada, y que se han detallado en el apartado anterior.

Aunque en todo caso dependerá del tamaño, complejidad de las actividades y otras circunstancias de la entidad, para analizar si existe una adecuada gobernanza sobre las TI el auditor podrá atender a las siguientes áreas[13]:

7.1 Estrategia de TI

Objetivo de auditoría: Comprobar si existe una estrategia de TI, que incluya procesos para garantizar la alineación de los objetivos de servicio y los objetivos de TI.

Criterio: Existe un documento de estrategia de TI, que incluye un plan estratégico y procesos, en los que las funciones de TI se han alineado con los objetivos de negocio. Este documento se revisa y actualiza periódicamente.

Información a solicitar	Procedimientos de auditoría
Plan estratégico TIC (o equivalente)	Revisar el documento para determinar si los objetivos de TI están alineados con los objetivos del negocio, incluida la forma en que TI agrega valor a la organización.
Actas de las reuniones del Comité de gobierno TIC o equivalente.	Revisar las órdenes del día para confirmar que son coherentes con la estrategia y el mandato de TI. Revisar las actas para confirmar que las reuniones se han celebrado según lo previsto, que se siguió el orden del día y que los miembros asistieron habitualmente. Revisar las actas para verificar que las decisiones estratégicas se toman únicamente a nivel estratégico.
El mecanismo de aprobación de los presupuestos y/o proyectos TIC	Revise los procesos de aprobación del presupuesto/proyectos de TI para determinar que los procedimientos de aprobación de proyectos de TI vigentes son inequívocos, involucran a todas las partes interesadas relevantes y están alineados con los objetivos definidos en el plan estratégico de TI.
Requisitos/propuestas de los responsables funcionales.	Entrevistar a los responsables funcionales para evaluar si sus necesidades están alineadas con los objetivos de la entidad y se consideran adecuadamente en el desarrollo de la estrategia de TI.

7.2 Estructura de la Gobernanza sobre las TI

Objetivo de auditoría: Evaluar si existe una estructura de gobierno sobre las TI adecuada para permitir a la organización cumplir sus objetivos de TI.

Criterios: Las estructuras de gobierno de TI como la del comité de gobierno TIC, compuestas por miembros de la alta dirección, se ubican en un nivel estratégico dentro de la organización. Las funciones y responsabilidades de esas estructuras (comités/funcionarios individuales) están claramente definidas, incluidas las del director de TI, del responsable de seguridad de la información o equivalentes.

Información a solicitar	Procedimientos de auditoría
Organigrama	Revisar el organigrama general y documentos equivalentes para determinar que las estructuras de gobierno sobre las TI están posicionadas a un nivel estratégico. Determinar si la estructura de gobierno de TI se establece adecuadamente con los miembros de la dirección de la entidad.
Documentos reguladores del comité de gobierno TIC	Revisar los documentos (normas/políticas) que regula los comités de gobierno de TI para determinar si las funciones y responsabilidades han sido claramente definidas, comunicadas y los responsables funcionales están suficientemente representados.
Actas del comité de gobierno TIC	Revisar las actas de las reuniones para ver si el comité de gobierno TIC está desempeñando adecuadamente las funciones y responsabilidades definidas.

[13] Basado, fundamentalmente, en Guidance on Audit of IT Management functions: IT Governance, Contracts & Sustainability de INTOSAI Working Group on IT Audit, publicado en 2022.

7.3 Políticas, normas y procedimientos

a) *Objetivo de auditoría: Evaluar si la organización tiene políticas, normas y procedimientos adecuados, están aprobados y actualizados para guiar sus funciones de TI.*

Criterio: La organización documenta, aprueba y comunica las políticas, normas y procedimientos de TI adecuados para guiar las funciones de TI.

Información a solicitar	Procedimientos de auditoría
Políticas de TI (política de seguridad de la información, política de desarrollo y adquisición de software, etc.). Normas y procedimientos que complementan la política de seguridad aprobada. Correos electrónicos y materiales para comunicar las políticas y normas de TI.	Revisar las políticas de TI para verificar si están aprobadas, están actualizadas, completas y reflejan las necesidades de la entidad. Revisar si las políticas, normas y procedimientos se han comunicado adecuadamente a las partes interesadas y son accesibles. Revisar el historial de control de cambios de políticas para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos

b) *Objetivo de auditoría: Evaluar si la organización cuenta con mecanismos adecuados para garantizar el cumplimiento de las políticas, normas y procedimientos de TI.*

Criterio: La organización tiene un mecanismo de cumplimiento para garantizar que todas las políticas, normas y procedimientos sean seguidos por los usuarios.

Información a solicitar	Procedimientos de auditoría
Las políticas TI, las normas, los procedimientos, y materiales de formación para comunicar dichas políticas y procedimientos.	Seleccionar una muestra de políticas, normas y procedimientos para evaluar el cumplimiento. Entrevistar al personal de cumplimiento para analizar los mecanismos de seguimiento y sus logros.
Informes de cumplimiento, sistema de gestión de la información, auditoría Interna e Informes de Garantía de Calidad.	Revisar los informes de cumplimiento para comprobar los incumplimientos detectados y las medidas adoptadas al respecto. Revisar las actas de las reuniones del comité corporativo sobre las TI para ver si las cuestiones de cumplimiento de alto nivel se discuten a nivel estratégico. Verificar que las medidas adoptadas para solventar los incumplimientos detectados han impedido que se repitan y, en caso contrario, analizar los motivos. Verificar si las acciones tomadas fueron suficientes para evitar la recurrencia.

c) *Objetivo de auditoría: Evaluar si la gobernanza sobre las TI ha garantizado el cumplimiento de los requisitos legales y reglamentarios.*

Criterio: La organización tiene un proceso establecido para obtener y actualizar los requisitos específicos de TI, legales y regulatorios, y asegurar su cumplimiento.

Información a solicitar	Procedimientos de auditoría
Reglamentos internos relacionados con las descripciones de puestos de trabajo.	Evaluar si los requisitos legales y reglamentarios aplicables han sido identificados por la entidad y las normas internas con las descripciones de puestos son conformes con estos.
Normativa interna relacionada con la seguridad informática.	Revisar si las normas internas relacionadas con la seguridad de TI cumplen con los requisitos legales y reglamentarios.
Normas internas relacionadas con la privacidad de los datos.	Evaluar si las normas internas relacionadas con la privacidad de los datos cumplen con los requisitos legales y reglamentarios.
Normas internas sobre compras de TI y contratación de servicios.	Comprobar si las normas internas cumplen con las directrices específicas de cada país.

Información a solicitar	Procedimientos de auditoría
Política de comunicaciones y operaciones informáticas.	Evaluar si la política para las operaciones de comunicaciones y TI cumple con los requisitos legales y reglamentarios.

7.4 Estructura de control y dirección de la infraestructura de TI, los servicios y componentes organizativos

Objetivo de auditoría: Evaluar si la estructura de control y dirección de la infraestructura de TI está fragmentada, lo que conlleva el riesgo de duplicación y un uso subóptimo de los recursos.

Criterio: La organización cuenta con una estructura de control y dirección centralizada y un canal de aprobación para garantizar que las decisiones estratégicas relacionadas con la infraestructura y los servicios de TI se tomen en los niveles adecuados para optimizar el uso de los recursos de TI.

Información a solicitar	Procedimientos de auditoría
Organigramas y documentos que definen funciones y responsabilidades.	Revisar el organigrama y los documentos que establecen los comités de gobernanza sobre las TI para determinar si las funciones y responsabilidades definen los poderes de decisión y las delegaciones correspondientes.
Presupuesto de TI/procedimientos de aprobación de proyectos.	Revisar los procesos de aprobación del presupuesto y de proyectos de TI para determinar que la aprobación de los presupuestos y proyectos estratégicos y de alto nivel relacionados con la infraestructura y los servicios de TI se realizan solo en los niveles apropiados.
Estructura de TI departamental y decisiones adoptadas. Informes contables de los gastos en TIC hecho por los distintos departamentos y servicios.	Entrevistar a una muestra de personal clave en todos los departamentos y servicios para determinar el grado de armonización y control centralizado en la toma de decisiones. Comprobar la información contable relativa a los gastos de mantenimiento de TI de los distintos servicios para verificar si todos los gastos de TI se registran correctamente, son trazables y están disponibles de forma centralizada para el comité de gobierno TIC.

7.5 Personas, habilidades y competencias

Objetivo de auditoría: Evaluar si hay personal de TI suficientemente cualificado y capacitado para desempeñar las funciones de TI.

Criterio: La organización tiene un plan para satisfacer sus necesidades actuales y futuras de personal de TI.

Información a solicitar	Procedimientos de auditoría
Estrategia de TI.	Revisar el documento de estrategia de TI para determinar si contiene una estrategia para garantizar los recursos de TI presentes y futuros y dónde se identifican las lagunas de habilidades que llevan a la entidad a involucrar estratégicamente recursos de terceros.
Política de recursos humanos y formación para el personal de TI.	Revisar las políticas para determinar si están aprobadas y son actuales y completas. Revisar la política de recursos humanos y los documentos relacionados para comprobar si los requisitos de cualificación están claramente definidos. Revisar la política de formación de TI y los documentos relacionados para comprobar si los requisitos de formación sobre TI están claramente definidos.
Planes y prácticas de contratación.	Verificar que los planes y prácticas para la contratación de personal para comprobar si están en sintonía con la estrategia de TI y los requisitos actuales.
Planes y prácticas de formación de TI.	Comprobar que los planes y prácticas de formación de TI están en sintonía con la estrategia de TI y las necesidades de capacitación actuales.

7.5 Monitorización/seguimiento del desempeño/rendimiento

Objetivo de auditoría: Evaluar si se han establecido indicadores de desempeño y la comisión de gobierno TI ha definido un mecanismo de comunicación adecuado que la dirección utiliza para informarles de estos indicadores.

Criterio: La organización ha establecido indicadores (KPIs, Key Performance Indicators) a nivel estratégico para evaluar el valor derivado de las decisiones y procesos de TI.

Información a solicitar	Procedimientos de auditoría
Indicadores de desempeño (*KPIs*).	Revisar las medidas de rendimiento para garantizar que cubren tanto los indicadores de servicio como los de TI, evalúan la efectividad de las prácticas de TI e incluyen métricas y puntos de referencia adecuados.
Informes de estado disponibles con los órganos de gobierno de proyectos.	Revisar el proyecto, los informes de estado (u otra documentación que contenga el estado del proyecto (actas de reunión, correos electrónicos, etc.)) para asegurar que contiene los indicadores que permiten realizar el seguimiento de los costes, el calendario y las desviaciones sobre lo previsto.
Actas de la comisión de gobierno TI en las que se revisen los KPIs.	Revisar una muestra de decisiones de gestión de TI adoptadas, para asegurar que son claras y están bien fundamentadas y libres de ambigüedades.

8. Bibliografía

INTOSAI Working Group on IT Audit

- Governance Evaluation Techniques for Information Technology, 2016.
- Manual sobre auditoría de TI para EFS, Revisión 2022.
- Guidance on Audit of IT Management functions: IT Governance, Contracts & Sustainability, 2022.

ASOCEX

- GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).
- GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).
- GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría
- GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica.

OTROS

- AENOR, UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información (TI).
- AFAI-ISACA/CIGREF/IFACI, Guide d'audit de la gouvernance du système d'information de l'entreprise numérique, 2019.
- The Institute of Internal Auditors, Auditing IT Governance, 2020.
- Fundación para la investigación sobre el Derecho y la Empresa, Plan "5-25" Para la mejora de la Gobernanza de las Empresas Públicas en España, 2019.