## Guía práctica de fiscalización de los OCEX

## GPF-OCEX 5331 Gobernanza corporativa, gobernanza de 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 y actualizada el 11/12/2024*



### 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.

Interesa resaltar cómo las NIA-ES distinguen claramente entre gobierno corporativo y dirección, con diferentes responsabilidades y funciones (ver más adelante las definiciones de la NIA-ES-SP 1260).

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, el *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.

## 2. Por qué es importante para el auditor conocer la estructura de gobierno y dirección de la entidad, incluida la gobernanza de 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.

Continúa señalando la GPF-OCEX 1315R/NIA-ES 315R citada en su 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 de 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.

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 al conocimiento de la gobernanza corporativa y sobre las TI.**

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.

Un auditor de los OCEX puede necesitar analizar la situación de la gobernanza de 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 los controles generales de TI (CGTI), tal como establece la GPF-OCEX 5330.

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

Hemos visto que de acuerdo con la GPF-OCEX 1315R/NIA-ES 315R el auditor debe obtener un conocimiento suficiente del diseño y la implementación de las prácticas de gobernanza de 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 área pueden estar relacionadas con mecanismos de gobernanza inadecuados**.

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

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

La auditoría puede desempeñar un papel importante en la mejora de la gobernanza de las TI en una entidad pública ya que el auditor de TI podrá identificar los riesgos derivados de la falta de una gobernanza adecuada sobre las TI, los elementos clave que son inadecuados y hacer recomendaciones pertinentes para su subsanación.

## 3. Qué es la gobernanza corporativa o gobierno de la entidad

Aclaremos en primer lugar qué debe entenderse por **gobierno de la entidad**, término utilizado por las NIA-ES-SP, 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.

La NIA-ES-SP 1260, en el apartado 10, define a la "**Dirección**" como la "persona o personas con responsabilidad ejecutiva para dirigir las operaciones de la entidad. En algunas entidades de determinadas jurisdicciones, la dirección incluye a algunos o a todos los responsables del gobierno de la entidad, por ejemplo, los miembros ejecutivos del consejo de administración".

En la misma NIA-ES-SP 1260 se define a los "**Responsables del gobierno de la entidad"** como la persona o personas u organizaciones con responsabilidad en la supervisión de la dirección estratégica de la entidad y con obligaciones relacionadas con la rendición de cuentas de la entidad. Ello incluye la supervisión del proceso de información financiera. En algunas entidades de determinadas jurisdicciones, los responsables del gobierno de la entidad pueden incluir miembros de la dirección, por ejemplo, los miembros ejecutivos del consejo de administración de una empresa del Sector Público o privado. En la consideración de esta definición en el Sector Público Español habrá de estarse a las normas que resulten de aplicación a la entidad según su naturaleza jurídica. Con carácter general, se entenderá que se refiere, al menos, a los miembros del órgano de administración o equivalente de la entidad auditada o a aquel otro que, de acuerdo con las competencias establecidas en la organización correspondiente, tenga similares funciones.

Continúa señalando el apartado A1 de la NIA-ES-SP 1260 que las estructuras de gobierno varían según la jurisdicción y el tipo de entidad de que se trate, reflejando los diferentes entornos culturales y normativos, y las características de dimensión y propiedad. Por ejemplo:

- En algunas jurisdicciones existe un consejo de supervisión (total o mayoritariamente no ejecutivo) separado legalmente del consejo ejecutivo (de dirección). En otras jurisdicciones, un sólo consejo (una estructura de "consejo único") tiene la responsabilidad tanto de las funciones de supervisión como de las funciones ejecutivas.
- En algunos casos, la totalidad o parte de los responsables del gobierno de la entidad participan en la dirección de la entidad. En otros, los responsables del gobierno de la entidad y la dirección son personas diferentes.
- En algunos casos, los responsables del gobierno de la entidad tienen la responsabilidad de aprobar los estados financieros de la entidad (en otros casos, es la dirección la que tiene esta responsabilidad).

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.

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 relativamente 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).

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

| Función | Definición | Órgano responsable | |
|---|---|---|---|
| **Gobierno de la entidad o gobernanza corporativa** | El sistema por el cual se dirigen y controlan las organizaciones.<br>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 aprobación 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 aprobar 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 |

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. |

Aunque en todo caso dependerá del tamaño, complejidad de las actividades y otras circunstancias de la entidad, para analizar si existe una adecuada gobernanza corporativa el auditor podrá utilizar la tabla de Anexo 1 Visión general de los principios de gobernanza para elaborar un programa de auditoría.

## 4. Qué es la gobernanza de las TI y por qué es importante

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 de 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 en materia de TI se tomen en función de las necesidades del negocio o actividad, y se sustenten en ellas.[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 que debemos entender por gobernanza de 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 TI o gobernanza de 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.

Los **beneficios** derivados de la existencia de una gobernanza de las TI diseñada adecuadamente incluyen[5]:

- Las estrategias de TI están alineadas con los objetivos de la organización.
- Los riesgos se identifican y gestionan adecuadamente.
- Las inversiones en TI están optimizadas para aportar valor a la organización.
- El rendimiento de TI se define, mide y supervisa utilizando métricas significativas.
- Los recursos de TI se gestionan de forma eficaz.

La alineación de los objetivos de la organización y las TI tiene más que ver con la gobernanza y menos con la tecnología. La gobernanza garantiza que se evalúen las alternativas, que la ejecución se dirija adecuadamente y que se supervisen el riesgo y el rendimiento.

Un gobierno de las TI eficaz contribuye a la eficiencia y eficacia del control. **A menudo, cuando los controles están mal diseñados o son deficientes, una causa raíz es una gobernanza de TI débil o ineficaz**.

---

[3] Capítulo 2.I.A de IT Audit Handbook, INTOSAI.

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

[5] Auditing IT Governance, TheIAI, 2018.

En la evaluación de los sistemas de gobernanza TI de las administraciones públicas debe prestarse una especial atención al carácter horizontal de algunas organizaciones o entidades que prestan servicios transversales y comunes al conjunto de la administración pública en la que se integran. La existencia de direcciones generales (o agencias) proveedoras de servicio TI para la totalidad de las entidades de una determinada administración exige un mecanismo de gobernanza que garantice la coordinación de necesidades y decisiones, evitando que el marco de gestión de la entidad TI de carácter horizontal, que por definición tienen un mayor conocimiento tecnológico, "sustituya" las decisiones de las restantes entidades que se convierten en "clientes".

La gobernanza de TI está directamente relacionada con la supervisión organizacional de los activos y riesgos de TI, lo que la convierte en una responsabilidad compartida de la alta dirección y el órgano de gobierno. La alta dirección lleva a cabo la dirección diaria que se alinea tácticamente con la orientación estratégica general del órgano de gobierno para garantizar el uso eficaz, eficiente y aceptable de los recursos de TI.

El diseño de la gobernanza de 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 TI 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. En el caso de entidades que prestan su servicio al conjunto de su administración pública, esta supervisión desligada de la gestión exige una mayor evaluación.

El mensaje importante es que **las decisiones críticas sobre TI 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.

**Cuanto mayor sea la entidad y más complejo sea el entorno TI más necesaria será la existencia de una gobernanza TI bien establecida.**

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

Para evaluar si las decisiones de TI, los recursos y el seguimiento del desempeño respaldan las estrategias y objetivos de la organización, los auditores deben comprender y evaluar los diferentes componentes de la gobernanza de las TI. 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 Estructura organizativa de la gobernanza de las TI*

#### *Gobernanza general sobre las TI*

Las estructuras organizativas juegan un papel clave en el proceso de toma de decisiones. Las cuestiones importantes relacionadas con la asignación de recursos, las inversiones y la priorización de los proyectos de TI son decididas por los órganos superiores y el comité de gobernanza de las TI. El auditor debe examinar si las funciones de los distintos órganos de gobierno y dirección de la entidad están claramente definidas y apoyadas con procesos que faciliten la toma de decisiones.

En particular, en las entidades horizontales proveedoras de servicios TI, el auditor debe revisar los mecanismos de coordinación con las organizaciones receptoras de sus servicios.

Al auditar una entidad pública grande y compleja, con distintas ubicaciones geográficas, el auditor 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.) pueden estar muy fragmentadas, recayendo en órganos diferentes, con poca o ninguna coordinación y cohesión entre ellos. En estos casos, **el**

[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.

**auditor debe evaluar si las distintas subestructuras organizativas están alineadas para optimizar los recursos dentro de la entidad**. Para ello es importante conocer bien cómo está organizado el departamento o los departamentos TI de una entidad y las dependencias jerárquicas.

Toda entidad de tamaño mediano o grande debería crear un ***comité de gobernanza de 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 clave, revisar la disponibilidad de fondos y tomar decisiones de inversión en TI comprometiendo los recursos necesarios. Es la pieza central de la estructura organizativa de las TI. Será el órgano encargado de la definición y supervisión de la estrategia sobre las TI en una entidad.

El comité de gobernanza de las TI debe ser determinante en la toma de las decisiones organizativas en las que se debe invertir en tecnología, así como en la aprobación de la forma para adquirir esta tecnología. Las decisiones de inversión que involucran las soluciones de desarrollo vs. compra o cloud vs. no cloud, son responsabilidad del comité de gobernanza de las TI, y generalmente se toman después de efectuadas las recomendaciones pertinentes por parte de los grupos o comités designados[7].

En el caso de organizaciones complejas caracterizadas por una entidad horizontal prestadora de servicios, el auditor verificará el grado de intervención en las decisiones de las organizaciones a las que se presta el servicio y en particular algunas decisiones de inversión. Puede resultar conveniente examinar la justificación para el empleo de soluciones de reutilización de soluciones TI que son aplicadas en otras administraciones, para solventar entornos de negocio semejantes mediante el recurso a centros de transferencia de tecnología.

En determinadas entidades, en función de su estructura organizativa y sus características propias, el comité de gobernanza de las TI puede delegar parte de sus funciones o contar con el apoyo de otros comités o comisiones, con mayor capacidad operativa y que puedan llevar a cabo una actividad más continua e intensa. Este enfoque organizativo puede ser válido también, siempre y cuando se encuentre formalizado, haya sido adecuadamente comunicado y, sobre todo, el comité de gobernanza de TI no delegue su responsabilidad sobre las TI.

***Gobernanza de la ciberseguridad***

Existe una relación directa entre la gobernanza de las TI y la gobernanza de la ciberseguridad. Mientras que la primera abarca todos los aspectos de TI (complejidad, innovación, optimización de recursos, etc.), la gobernanza de la ciberseguridad se encarga de los aspectos relacionados con la seguridad de la información (amenazas y su evolución constante, concienciación, recursos humanos y materiales, etc.). La gobernanza de la ciberseguridad forma parte de la gobernanza de las TI, por lo que no puede existir una adecuada gobernanza de la ciberseguridad sin una gobernanza de las TI bien definida.

La ciberseguridad se ha convertido en una prioridad para las organizaciones. Las entidades deben implantar sistemas de gestión continuada de la ciberseguridad que incluyen, además de políticas y procedimientos de seguridad y el cumplimiento normativo en esta materia, el establecimiento de una adecuada gobernanza de la ciberseguridad. Esta materia es tratada en la *GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría.*

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. En las entidades de pequeño tamaño el comité de gobernanza de 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 sistemas de información*[8] 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 sistemas de información que garanticen la alineación de la organización y medios de los sistemas de información 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.

[7] IT Audit Handbook, INTOSAI.

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

***Gobernanza de proyectos***

Un órgano separado de *gobernanza de proyectos TI*[9] 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]

En este sentido, se recomienda revisar por el auditor la implicación de las "entidades cliente" y el grado de participación en los procesos de preparación de so-luciones y de su posterior compra.

***Gobernanza del dato***

Adicionalmente, en la sociedad actual, los datos se han convertido en un activo fundamental, tanto para las personas como para las organizaciones. Con ello, surge un nuevo reto para las Administraciones públicas ya que, por una parte, deben convertirlos en un bien común, que sirva para potenciar la transparencia, el conocimiento y el desarrollo, y, por otra, han de utilizarlos para mejorar su funcionamiento, los servicios que prestan y la toma de decisiones. Para conseguir estos objetivos, es preciso disponer de un *gobierno del dato*, que garantice que estos se obtienen, gestionan y explotan de forma apropiada, definiéndose como *los mecanismos organizativos y técnicos dispuestos para obtener y tratar los datos conforme a los derechos de las personas, cumpliendo con los requisitos de calidad y orientándose al logro de los objetivos de la Administración de la entidad*.[11]

En las organizaciones complejas con entidades horizontales, el auditor debe verificar los mecanismos de coordinación dirigidos al conjunto de la organización que se dirijan a mejorar la calidad de los datos existentes, de modo que puedan ser utilizados de forma transversal.

El primer paso para realizar un buen gobierno del dato es definir y aprobar una política por parte del órgano de gobierno corporativo. El segundo paso consiste en desarrollar e implantar procedimientos operativos para implantar dicha política. Pero no todos los procedimientos a desarrollar serán nuevos, por lo que habrá que modificar algunos de los ya existentes. Por ejemplo, si las entidades ya han aprobado sus políticas de seguridad de la información y han desarrollado procedimientos sobre esta materia, es posible que sea necesario modificarlos dado que el gobierno del dato también incorpora un componente de seguridad del dato. Los procedimientos más relevantes que una organización tendría que desarrollar en esta materia son[12]:

- Procedimiento para la identificación y clasificación del dato.
- Procedimiento para medir la calidad del dato.
- Procedimiento para garantizar la trazabilidad del dato.

AENOR publicó en 2023 una serie de guías (ver apartado 8) sobre la gestión del dato y su gobierno.

***Gobernanza de la inteligencia artificial***

Finalmente, el auge de la inteligencia artificial y la preocupación sobre su uso incorrecto provoca que el establecimiento de una adecuada *gobernanza sobre la IA* sea una necesidad en aquellas entidades que hagan uso de esa tecnología. El nuevo Reglamento Europeo de Inteligencia Artificial (Reglamento (UE) 2024/1689, del

[9] El Plan de Digitalización de las Administraciones Públicas 2021 -2025 señala que el despliegue del plan requiere de un modelo de gobernanza que garantice la eficiencia en el control, dirección, ajuste y toma de decisiones para que avance en línea con los objetivos definidos y con el modelo estratégico de Administración digital planteado. La gobernanza se realizará a dos niveles:

Plan: Este primer nivel tiene como objetivo realizar un seguimiento, control y dirección de las líneas estratégicas del plan estratégico.

Proyectos: Cada proyecto contará con un modelo de gobernanza específico en función de sus características.

[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.

[11] Ordenanza tipo de gobierno del dato en la entidad local, Aprobada por la Junta de Gobierno de la FEMP, 28/11/2023.

[12] Auditoría Interna del Gobierno del Dato, Instituto de Auditores Internos de España, 2020.

Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de IA) establece nuevas exigencias en este sentido.

Cuando se utilicen herramientas de IA para el conjunto de la organización, el auditor debe verificar el proceso de toma de decisiones con el objeto de garantizar la comprensibilidad de los algoritmos por todos los intervinientes en el proceso de desarrollo de la herramienta, evitando que las decisiones sean tomadas exclusivamente por la entidad de gestión.

***Estructura general de la gobernanza***

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:


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 el adecuado funcionamiento de las estructuras de gobernanza de las TI.

***5.2 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*)[13] de la entidad pueden no ser adecuadas 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 (en el caso de organizaciones complejas con entidades horizontales este aspecto cobra singular importancia).

**El auditor debe examinar si existe un Plan Estratégico TI (PETI), documento de estrategia TI o sus componentes equivalentes[14], si satisface adecuadamente la necesidad de alinear las decisiones de TI con los objetivos de servicio de la entidad pública, si dispone de indicadores para su seguimiento y si este se realiza.**

Además, verificará la intervención de las entidades "clientes" en la adopción de las decisiones de mayor trascendencia en su esfera de negocio.

Para garantizar el éxito de un PETI es imprescindible realizar acciones de **control y seguimiento continuo**, de manera que se pueda realizar una evaluación de los logros alcanzados, detectar los riesgos para su cumplimiento y ejercer acciones para mitigarlos.[15]

---

[13] 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.

[14] En la práctica pueden darse casos de entidades que tengan una estrategia TI definida de forma independiente, en otros casos puede ser un capítulo de la estrategia general de la entidad y en otros pueden existir documentos de planificación parciales. En cada caso se valorarán esos documentos en el contexto de la entidad.

[15] En este sentido, véase a modo de ejemplo, el apartado 6 Control y seguimiento, del Plan Estratégico de Transformación Digital de la Administración de la Generalitat Valenciana, GEN Digital 2025.

El órgano competente para el control de la ejecución del PETI será *el comité de gobernanza de las TI*, en cuyo seno podrá formarse un *comité de seguimiento*, que se reunirá periódicamente y siempre que las necesidades de evaluación y seguimiento del plan lo requieran. Se deben elaborar informes para la evaluación y el seguimiento del plan, que incluirán el estado de ejecución de las acciones, con especial atención a determinados aspectos como:

- El estado general de las acciones previstas en el PETI.
- Su evolución en el tiempo y las medidas correctoras que fueran necesarias para su mejora.
- Los riesgos detectados en la ejecución y las medidas mitigadoras.
- Las adaptaciones necesarias, cuando se produzcan cambios sustanciales que modifiquen los objetivos estratégicos del plan o identifiquen nuevas necesidades y prioridades.
- La evaluación de aquellas nuevas propuestas que hubieran sido remitidas por los distintos departamentos de la entidad, individual o colectivamente.
- La propuesta de nuevas acciones.

Los informes periódicos del comité de seguimiento serán elevados para su discusión y validación formal al comité de gobernanza de las TI.

Además del análisis del PETI y su seguimiento, el auditor deberá revisar la existencia de un **Plan anual de proyectos TI.** El objetivo principal de este plan es la definición de una hoja de ruta concreta, con un horizonte temporal de un año, de los proyectos TI a realizar, y que combinará las iniciativas derivadas del plan estratégico con otros proyectos que la entidad debe acometer por diferentes motivos (por ejemplo, requerimientos normativos). En organizaciones complejas la definición de los proyectos requiere una especial implicación de las entidades perceptoras de las soluciones TI, extremo que será revisado por el auditor.

La planificación anual en materia TI es un proceso muy importante en el ámbito de la gobernanza de las TI, ya que permite plantear proyectos concretos que permitan alcanzar los objetivos marcados a nivel estratégico. En la planificación anual será más fácil ajustar y priorizar los proyectos a realizar en función de la disponibilidad de los recursos.

El plan anual de TI debe ser también objetivo de seguimiento, con el objetivo de identificar desviaciones frente a lo previsto, gestionar los riesgos identificados, redefinir las prioridades si es necesario, etc.

En materia de responsabilidades, suele ser habitual que la definición y seguimiento del plan anual de TI sea realizada por el responsable del departamento de TI y que las principales conclusiones derivadas de su seguimiento sean elevadas al comité de gobernanza.

De nuevo para el caso de organizaciones complejas con una entidad proveedora, resulta indispensable analizar los grados de responsabilidad entre la entidad provisora de servicios TI y las entidades perceptoras de servicios.

***5.3 Políticas, normas y procedimientos***

El auditor necesita revisar las **políticas de TI** y verificar si están aprobadas por el comité de gobernanza de las TI, u otro órgano competente, 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.

La política de TI es un documento de alto nivel que define conjunto de directrices que rigen la forma en que una organización gestiona las TI. Constituye la expresión formal del compromiso y liderazgo de la alta dirección con las TI. Debe ser aprobada por el órgano de gobierno de la entidad, debe ser un documento breve, dejando detalles técnicos para las normas que la desarrollan, debe ser revisada y actualizada periódicamente y debe ser accesible (**publicada y dada a conocer**) a los empleados y colaboradores de la organización.

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.
- Planificación y desarrollo de proyectos.
- Procedimientos de mantenimiento y de adquisición,
- Estudios de viabilidad,
- Gestión de los niveles de servicio,
- Uso de un organigrama de toma de decisión.
- Gestión de la calidad.
- 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. Este aspecto se trata específicamente en la GPF-OCEX 5314.

El auditor debe verificar si la política, las normas y los procedimientos están bien comunicados y entendidos por las partes interesadas de acuerdo con sus necesidades, 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 periódicamente y, en su caso, se modifican y aprueban según las necesidades** para seguir siendo efectivos.

***5.4 Recursos, personas, habilidades y competencias***

Conviene recordar que la nueva GPF-OCEX 1315R/NIA-ES 315R, requiere que el auditor conozca el entorno de TI relevante para los flujos de transacciones y el procesamiento de la información en el sistema de información de la entidad porque la utilización de aplicaciones de TI 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 los procesos que una entidad utiliza para respaldar las operaciones de negocio y para lograr la consecución de las estrategias de negocio.[16]

De acuerdo con la GPF-OCEX 1315R/NIA-ES 315R (apartado 25 y 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 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.

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

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

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.

***5.5 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.

**5.6 Gestión del riesgo**

Como se ha señalado anteriormente, una adecuada gobernanza de las TI puede proporcionar a las organizaciones beneficios que impactan positivamente en la consecución de sus objetivos. Sin embargo, una gobernanza mal implantada o que no funciona de manera adecuada es claramente perjudicial para el funcionamiento eficaz de las organizaciones.

Más allá de invertir en mera tecnología, las organizaciones han de hacer énfasis en que la tecnología adquirida impulse sus objetivos de negocio, es decir, esté alineada con los mismos. Esta alineación entre tecnología y negocio es la que hace posible que las entidades aporten el máximo valor posible y de la manera más eficiente. De otra manera, si la tecnología no funciona como habilitador para el desarrollo del negocio puede impactar negativamente en sus objetivos, con consecuencias como las que detalla el apartado siguiente.

Para asegurar que las TI se alineen con los objetivos de negocio, las entidades deben identificar, evaluar y atajar los riesgos asociados al uso de TI. Además de la identificación, análisis y tratamiento de los riesgos asociados, una adecuada gestión del riesgo incluirá su revisión periódica, de sus medidas correctoras y de los protocolos de comunicación de riesgos, fomentando en las organizaciones una cultura de concienciación y responsabilidad.

La auditoría deberá revisar estos aspectos.[17]

[17] Ver párrafo 20 de la INTOSAI GUID 5101 (Revised draft)-Guidance on audit of information security.

### 5.7 Cumplimiento normativo

La norma ISO 38500 recomienda, como principio de buen gobierno de las TI, el cumplimiento normativo (fundamentalmente con materias relacionadas con la seguridad, la protección de datos o la interoperabilidad) y la incorporación de estándares en los procesos de una organización.

Idealmente se debe disponer de un plan de cumplimiento normativo relacionado con TI, que integre todas las leyes externas y las normativas internas relacionadas con las TI. El liderazgo de los órganos de gobierno y dirección es fundamental y debe comenzar por asignar las responsabilidades relacionadas con el cumplimiento de la legislación y las normativas internas, manteniendo una actitud proactiva de cara a conocer, aplicar y supervisar el cumplimiento de todas las normas relacionadas con las TI.

## 6. Riesgos asociados a una gobernanza de las TI inadecuada

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 de 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.

En particular, conviene analizar el grado de implicación de los receptores de servicios TI en el proceso de toma de decisiones, puesto que la delegación a la entidad horizontal que gestiona la TI puede provocar riesgos de insatisfacción de los objetivos y sobrecoste en los recursos.

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

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. Este riesgo puede ser crítico en el caso de organizaciones complejas dependientes de una única entidad proveedora.

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.

Conviene analizar en este apartado la capacidad de reutilización de soluciones TI para necesidades de negocio semejantes en las diferentes entidades recepto-ras, por ejemplo, en el caso del área de subvenciones, con aplicaciones corporativas que permitan particularizar las singularidades de cada entidad.

Además, en la auditoría se analizará el grado de participación conjunta con otras administraciones públicas para el desarrollo de soluciones TI de características comunes, como ya está sucediendo en el caso de tecnologías sanitarias.

***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 de 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 de pruebas de aceptación del usuario; 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 de 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. En organizaciones complejas que cuentan con entidades horizontales prestadoras de servicios TI, el riesgo de priorización es más complejo de gestionar y, por tanto, la coordinación entre los diferentes agentes implicados exige mejores herramientas de preparación de la toma de decisiones, de modo que se evite el riesgo de toma de decisiones de inversión adoptadas sin la suficiente información, a las restantes entidades receptoras de los servicios e inversiones.

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.

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 de 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.

El presente riesgo está conectado con las decisiones de no reutilización de soluciones TI que provengan de otras administraciones o entidades TI, por lo que el auditor verificará la suficiente motivación para no acogerse a esta posibilidad y, por el contrario, adoptar la decisión de externalizar una solución presuntamente nueva, pero con altos grados de dependencia. El mismo análisis se puede realizar sobre la participación conjunta de varias administraciones en el desarrollo de tecnologías TI.

## 7. Cómo puede el auditor evaluar si existe una adecuada gobernanza de 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 de 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, 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 de las TI el auditor debe ser consciente de los riesgos asociados a la insuficiencia de cada uno de sus componentes en la entidad auditada, 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 de las TI el auditor podrá utilizar el programa de auditoría/cuestionario del Anexo 2, que se estructura en las áreas mencionadas en el apartado 5 anterior.

Este programa “base” se adaptará a las circunstancias particulares de cada auditoría.

## 8. Bibliografía

AENOR

- UNE-ISO 37000: 2022 Gobernanza de las organizaciones. Orientación.
- UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información (TI).
- UNE 077 Gobierno del Dato.

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.

Crue Digitalización, Comisión Sectorial de Digitalización de Crue Universidades Españolas

- Gobierno de las TI para universidades, 2011.
- Gobierno de las Tecnologías de la Información en universidades, 2009.

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.

OTROS

- Guide d'audit de la gouvernance du système d'information de l'entreprise numérique, AFAI-ISACA/CIGREF/IFACI, 2019.
- Auditing IT Governance, The Institute of Internal Auditors, 2018.
- Plan "5-25" Para la mejora de la Gobernanza de las Empresas Públicas en España, Fundación para la investigación sobre el Derecho y la Empresa, 2019.
- IT and Data Governance: Technology Spotlight, CPA Canada, 2019.

## Control de versiones

| Versión | Cambios |
|---|---|
| 19-10-2023 | Versión inicial |
| 04-11-2024 | Se subsanan varias erratas y se corrigen ligeramente algunas oraciones para que sea más comprensible el texto, sin alterar el sentido original del documento. También se eliminan algunas reiteraciones.<br>Se han reubicado varios párrafos de los apartados 1 y 2.<br>Se ha eliminado el último párrafo del apartado 2 por ser reiterativo.<br>Se han añadido nuevas definiciones en el apartado 3.<br>Se ha intercambiado el orden de los apartados 5.1 y 5.2<br>Se complementa el apartado actual 5.1 con una mención a la gobernanza del dato y de la IA por la importancia creciente que están adquiriendo en el sector público y se actualiza el gráfico.<br>En el apartado 5.3 se añade un párrafo definiendo la política de TI y un último párrafo con una referencia a la ciberseguridad.<br>El contenido del apartado 5.4 pasa a ser el segundo párrafo del apartado 5.2.<br>El apartado 5.5 pasa a ser el 5.4 ha enriquecido su título y cambiado el orden de los párrafos.<br>El apartado 5.6 pasa a ser el 5.5.<br>Se añade un nuevo apartado 5.6 sobre gestión del riesgo ya que es un elemento muy importante de la gobernanza.<br>Se añade un nuevo apartado 7 con referencia al cumplimiento normativo.<br>El programa de trabajo que estaba en el apartado 7 se ha revisado y pasado al anexo. Se ha simplificado el anexo fruto de la experiencia de su aplicación práctica desde la aprobación inicial de la guía.<br>El apartado 7 pasa a ser el 8.<br>Se han introducido varios párrafos a lo largo del texto para tener en cuenta los casos de entidades complejas que prestan servicios TI a otras entidades de la misma administración.<br>Apartado 8: Se ha completado la bibliografía.<br>Se crea un Anexo 1 nuevo. |

| Categoría | Descripción de la categoría | Principio | Declaración de principio |
|---|---|---|---|
| **Primario** | La búsqueda de un propósito está en el centro de todas las organizaciones y es de primordial importancia para la gobernanza de las organizaciones. Por lo tanto, este principio es la consideración principal para la gobernanza y el punto central de todos los demás principios de este documento. Todos los demás principios tienen que leerse en el contexto de la aplicación de este principio. | Propósito (6.1) | El órgano de gobierno debería asegurar que la razón de ser de la organización, con respecto a sus intenciones hacia el ambiente natural, la sociedad y las partes interesadas de la organización, esté claramente definida como un propósito organizacional. El órgano de gobierno también debería asegurar que el conjunto asociado de valores organizacionales esté claramente definido. |
| **Fundacionales** | Los cuatro principios fundacionales de gobernanza son la esencia para asegurar que se lleve a cabo una gobernanza eficaz de una organización.<br>El núcleo de la capacidad de gobernar eficazmente una organización es:<br>– determinar el enfoque de la organización para la generación de valor;<br>– dirigir y comprometerse con la estrategia para generar ese valor;<br>– supervisar que la organización se desempeñe y se comporte de acuerdo con las expectativas establecidas por el órgano de gobierno;<br>– demostrar responsabilidad por el desempeño, el comportamiento, las decisiones y las actividades de la organización. | Generación de valor (6.2) | El órgano de gobierno debería definir los objetivos de generación de valor de la organización de manera que cumplan con el propósito de la organización de acuerdo con los valores organizacionales y el ambiente natural, el contexto social y económico en el que opera. |
| | | Estrategia (6.3) | El órgano de gobierno debería dirigir y comprometerse con la estrategia organizacional, de acuerdo con el modelo de generación de valor, para cumplir con el propósito organizacional. |
| | | Seguimiento (6.4) | El órgano de gobierno debería dar seguimiento al desempeño de la organización para asegurarse de que cumpla con las intenciones y expectativas del órgano de gobierno para la organización, su comportamiento ético y sus obligaciones de *compliance*. |
| | | Rendición de cuentas (6.5) | El órgano de gobierno debería rendir cuentas por la organización en su conjunto y exigir que le rindan cuentas aquellos en quienes ha delegado. |

Fuente: Tabla 1 de la UNE-ISO 37000: 2022 Gobernanza de las organizaciones. Orientación.

## Anexo 1 Visión general de los principios de gobernanza

| Categoría | Descripción de la categoría | Principio | Declaración de principio |
|---|---|---|---|
| Facilitadores | Los seis principios facilitadores abordan las responsabilidades de gobernanza pertinentes a las organizaciones de hoy – para cumplir con las expectativas en evolución de las partes interesadas y el ambiente natural cambiante, el contexto social y económico. | Involucramiento con las partes interesadas (6.6) | El órgano de gobierno debería asegurar que las partes interesadas de la organización estén involucradas adecuadamente y que se consideren sus expectativas. |
| | | Liderazgo (6.7) | El órgano de gobierno debería dirigir la organización de manera ética y eficaz y asegurar dicho liderazgo en toda la organización. |
| | | Datos y decisiones (6.8) | El órgano de gobierno debería reconocer a los datos como un recurso valioso para la toma de decisiones por parte del órgano de gobierno, la organización y otros. |
| | | Gobernanza del riesgo (6.9) | El órgano de gobierno debería asegurarse de considerar el efecto de la incertidumbre sobre el propósito organizacional y los resultados estratégicos asociados. |
| | | Responsabilidad social (6.10) | El órgano de gobierno debería asegurar que las decisiones sean transparentes y estén alineadas con las más amplias expectativas sociales. |
| | | Viabilidad y desempeño a lo largo del tiempo (6.11) | El órgano de gobierno debería asegurar que la organización siga siendo viable y funcione a lo largo del tiempo, sin comprometer la capacidad de las generaciones actuales y futuras para satisfacer sus necesidades. |

Este documento proporciona aspectos clave de la práctica que guían a los órganos de gobierno en su aplicación de los principios de gobernanza. Estos aspectos clave no pretenden proporcionar una lista exclusiva de prácticas.

## *A. GOBERNANZA DE LAS TI*

### *1. Estructura organizativa de la gobernanza de las TI (ver apartado 5.1 de la GPF-OCEX 5331)*

**Objetivo de auditoría**: Evaluar si existe una estructura de gobierno sobre las TI adecuada al tamaño y complejidad de la entidad para permitir a la organización cumplir sus objetivos de TI, alineados con los objetivos generales

**Criterios**: Las estructuras de gobierno de TI como la del comité de gobierno sobre las TI, 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.

**Preguntas y procedimientos de auditoría**:

1.1 ¿Dispone la entidad de un organigrama general, reglamento de organización o documento equivalente en el que se determine la composición y ubicación de las estructuras de gobierno sobre las TI?

Sí: _____

No

*Solicitar el organigrama, reglamento interno o equivalente del conjunto del departamento TI.*

¿De quién depende el departamento de TI?

1.2 ¿Dispone la entidad de un comité de gobierno sobre las TI?

Sí: _____

No

Si existe, ¿ha sido la composición del comité de gobierno sobre las TI, las funciones y responsabilidades de sus miembros, claramente definidas y comunicadas?

Sí: _____

No

¿Los responsables funcionales están suficientemente representados?

Sí: _____

No

*Solicitar los documentos justificativos y revisar los documentos que regulan los comités de gobierno sobre las TI para determinar si las funciones y responsabilidades definen los poderes de decisión y las delegaciones correspondientes, han sido claramente definidas, comunicadas y los responsables funcionales están suficientemente representados.*

1.3 ¿Existe un liderazgo efectivo de los órganos de gobierno? (rector/consejo de gobierno?

*Constatar su materialización, cómo se refleja en la entidad.*

1.4 ¿Desempeña el comité de gobierno sobre las TI sus funciones adecuadamente? ¿Se reúne periódicamente?

Sí

No

*Solicitar actas de las reuniones celebradas y verificar si el comité de gobierno sobre las TI se reúne realmente y está desempeñando de forma efectiva las funciones y responsabilidades definidas.*

***2. Estrategia de TI*** *(ver apartado 5.2 de la GPF-OCEX 5331)*

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

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

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, con lo que se consigue optimizar el uso de los recursos TI.

**Preguntas y procedimientos de auditoría**:

2.1 ¿Dispone la entidad de un Plan Estratégico TI o documento equivalente que abarque el periodo auditado?

Sí: _____
No

¿El Plan Estratégico TI ha sido aprobado por el comité de gobernanza TI y/o órgano de gobierno de la entidad?

Sí: _____
No

¿Se recoge en el plan las necesidades presupuestarias para llevarlo a cabo?

Sí: _____
No

*Solicitar plan estratégico o documento equivalente y acuerdo de aprobación*

*Revisar el Plan Estratégico TI para determinar si los objetivos de TI están alineados con los objetivos del negocio.*

2.2 ¿Dispone el Plan Estratégico TI o documento equivalente de métricas o indicadores de desempeño?

Sí
No

En caso afirmativo, ¿son los indicadores seguidos y revisados periódicamente por el comité de gobernanza TI o por el órgano competente?

Sí
No

*Solicitar KPIs (indicadores de desempeño) utilizados para el seguimiento del Plan Estratégico TI.*

*Solicitar relación de informes de estado de proyectos (u otra documentación que contenga su estado, como actas de reunión, correos electrónicos, etc.) que se utilicen para el seguimiento del Plan Estratégico TI.*

*Solicitar relación de las actas de la comisión de gobierno TI o del comité de seguimiento que recojan el seguimiento de los KPIs definidos.*

2.3 ¿Se ha creado un Comité de seguimiento del Plan Estratégico TI?

Sí

No

Si existe, ¿cuál es su composición?

¿Se mantienen reuniones periódicas de revisión/seguimiento de cumplimiento del plan?

*Solicitar relación de actas y órdenes del día de las reuniones de revisión/seguimiento del plan vigente.*

*Revisar una muestra de las actas del Comité de seguimiento Plan Estratégico TI para confirmar que:*

*- las reuniones se han celebrado según lo previsto y los miembros asistieron habitualmente,*

*- las decisiones son coherentes con la estrategia TI.*

*Solicitar indicadores de cumplimiento de los objetivos.*

2.4 ¿Se alinean las necesidades de los distintos departamentos con los objetivos de la entidad y son consideradas adecuadamente en el desarrollo de la estrategia de TI?

Sí

No

*Describir brevemente el proceso y solicitar la documentación justificativa sobre el análisis de las necesidades de los distintos departamentos y cómo son atendidas.*

*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.*

*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.*

2.5 La aprobación de los proyectos estratégicos y presupuestos relacionados con la infraestructura y los servicios de TI se realiza solo en los niveles apropiados.

¿Existe un proceso de propuesta y aprobación de proyectos de TI, y de sus presupuestos, para determinar que estos proyectos, involucran a todas las partes interesadas relevantes, se priorizan y están alineados con los objetivos definidos en el plan estratégico de TI?

Por ejemplo, ¿existe un proceso formalizado y conocido por los usuarios funcionales para gestionar la cartera de proyectos?

Sí

No

¿Se dota de los recursos necesarios?

Sí

No

*Solicitar procedimientos relacionados el estudio y la aprobación de proyectos de TI y con la aprobación del presupuesto u otra documentación justificativa.*

*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.*

*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.*

2.6 ¿Dispone la entidad de un Plan de proyectos TI anual (Cartera de Proyectos o documento equivalente) que abarque el periodo auditado?

Para la confección del Plan de Proyectos / Cartera de Proyectos ¿se dispone de un procedimiento definido y adecuadamente formalizado y comunicado a todos los interesados?

¿Dispone el Plan Anual de TI o documento equivalente de métricas o indicadores de desempeño?

En caso afirmativo, ¿son los indicadores seguidos y revisados periódicamente por el comité de gobernanza TI o por el órgano competente?

2.7 ¿Se registran todos los gastos de TI correctamente, son trazables y están disponibles de forma centralizada para el comité de gobierno TIC?

Sí

No

*Solicitar la información contable relativa a los gastos TI.*

*Comprobar la información contable relativa a los gastos de mantenimiento de TI.*

## *3. Políticas, normas y procedimientos en materia de TI (ver apartado 5.3 de la GPF-OCEX 5331)*

***Respecto a las Políticas y normas relacionadas con las TI***

**Objetivo de auditoría**: Evaluar si la organización tiene políticas, normas (uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido) y procedimientos (cómo realizar las tareas habituales y quiénes son sus responsables) adecuados, están aprobados, actualizados y comunicados 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.

**Preguntas y procedimientos de auditoría**:

3.1 ¿Dispone la organización de normas y procedimientos TIC debidamente aprobados que se adapten a la realidad y necesidades de la entidad?

Sí

No

*Solicitar una relación de las normas aprobadas, indicando nombre, fecha de aprobación y órgano que la aprobó.*

*Revisar las políticas de TI para verificar si están aprobadas, están actualizadas, completas y reflejan las necesidades de la entidad.*

*Evidencia de su aceptación por empleados y colaboradores.*

*Revisar si las políticas, normas y procedimientos se han comunicado adecuadamente a las partes interesadas y son accesibles.*

3.2 ¿Se actualiza periódicamente la normativa interna en materia TI, de manera que se alineen con los objetivos de negocio y los requisitos normativas?

Sí

No

*Solicitar historial de cambios de los documentos solicitados y revisar si se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos*

***Respecto a los mecanismos para garantizar el cumplimiento de las políticas, normas y procedimientos TI***

**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.

**Preguntas y procedimientos de auditoría**:

3.3 ¿Dispone la entidad de mecanismos de seguimiento para asegurar que se cumplen las políticas y normas TI?

Sí

No

*Explicar brevemente los mecanismos implantados y aportar la documentación justificativa.*

*Entrevistar al personal encargado de supervisar el cumplimiento para analizar los mecanismos de seguimiento y sus logros.*

3.4 Respecto a los incumplimientos detectados ¿son tratados en las reuniones del comité de gobierno sobre las TI?

Sí

No

*Revisar las actas de las reuniones del comité de gobierno 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.*

## *4. Recursos, personas, habilidades y competencias (ver apartado 5.4 de la GPF-OCEX 5331)*

**Objetivo de auditoría**: comprobar si la organización asigna al departamento TIC y a la seguridad los recursos humanos y materiales necesarios para llevar a cabo sus tareas, y si estos son adecuados al tamaño de la entidad y 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 infraestructura y personal de TI.

**Preguntas y procedimientos de auditoría**:

4.1 El documento de estrategia de TI contiene una estrategia para garantizar los recursos de TI presentes y futuros y se identifican las lagunas de habilidades que llevan a la entidad a involucrar estratégicamente recursos de terceros.

Sí

No

*Revisar la política de recursos humanos y los documentos relacionados para comprobar si los requisitos de cualificación están claramente definidos.*

4.2 ¿Dispone la entidad de un plan de recursos humanos (PRH) que está en sintonía con la estrategia de TI?

Sí

No

*Solicitar y revisar el plan de recursos humanos para verificar que los planes y prácticas para la contratación de personal están en sintonía con la estrategia de TI y los requisitos actuales.*

*Solicitar y revisar documentación relacionada con los requisitos de cualificación necesarios para los puestos del departamento TI.*

4.3 ¿Dispone la entidad de una política o documento equivalente que define los requisitos de formación de los empleados en materia TI alineado con el plan estratégico TI o el PRH?

Sí

No

*Solicitar la política y los documentos relacionados para comprobar si los requisitos de formación sobre TI están claramente definidos y en sintonía con la estrategia de TI y las necesidades de capacitación actuales.*

4.4 ¿Dispone la entidad de los recursos humanos necesarios para cumplir adecuadamente con obligaciones con respecto a las necesidades TIC de la organización?

Solicitar información sobre:

| | **Año anterior** | **Año fiscalizado** |
|---|---|---|
| Número total de funcionarios/empleados al cierre del ejercicio. | | |
| Número de funcionarios/empleados tiempo completo (o equivalente) pertenecientes en al departamento de TIC al cierre del ejercicio. | | |
| Número de funcionarios/empleados tiempo completo (o equivalente) dedicadas a la seguridad TIC.<br>Señalar si están incluidas o no en los datos anteriores. | | |
| Número de personas contratadas a proveedores a tiempo completo que prestan servicio o asistencia al departamento TIC. | | |
| Número de personas contratadas a proveedores a tiempo completo que prestan servicio o asistencia al departamento TI dedicadas a la seguridad. | | |

*Solicitar documentación relacionada para analizar el número de personal a tiempo completo (o equivalente) pertenecientes en al departamento/área/negociado de gestión de las TIC de la entidad.*

4.5 ¿Dedica la entidad los recursos necesarios para cubrir sus necesidades TI y cumplir adecuadamente con sus obligaciones con respecto a las necesidades de la organización?

Solicitar información sobre:

| *(Cifras en miles de euros)* | **Año N** | **Año N+1** |
|---|---|---|
| Obligaciones reconocidas netas (ORN) totales de la entidad | | |
| ORN capítulo 1 del departamento TIC | | |
| ORN capítulo 2 del departamento TIC | | |
| ORN capítulo 6 del departamento TIC | | |
| ORN capítulo 1 del departamento TIC -SOLO SEGURIDAD | | |
| ORN capítulo 2 del departamento TIC -SOLO SEGURIDAD | | |
| ORN capítulo 6 del departamento TIC -SOLO SEGURIDAD | | |

*Se revisará la dotación presupuestaria de los Capítulos 1, 2 y 6 del departamento TIC.*

*Se revisará el total de ORN de los Capítulos 1, 2 y 6 del presupuesto.*

4.6 ¿Se registran todos los gastos de TI correctamente, son trazables y están disponibles de forma centralizada para el comité de gobierno TI?

### *5. Monitorización/seguimiento del desempeño/rendimiento (ver apartado 5.5 de la GPF-OCEX 5331)*

**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.

**Preguntas y 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.*

### *6. Gestión de riesgos (ver apartado 5.6 de la GPF-OCEX 5331)*

**Objetivo de auditoría**: evaluar si la entidad ha realizado y documentado un análisis sobre los riesgos operativos que afectan a cualquier sistema, servicio o proyecto TI.

**Criterio**: La organización ha establecido un sistema de gestión de riesgos TI de manera que estos son identificados y analizados antes de materializarse.

**Preguntas y procedimientos de auditoría:**

6.1 ¿Existe un sistema para la gestión de riesgos TI?

Sí

No

*Solicitar y revisar la documentación sobre el sistema de gestión de riesgos TI de la entidad.*

*Verificar que incluye los sistemas de información críticos de la entidad y que está actualizado.*

6.2 ¿Participa activamente la dirección/alta dirección en la gestión de riesgos, la definición de los criterios de aceptación del riesgo, de los niveles aceptables de riesgo y en la articulación de medidas para mitigarlos?

Sí

No

¿Cómo se materializa esa participación?

*Solicitar documentación justificativa.*

## *B. CUMPLIMIENTO NORMATIVO* *(ver apartado 5.7 de la GPF-OCEX 5331)*

### *1. Esquema Nacional de Seguridad*

**Objetivo de auditoría**: evaluar si existe un adecuado nivel de cumplimiento legal respecto al Esquema Nacional de Seguridad.

**Criterio**: Se han establecido las condiciones necesarias para garantizar el adecuado nivel de seguridad en los sistemas y aplicaciones empleados de acuerdo con el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

**Preguntas y procedimientos de auditoría:**

1.1 ¿La entidad ha formalizado un documento con la **declaración de aplicabilidad**, que recoge las medidas de seguridad que le son de aplicación en función del nivel y categoría del sistema, que además ha sido firmada por el responsable de seguridad?

Sí

No

1.2 ¿La entidad ha realizado la auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta?

Sí

No

En caso afirmativo, indicar la empresa que ha realizado la auditoría y los resultados del trabajo.

*Solicitar el informe de auditoría del ENS.*

1.3 ¿Los resultados de la auditoría y de la autoevaluación han sido revisados por el responsable de seguridad y las conclusiones presentadas al responsable del sistema para que adopte las medidas correctoras adecuadas?

Sí

No

1.4 ¿La entidad facilita los datos necesarios para el Informe del Estado de la Seguridad a través de la herramienta INES, cumpliendo así la Instrucción Técnica de Seguridad aprobada por resolución de 7 de octubre de 2016?

Sí

No

*Solicitar informe INES.*

1.5 ¿La entidad ha publicado en su sede electrónica las declaraciones de conformidad y los distintivos de seguridad correspondientes, según los resultados de la autoevaluación o auditoría?

Sí, indicar la URL.: _____

No

1.6 ¿La entidad ha aprobado y publicado en su sede electrónica la Política de Seguridad de la Información?

Sí, indicar la URL.: _____

No

## *2. Normativa de protección de datos de carácter personal*

**Objetivo de auditoría**: evaluar si existe un adecuado nivel de cumplimiento en materia de protección de datos de carácter personal

**Criterio**: Se han establecido las condiciones necesarias para garantizar el adecuado nivel de cumplimiento de los aspectos básicos de la normativa de protección de datos personales.

**Preguntas y procedimientos de auditoría:**

2.1 ¿La entidad ha designado un **Delegado de Protección de Datos (DPD)** y su nombramiento ha sido comunicado a la AEPD?

*Solicitar documento acreditativo del nombramiento y de la notificación a la AEPD*

2.2 ¿La entidad dispone del registro de actividades de tratamiento (RAT) con la información requerida por el RGPD?

Sí

No

*Solicitar RAT*

2.3 ¿La entidad ha realizado análisis de riesgo de los tratamientos de datos personales y evaluaciones de impacto para aquellos de riesgo alto?

Sí

No

*Solicitar registro de los análisis de riesgo realizados.*

2.4 ¿La entidad evalúa periódicamente la eficacia de las medidas técnicas y organizativas implantadas?

Sí

No

*Solicitar informes de auditoría para dar cumplimiento al requisito anterior.*

## *3. Esquema Nacional de Interoperabilidad*

**Objetivo de auditoría**: evaluar si la entidad cumple con los criterios y recomendaciones establecidos en el Esquema Nacional de Interoperabilidad.

**Criterio**: Se han establecido las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados de acuerdo con el RD 4/2010, de 8 de enero, por el que se regula el ENI en el ámbito de la Administración Electrónica.

**Preguntas y procedimientos de auditoría:**

3.1 ¿Dispone la entidad de un plan o estrategia de adecuación al ENI?

Sí
No

*Solicitar y revisar el plan de adecuación al ENI y su aprobación.*
*Revisar las medidas que establece el plan y si estas han sido aplicadas a los sistemas de la entidad.*

3.2 ¿Se han adecuado los sistemas a los criterios y recomendaciones establecidos en el ENI?

Sí
No

*Revisar si las aplicaciones utilizadas cumplen con los requisitos del ENI y las contrataciones exigen cumplir con el RD.*