La gobernanza en las entidades públicas, su importancia en el establecimiento de una sólida ciberseguridad y su auditoría

ESPERANZA PINAR LORENTE
Jefa de la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Cuentas de la Comunidad Valenciana

ANTONIO MINGUILLÓN ROY
Auditor director del Gabinete Técnico de la Sindicatura de Cuentas de la Comunidad Valenciana

RESUMEN

La gobernanza corporativa es el sistema por el cual se dirigen y controlan las organizaciones. Es un asunto del máximo interés para los auditores, ya que establece el tono directivo *(tone at the top)* de una organización y comprende tres de los cinco componentes de un sistema de control interno de acuerdo con el modelo COSO: el entorno de control, el proceso de valoración del riesgo, y el proceso de seguimiento.

Dentro del sistema de control interno y de gobernanza de las entidades públicas se encuentran la gobernanza de las TI y de la ciberseguridad, que deben estar integradas de forma coherente.

La gobernanza de las TI es un componente clave de la gobernanza corporativa, y es el sistema por el cual se dirige y controla el uso, actual y futuro, de las TI, alineando su uso con los objetivos de la organización.

En el contexto actual de la administración electrónica hiperconectada en el que deben actuar las instituciones de control, los riesgos de ciberseguridad adquieren una importancia crítica en la valoración de los riesgos.

La gobernanza de la ciberseguridad, que es una parte muy relevante de la gobernanza de las TI, consiste en el conjunto de responsabilidades y actividades que buscan proporcionar una dirección estratégica en esa materia, gestionar el riesgo y garantizar el uso responsable de recursos, asegurando la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos.

PALABRAS CLAVE

Ciberseguridad | Gobernanza | Control interno | Auditoría pública | Riesgo

ABSTRACT

Corporate governance is the system by which organizations are directed and controlled. It is a matter of utmost interest to auditors because it sets the tone at the top of an organization and comprises three of the five components of an internal control system according to the COSO model: the control environment, the risk assessment process, and the monitoring process.

Within the internal control and governance system of public entities are the governance of IT and cybersecurity, which must be integrated in a coherent way.

IT governance is a key component of corporate governance, and it is the system by which the current and future use of IT is directed and controlled, aligning its use with the organization's objectives.

In the current context of hyper-connected world in which control institutions must act, cybersecurity risks acquire an absolutely relevant importance in the assessment of risks.

Cybersecurity governance, which is a very relevant part of IT governance, consists of the set of responsibilities and activities that seek to provide strategic direction in this area, manage risk and guarantee the responsible use of resources, ensuring the confidentiality, integrity, availability, traceability and authenticity of data.

KEYWORDS

Cybersecurity | *Governance* | *Internal Control* | *Public Audit* | *Risk* | *Decisional Autonomy*

1. El sistema de control interno de las organizaciones públicas y la gobernanza

De acuerdo con el modelo COSO, un **sistema de control interno** es 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.

Tal sistema de control interno, a los efectos de las normas internacionales de auditoría, en particular la NIA-ES 315 Revisada, que es la norma base del enfoque de riesgo de auditoría, 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.

Los tres primeros componentes son los que, desde el punto de vista del auditor, forman el núcleo del sistema de gobernanza de una entidad.

El primero es el **entorno de control,** que incluye[1] 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 y su importancia para ella.

Comprende los siguientes elementos[2]:

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) el modo en que los responsables del gobierno demuestran su **independencia de la dirección y ejercen la supervisión del sistema de control interno de la entidad** cuando los responsables del gobierno de la entidad son distintos de la dirección;

c) el modo en que la entidad asigna **autoridad y responsabilidad** para la consecución de sus objetivos,

d) el modo en que la entidad atrae, desarrolla y retiene personas competentes en línea con sus objetivos; y

e) el modo en que la entidad **exige responsabilidades** por la consecución de los objetivos del sistema de control interno a las personas responsables.

1. Párrafo 4 del Anexo 3 de la NIA-ES 315 Revisada.
2. Véase el apartado 21 y el Anexo 3 de la NIA-ES 315 Revisada.

El segundo componente de un sistema de control interno es **el proceso de valoración del riesgo por la entidad,** que incluye[3]:

a) el modo en que la dirección identifica los riesgos de negocio relevantes para los objetivos de la información financiera,

b) el modo en que la dirección estima su significatividad, valora la probabilidad de que ocurran; y

c) cómo se toman decisiones con respecto a las actuaciones necesarias para gestionarlos, así como los resultados de todo ello.

Los riesgos relevantes para una información financiera fiable incluyen hechos externos e internos, transacciones o circunstancias que pueden tener lugar y afectar negativamente a la capacidad de la entidad de iniciar, registrar, procesar e informar sobre información financiera congruente con las afirmaciones de la dirección incluidas en los estados financieros. Sin ninguna duda, actualmente, cuando todas las entidades públicas operan en entornos de administración electrónica hiperconectados a través de internet, cada vez más complejos tecnológicamente, los riesgos de ciberseguridad adquieren una importancia absolutamente relevante.

El tercer componente de un sistema de control interno, de interés para este pequeño estudio, es el **proceso de seguimiento del sistema de control interno realizado por la entidad,** que consiste en[4]:

a) un proceso continuo para evaluar la eficacia de su sistema de control interno,

b) la identificación y corrección de las deficiencias de control identificadas de modo oportuno, y

c) en su caso, la función de auditoría interna de la entidad.

Los tres componentes de un sistema de control interno que se acaban de comentar forman el núcleo principal de la gobernanza corporativa y, en su ámbito, también de la gobernanza de las TI y de la ciberseguridad.

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

Conviene tener claro el significado del concepto de **gobierno de la entidad**, término utilizado por las NIA-ES/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, que se puede definir como la función de la persona o personas u organizaciones responsables de la supervisión de la dirección estratégica y de las obligaciones relacionadas con la rendición de cuentas de la entidad.

3. Véase el apartado 22 y el Anexo 3 de la NIA-ES 315 Revisada.

4. Véase el apartado 24 y el Anexo 3 de la NIA-ES 315 Revisada.

En la nota explicativa que acompaña a 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, habrá que tener en cuenta, en particular, la correspondiente norma de creación de la organización auditada y, en general, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En tal sentido, generalmente hay que entender como **Dirección** a aquellas personas que tienen la responsabilidad ejecutiva, y deberá determinarla el auditor público en función de la legalidad y el diseño de la estructura de la organización auditada; por otra parte, se entiende como **Gobierno de la entidad auditada** u órgano superior de la entidad auditada a aquella persona o conjunto de personas que tiene la facultad de supervisar a la «Dirección» y de formular las cuentas anuales.

Atendiendo a la definición dada en la UNE-ISO/IEC 38500[5] 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.

En resumen, debemos distinguir entre la función y el órgano responsable de ejecutarla:

FUNCIÓN	DEFINICIÓN	ÓRGANO	
Gobierno de la entidad o **gobernanza corporativa**	• El sistema por el cual se dirigen y controlan las organizaciones. • Función de la persona o personas u órganos responsables de la supervisión de la dirección estratégica de la entidad y de las obligaciones relacionadas con la formulación y rendición de cuentas de la entidad.	Órgano de gobierno de la entidad	• Consejo de administración • Junta de gobierno y presidente • Consejo de gobierno • Consejo social
Gestión o **dirección**	• Sistema de controles y los procesos necesarios para alcanzar los objetivos estratégicos establecidos por el órgano de gobierno de la entidad.	Dirección	• Aquellas personas que tienen la responsabilidad ejecutiva

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

Sin embargo, en las administraciones públicas esta cuestión no es evidente, debido a 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, de la que también forman parte estos mismos órganos.

En particular, en referencia a las entidades locales, habrá que estar a lo previsto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. En las universidades públicas esta materia está regulada en el «Capítulo II Gobernanza de las universidades públicas» de la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario que cada universidad debe desarrollar en sus estatutos.

5. UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información.

3. Por qué es importante para el auditor conocer la estructura de gobierno y dirección de la entidad

De acuerdo con la NIA-ES 315 Revisada, el auditor debe adquirir un conocimiento del sistema de control interno de la entidad, cuyos tres primeros componentes incluyen 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.

Es importante conocerlos al planificar la auditoría, 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 adecuado de los demás componentes del sistema de control interno de la entidad. Los responsables del gobierno ejercen una influencia determinante sobre la conciencia de control de una entidad, sobre su «cultura» de control.

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 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, así como si los estados financieros incluyen la información a revelar adecuada.

El grado de conocimiento de estas cuestiones importantes por parte del auditor será acorde con el tamaño y complejidad de la entidad auditada. Cuanto mayor y más compleja sea la entidad mayor importancia le dará el auditor a esta cuestión.

Centrándonos más en los aspectos tecnológicos, la NIA-ES 315 Revisada (apartado A108) señala que la evaluación por el auditor del entorno de control en relación con la utilización de las TI por la entidad incluye cuestiones tales como:

a) 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 las TI, incluida la complejidad o madurez de su plataforma o arquitectura tecnológica y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera.

b) 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.

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, ha ocasionado que las entidades públicas sean totalmente dependientes de las TI, lo que a su vez ha provocado que sea mucho más importante su adecuada gobernanza.

La 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 relacionadas con TI sean tomadas y conducidas por la organización y no a la inversa[6].

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 (1.6.3) la gobernanza corporativa de las TI como **el sistema por el cual se dirige y controla el uso, actual y futuro, de las TI**. Implica evaluar y dirigir la utilización de las 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.

Gartner define el gobierno de TI como los procesos que aseguran el uso efectivo y eficiente de las TI para permitir que una organización logre sus objetivos[7].

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

a) **evaluar** el uso actual y futuro de las TI;
b) **dirigir** la preparación y ejecución de planes y políticas para asegurar que el uso de las TI satisface los objetivos de la organización;
c) **monitorizar** el cumplimiento de las políticas y el desempeño en relación con lo planificado.

La gobernanza de las TI se refiere, por tanto, a los siguientes aspectos clave:

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.

Comprende la estructura organizativa y directiva necesaria para asegurar que las TI respaldan y facilitan el desarrollo de los objetivos estratégicos establecidos. Esto garantiza que:

6. Apartado 1.1 de *IT Audit Handbook,* INTOSAI, 2014.
7. Glosario de Gartner (https://www.gartner.com/en/information-technology/glossary/it-governance)

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

En definitiva, **las decisiones críticas sobre la informática no corresponden al departamento de informática, sino al órgano de gobierno de la entidad**. El conjunto de acciones las debe realizar el área de TI en coordinación con la alta dirección para movilizar los recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

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

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

Un gobierno de las TI maduro contribuye al éxito de las iniciativas de transformación digital que desea poner en marcha una entidad. Un buen gobierno debería planificar sus iniciativas de digitalización y de transformación digital de manera integral y las priorizaría de forma alineada con la estrategia para asegurarse el impacto estratégico y el retorno de un gran valor para la institución.

5. Relación entre gobernanza de las TI y de la ciberseguridad

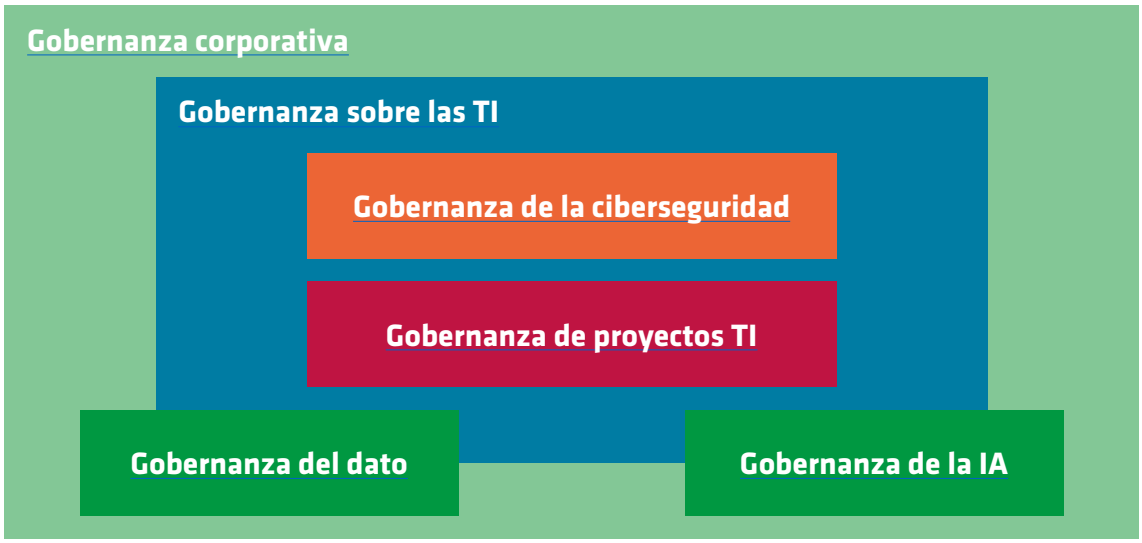
Existe una relación directa entre la **gobernanza de las TI** y la **gobernanza de la ciberseguridad**. Sin embargo, mientras que la primera abarca todos los aspectos de TI (complejidad, innovación, optimización de recursos, etc.), la gobernanza de la ciberseguridad se encarga de los aspectos relacionados con la seguridad de la información (amenazas y su evolución constante, concienciación, recursos humanos y materiales dedicados a la seguridad, etc.).

En definitiva, 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 y a la inversa**.

Del mismo modo, y atendiendo a los diferentes planos a considerar dentro de la gobernanza de las TI, esta debe contemplar estructuras, órganos y directrices para establecer una adecuada gobernanza sobre ámbitos que también son relevantes, entre los que destacamos:

- La **gobernanza de proyectos TI**[8], que permita asegurar que los proyectos tecnológicos se alinean con los objetivos estratégicos, generan valor y se ejecutan de manera eficaz y eficiente.
- El **gobierno del dato**, que garantice que estos se obtienen, gestionan y explotan de forma apropiada. El gobierno del dato se define 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.
- La **gobernanza de la IA**, vertiente que está cobrando una importancia cada vez mayor, debido al auge de esta tecnología y los riesgos asociados a su uso inadecuado.

Los distintos ámbitos de gobernanza de una entidad deben estar integrados en un sistema coherente que, de una forma esquemática, puede representarse de la siguiente forma[9]:



Fuente: GPF-OCEX 5331

En los siguientes apartados profundizamos en los conceptos de gobernanza de las TI y de la ciberseguridad.

8. 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.

9. Véase la *GPF-OCEX 5331*.

6. Elementos clave de la gobernanza de las TI

Para evaluar si las decisiones de TI, los recursos y el seguimiento del desempeño respaldan las estrategias y objetivos de la organización, de acuerdo con la metodología de las instituciones de control externo[10] se deben comprender y evaluar los diferentes componentes de la gobernanza de las TI. Para llevar a cabo esta evaluación, el auditor debe ser consciente de los riesgos asociados a la insuficiencia de cada componente en una entidad.

Los principales componentes o elementos clave de la gobernanza de las TI se detallan en los siguientes subapartados.

Estructura organizativa de la gobernanza de las TI

Todas las entidades, atendiendo al principio de proporcionalidad, deberían 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, tomar decisiones de inversión en TI, comprometiendo los recursos necesarios, y supervisar el rendimiento a nivel estratégico.

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 esa 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. Este comité es la pieza central de la estructura organizativa de las TI y será el órgano colegiado encargado de la definición y supervisión de la estrategia en materia de TI en una entidad.

Estrategia de TI

Un objetivo común a muchas entidades públicas es introducir o ampliar los servicios ofrecidos telemáticamente. En determinados casos, la infraestructura y la arquitectura de TI heredada (*legacy*)[11] de la entidad pueden no ser adecuadas, penalizando hasta el punto de limitar, la posibilidad de llevar a cabo 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.

Para garantizar el éxito de un Plan Estratégico TI (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

10. Puede consultarse el documento *Guidance on Audit of IT Management functions: IT Governance, Contracts & Sustainability* de INTOSAI Working Group on IT Audit, publicado en 2022 y un desarrollo de este en nuestro país, la GPF-OCEX 5331 Gobernanza corporativa, gobernanza de las TI y su auditoría.

11. 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.

para mitigarlos. 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.
- La alineación del PETI con los planes de proyectos, normalmente anuales, que permitan alcanzar los objetivos definidos.
- 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 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.

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

Políticas, normas y procedimientos

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

Esta política debe estar soportada por **normas** y **procedimientos** detallados que definan cómo se aplicará y las directrices – con diferente nivel de detalle- bajo las que se realizará la planificación, gestión, operación y supervisión y uso de las TI. Todo lo anterior conformará el marco de gestión de las TI.

El auditor debe verificar si los diferentes componentes del marco de gestión de las TI están bien comunicados y entendidos por las partes interesadas de acuerdo con sus necesidades, incluido el personal y los proveedores para su adecuado cumplimiento. Además, también comprobará si este es revisado periódicamente y su nivel de actualización es el adecuado, de acuerdo con el entorno de TI y las propias necesidades de la organización.

Recursos, personas, habilidades y competencias

Un componente fundamental del entorno TI es 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.

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.

Véase al respecto el apartado A108 antes citado de la NIA-ES 315 Revisada, que considera esta información relevante para que el auditor evalúe el entorno de control de una entidad.

Cuando se implementan planes de formación, se 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 pueden estar fuera del control de la entidad debido a la normativa existente o a la dependencia de entidades que tengan otras prioridades, constituyendo así un riesgo que el auditor debe valorar.

Gestión del riesgo

Forma parte del segundo componente de un sistema de control interno.

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 riesgos de distinto tipo e impacto.

Para asegurar que las TI se alineen con los objetivos de negocio, las entidades deben identificar, evaluar y mitigar los riesgos asociados al uso de las 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.

Cumplimiento normativo

La norma ISO 38500 recomienda, como principio de buen gobierno de las TI, el cumplimiento normativo relacionado con TI, que integre todas las leyes y las normativas internas relacionadas con las TI. El liderazgo del órgano de gobierno 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 las normas relacionadas con las TI.

7. 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 en los elementos de la gobernanza de las TI vistos en el apartado anterior.

Puede suceder que los recursos comprometidos no se hayan proporcionado de acuerdo con el calendario previsto de un proyecto, que los órganos superiores de la entidad se desentiendan de la toma de decisiones en materia de TI, que los datos de referencia utilizados por la entidad pública sean inadecuados y conduzcan a que los proyectos de TI incumplan o incurran en sobrecostes y desvíos de calendario, al tiempo que contribuyan poco a los resultados relacionados con la misión de la entidad, etc.

El auditor de TI debe conocer los riesgos derivados de la falta de una gobernanza adecuada de 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[12]:

- Estructuras informáticas fragmentadas y duplicadas.
- Las TI proporcionan una baja contribución al valor del servicio.
- Sistemas informáticos ineficaces o poco fáciles de usar.
- Gestión ineficaz de los recursos de TI.
- Proyectos fracasados.
- Gasto en TI que es desconocido, excesivamente alto o insuficiente.
- Exposición a riesgos de ciberseguridad y privacidad, como la pérdida de datos y las violaciones de seguridad.
- Deficiente prestación de servicios públicos.
- Dependencia de terceros (proveedores).
- Inestabilidad asociada a los cambios en los órganos de gobierno.
- Exposición a las ciberamenazas.
- Incumplimiento de las obligaciones legales y reglamentarias.

8. Cómo puede el auditor evaluar si existe una adecuada gobernanza de las TI

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

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.

Hay una serie de componentes clave de la gobernanza de TI para el auditor. Son aquellos factores que impactan en la alineación estratégica y operativa de TI con los objetivos de

12. Ver más detalle en la guía *GPF-OCEX 5331 Gobernanza corporativa, gobernanza de las TI y su auditoría*.

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

Aunque dependerá del tamaño, complejidad de las actividades y otras circunstancias, para analizar si existe una adecuada gobernanza de las TI se atenderá a los siguientes criterios[13]:

- Existe un comité de gobernanza de las TI y de seguimiento del plan estratégico de las TI, con un funcionamiento efectivo.
- Existe un plan estratégico sobre las TI alineado con los objetivos de la entidad.
- Existe un marco normativo interno sobre la gestión de las TI: políticas, normas, procedimientos y procesos.
- Las personas, habilidades y competencias TI. Conviene recordar que la 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 esos procesos que una entidad utiliza para respaldar las operaciones de negocio y para lograr la consecución de las estrategias de negocio[14].
- Seguimiento del desempeño/rendimiento. Estas actividades de supervisión del rendimiento pueden ser llevadas a cabo por los auditores internos, que comunicarán periódicamente sus resultados a la dirección, que a su vez informará a los órganos superiores. Forman parte del tercer componente del sistema de control interno.

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[15]. Incluso si los objetivos de la auditoría no cubren expresamente la gobernanza de TI, muchas debilidades de control en cualquier dominio pueden estar relacionadas con mecanismos de gobernanza inadecuados.

9. La gobernanza de la ciberseguridad

Un componente esencial para una gobernanza adecuada de las TI es contar con una adecuada gobernanza de la ciberseguridad, como aspecto clave a considerar dentro de los distintos planos de las TI.

Los actuales sistemas de información, con la implantación de la administración electrónica avanzada, son más complejos y están más interconectados que nunca. En este contexto, los

13. Véase la sección 1.A.3 de *Guidance on Audit of IT Management functions de INTOSAI,* 2022.

14. Ver apartado 31 de la *GPF-OCEX 1316.*

15. Véase la sección 1.A.2 de *Guidance on Audit of IT Management functions.*

riesgos de ciberseguridad, su probabilidad y las consecuencias perturbadoras sobre los servicios prestados por los entes públicos aumentan de manera muy significativa. El informe de la Sindicatura de Cuentas *Análisis y seguimiento del Plan de Transformación Digital de la Generalitat 2016-2019* señala que «la total dependencia de los sistemas de información y de comunicaciones existente en la gestión pública hace que las Administraciones públicas sean más vulnerables frente a los ciberataques, de modo que la transformación digital debe ir inseparablemente unida a la ciberseguridad»[16].

Por esta razón, es imperativo que los responsables de los entes públicos gestionen dichos riesgos e implanten una sólida gobernanza de **la ciberseguridad como elemento fundamental para establecer una ciberdefensa eficaz.**

Se entiende por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta) el conjunto de responsabilidades y actividades que tienen como objetivo proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una forma responsable[17].

La gobernanza es el proceso de establecer y mantener un marco de referencia y apoyar la estructura y los procesos de gestión para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos, las cinco dimensiones de la seguridad que establece el Esquema Nacional de Seguridad.

Es más que una mera cuestión técnica, por lo que **exige un liderazgo efectivo**, procesos sólidos y estrategias en consonancia con los objetivos de la organización[18]. Este liderazgo debe ser ejercido por los órganos de gobierno y dirección de la entidad. Su compromiso con la seguridad es el factor clave que habilita el establecimiento de un marco de gobernanza efectivo en las organizaciones.

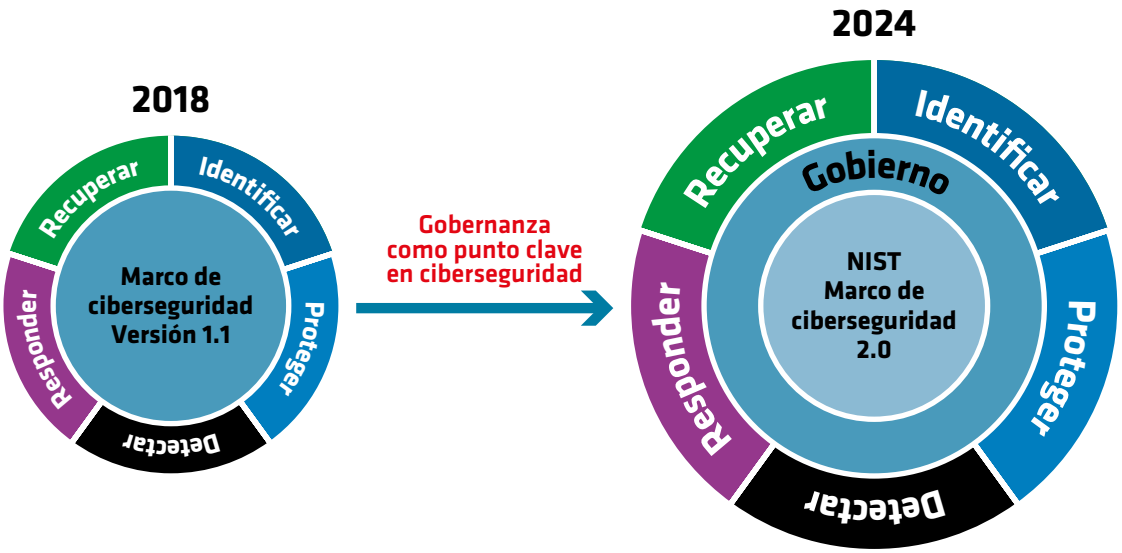
10. Por qué es importante la gobernanza de la ciberseguridad

Internacionalmente, la referencia en materia de ciberseguridad es el «Marco de Ciberseguridad del NIST 2.0» (CSF 2.0) y la principal novedad de esta última versión aprobada en 2024 fue la inclusión de una **nueva función transversal** en su núcleo, con el objetivo de resaltar la importancia de las tareas de gestión y gobierno alrededor de todo el proceso de implementación del marco: «**Gobernar**».

16. En términos muy similares se manifiesta el CCN en su publicación *Aproximación al marco de gobernanza de la ciberseguridad,* en la que se afirma que el éxito de la transformación digital depende, en gran medida, de garantizar los requisitos mínimos de seguridad protegiendo la información tratada y los servicios prestados, elementos consustanciales al desarrollo de nuestra sociedad.

17. Véase el glosario de la *Information Systems Audit and Control Association (ISACA)*.

18. Véase el apartado 66 de *Análisis N.º 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE* del Tribunal de Cuentas Europeo.



Fuente: NIST

De esta forma, «Gobernar» se une a las cinco funciones básicas existentes del NIST CSF: Identificar, Proteger, Detectar, Responder y Recuperar. Con esta nueva función se centra la atención en las personas, los procesos y la tecnología de cada organización necesarios para tomar y ejecutar decisiones de ciberseguridad. Porque, aunque la versión anterior del CSF especificaba lo que había que hacer, no se centraba en las personas que supervisaban esas tareas ni en las políticas y procedimientos que regulaban esos controles.

En nuestro país, la importancia de la gobernanza en la gestión de la ciberseguridad ha sido objeto de diversos documentos y guías del Centro Criptológico Nacional (CCN), entre los que destacan la *Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022*, la *Guía de Seguridad de las TIC CCN-STIC 201 Organización y Gestión para la Seguridad de las TIC* y la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*.

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

Algunas de las ventajas que la existencia de un marco efectivo de gobernanza proporciona a las entidades serían:

- Posibilita la alineación de las actividades relativas a la seguridad de la información con los objetivos estratégicos de la entidad.
- Facilita la coordinación entre distintas áreas de la organización y los implicados en materia de seguridad de la información.
- Posibilita que el conjunto de actividades realizadas y medidas de seguridad aplicadas constituyan un Sistema de Gestión de la Seguridad de la Información que trasciende las iniciativas individuales.

- Establece las responsabilidades del personal implicado, necesarias para garantizar que se cumplen los objetivos y se alcanza el nivel de seguridad requerido.
- Establece procesos que impiden que la eficacia de las actividades de seguridad dependa de roles concretos de la organización o solo de iniciativas personales, sino de un sistema bien establecido.
- Ayuda a fomentar una cultura en materia de ciberseguridad en las organizaciones.

Por el contrario, aquellas entidades que no disponen de un marco de gobernanza adecuadamente definido e implantado tienen una alta probabilidad de que se materialice alguno de los siguientes riesgos:

- El principal riesgo consiste en que la entidad sea vulnerable frente a ciberataques por carecer de un sistema de controles coherente y aceptado por toda la organización.
- Probable uso ineficiente de los recursos, dado que, independientemente de la idoneidad de dichos recursos con respecto a las necesidades identificadas, no existen mecanismos que aseguren que estos son utilizados de manera adecuada para responder a necesidades alineadas con los objetivos estratégicos.
- No asegura la existencia de mecanismos de coordinación interna entre las distintas áreas de la organización y los responsables de la seguridad, lo que impide garantizar que las necesidades sean adecuadamente identificadas en tiempo y forma. Además, posibilita que existan áreas que, de manera inadecuada, realicen una gestión no coordinada de la seguridad al margen las políticas y normas de seguridad de la organización.
- No se asegura que el conjunto de medidas y procesos de seguridad implantados constituyan un Sistema de Gestión de la Seguridad de la Información, integrado y coherente, lo que implica un riesgo de que no existan mecanismos de control que velen por la eficacia de dichas medidas y procesos.
- En caso de no haberse definido responsabilidades al nivel directivo adecuado, existe un riesgo de que las necesidades con respecto a la seguridad de la información identificadas por sus responsables no sean debidamente atendidas por la organización.
- No se asegura que existan mecanismos que independicen las medidas y procesos de seguridad de las personas encargadas de gestionarlas, de modo que existe un riesgo de que ante determinadas ausencias, las medidas de seguridad no sean aplicadas.

Por lo tanto, podemos concluir que una gobernanza adecuadamente establecida proporciona a las entidades mecanismos que garantizan que la seguridad es entendida como un sistema integrado y continuado, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad. La inexistencia de este marco de gobernanza, independientemente de los esfuerzos y recursos dedicados a la seguridad, impide asegurar su eficacia e idoneidad.

11. Responsables del establecimiento de una adecuada gobernanza de ciberseguridad

Aunque las responsabilidades relacionadas con la gobernanza se encuentran distribuidas entre distintos agentes implicados, con diferentes niveles de responsabilidad y atribuciones, **la responsabilidad de establecer una adecuada gobernanza de la ciberseguridad** mediante la aprobación de las políticas de seguridad de la información, de acuerdo con artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS-2010), **es del titular del órgano superior correspondiente**.

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[19].

Sin embargo, en la práctica, de forma general, se ha asumido de manera errónea que la responsabilidad de la seguridad de la información y los servicios, materializada en el cumplimiento de ENS, recae en exclusiva sobre los responsables de las áreas informáticas y tecnológicas, incurriendo en **un grave error de criterio** que menoscaba la ciberresiliencia de las instituciones. Los responsables de las áreas informáticas ya asumen la responsabilidad de la gestión de los sistemas, que es **incompatible** con la responsabilidad sobre la seguridad de la información (artículo 10 del ENS-2010 y artículo 11 del ENS-2022).

12. Elementos de la gobernanza de la ciberseguridad

Para lograr implantar una estrategia de ciberseguridad sólida y que contemple un enfoque **proactivo** de gestión de la ciberseguridad, las organizaciones deben establecer un marco de gobernanza, en el que se designe a los responsables en la materia y sus funciones, y describir los procesos de gestión relacionados con la ciberseguridad[20]. De acuerdo con este marco hay una serie de elementos que, o bien son componentes esenciales de la gobernanza o son condiciones imprescindibles para su buen funcionamiento.

La relación de estos elementos esenciales es la siguiente:

- **Los órganos superiores de la entidad deben ejercer liderazgo y compromiso** con respecto a la seguridad de la información y deben velar por que sean satisfechas todas las necesidades y condiciones necesarias para el establecimiento de una gobernanza adecuada.
- De acuerdo con el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, debe formularse la **política de seguridad de la información (PSI), que debe ser aprobada por el por el titular del órgano superior correspondiente,** es decir por el presidente de la entidad o por la Junta de Gobierno. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización.

19. Guía de iniciación a actividad profesional implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001, Colegio Oficial de Ingenieros de Telecomunicación.

20. Aproximación al marco de gobernanza de la ciberseguridad, CCN 2022.

- Debe existir un **comité de seguridad de la información** con un funcionamiento efectivo.
- Las entidades deben asignar **roles y responsabilidades en materia de seguridad de la información**.
- Debe existir una **planificación estratégica en materia de ciberseguridad**, que proporcione un marco de actuación a medio plazo que asegure la atención a las necesidades prioritarias con respecto a la seguridad, y se encuentre alineada con la estrategia corporativa. La planificación estratégica de la seguridad evita una gestión reactiva basada principalmente en necesidades sobrevenidas.
- La entidad debe **disponer de los recursos materiales y humanos** adecuados para atender a las necesidades identificadas e implementar las medidas de seguridad necesarias. El mantenimiento actualizado y la mejora de los controles de ciberseguridad requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.
- Deben existir **normas y procedimientos de seguridad formalizados y debidamente aprobados y deben ser de aplicación obligatoria en todos los sistemas de información de la entidad sin excepción.** Esta normativa interna debe diseñarse para ser aplicada, no para cumplir una formalidad.
- El conjunto de procesos implantados para la gestión de la seguridad debe constituir un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, que trate la seguridad de manera continuada y proactiva, y que abarque todas las fases del proceso de seguridad: conocer, evaluar y tratar los riesgos y establecer las medidas de seguridad necesarias.
- Se debe establecer una **cultura en materia de ciberseguridad** que afecte a todos los niveles de la organización. Dicha cultura de ciberseguridad debe ser impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, además de incluir **planes periódicos de formación y concienciación** de los trabajadores.

Aunque la ausencia de alguno de estos elementos no implica necesariamente la falta de efectividad de las medidas de seguridad que se encuentren implantadas en las entidades, la carencia de una correcta organización de la ciberseguridad impedirá asegurar que la efectividad se mantendrá a lo largo del tiempo, independientemente de las circunstancias y condicionantes existentes, lo que **incrementará los ciberriesgos**.

13. Conclusiones

1. **El auditor debe conocer el marco de gobernanza de las TI como parte del conocimiento del sistema de control interno**, de acuerdo con lo exigido en la NIA-ES 315 Revisada.
2. **La gobernanza de las TI es un componente clave de la gobernanza corporativa en general** y no debe ser considerada como una disciplina independiente.

3. 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 y a la inversa**.

4. **La gobernanza de las TI es un aspecto crítico y absolutamente indispensable** si se quiere asegurar que las TI están alineadas con los objetivos de la organización. Resulta muy ilustrativa la siguiente cita de Peter Weill, presidente del Centro de Investigación de Sistemas de Información del Instituto Tecnológico de Massachusetts: «**Si tuviera que elegir uno de los factores que más contribuyen al éxito de las TI, sería la gobernanza de las TI**»[21].

5. **La gobernanza de las TI y de la ciberseguridad** no son aspectos meramente técnicos, sino que **exigen un liderazgo efectivo, que debe ser ejercido por los órganos de gobierno y dirección de la entidad**.

Bibliografía

AENOR:

UNE-ISO 37000: 2022 Gobernanza de las organizaciones. Orientación.

UNE-ISO/IEC 38500 Gobernanza corporativa de la Tecnología de la Información (TI).

ASOCEX:

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.

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

Centro Criptológico Nacional (CCN):

Guía de seguridad de las TIC *CCN-STIC 201. Organización y gestión para la seguridad de las TIC,* CCN, 2021.

Guía de seguridad de las TIC *CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones,* CCN, 2019.

Aproximación al marco de gobernanza de la ciberseguridad, CCN, 2022.

Comisión Sectorial de Digitalización de Crue Universidades Españolas:

Gobierno de las TI para universidades, 2011.

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.

Sindicatura de Cuentas de la Comunidad Valenciana:

Informe de síntesis de las auditorías de ciberseguridad de los quince mayores ayuntamientos y de las tres diputaciones de la Comunitat Valenciana, publicado en mayo de 2023.

21. IT and Data Governance: Technology Spotlight, CPA Canada, 2019.

La gobernanza de las TI y de la ciberseguridad en las universidades públicas valencianas. Situación a 30 de junio de 2024, publicado en diciembre de 2024.

La gobernanza de la ciberseguridad en el sector público instrumental de la Generalitat Valenciana: Organismos autónomos. Situación a 31 de diciembre de 2024, publicado en noviembre de 2025.

Auditoría operativa sobre la evaluación de la estructura de gobierno corporativo en el sector público instrumental de la Generalitat. Ejercicio 2024.

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.

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

Código de buen gobierno de la ciberseguridad, Foro Nacional de Ciberseguridad, junio de 2023.