Guía práctica de fiscalización de los OCEX

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

Referencia: GPF-OCEX 1315 (Revisada), GPF-OCEX 5330, GPF-OCEX 5331 y GPF-OCEX 1313

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

1. Qué es la gobernanza de la ciberseguridad

Con la implantación de la administración electrónica avanzada los actuales sistemas de información son más complejos y están más interconectados que nunca. En este entorno interconectado aumentan los riesgos de ciberseguridad, su probabilidad y las consecuencias perturbadoras sobre los servicios prestados por los entes públicos. Como certeramente indica la reciente publicación *Cybersecurity Program Audit Guide* de la US Government Accountability Office, "*las amenazas de ciberseguridad continúan aumentando a medida que aumenta la conectividad de los sistemas y las técnicas de ataque crecen en sofisticación*".

El *Código de buen gobierno de la ciberseguridad*[1] señala que "***La ciberseguridad se ha convertido en el pilar estratégico sobre el que poder asentar la revolución digital que han experimentado todos los sectores de la sociedad, incluyendo Administraciones públicas, empresas y ciudadanía. Solo sobre la base de la ciberseguridad es posible continuar avanzando de forma segura en dicha transformación***." En términos muy similares se manifiesta el Centro Criptológico Nacional (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.

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 entenderá 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**.[2]

---

[1] Publicado en junio de 2023 por el Foro Nacional de Ciberseguridad.

[2] Véase el glosario de la Information Systems Audit and Control Association (ISACA).

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.

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[3]. Este liderazgo debe ser ejercido por la alta dirección/órganos superiores 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.

2. Por qué es importante la gobernanza de la ciberseguridad para una entidad

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.[4]

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 a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

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 experimentar las siguientes carencias:

- 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

[3] 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.

[4] Aproximación al marco de gobernanza de la ciberseguridad, CCN 2022.

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, continuado y proactivo, 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.

3. Por qué es importante la gobernanza de la ciberseguridad para el auditor

En la *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría* se señalan las razones por la que tiene gran relevancia en una auditoría financiera analizar la situación de la gobernanza sobre las tecnologías de la información (TI) y de la gobernanza de la ciberseguridad al revisar el componente "Entorno de control" del sistema de control interno de la entidad auditada, de acuerdo con los requerimientos de la NIA-ES 315 Revisada / GPF-OCEX 1315 Revisada.

Las ciberamenazas representan hoy en día uno de los principales riesgos al que deben hacer frente las organizaciones públicas, por ello, los auditores públicos deben vigilar que estas despliegan unos adecuados controles de ciberseguridad cuya organización y estructuración parte del establecimiento de una sólida gobernanza de la ciberseguridad.

Pero además de la importancia de la gobernanza en la revisión del control interno, el auditor público tiene la obligación de revisar el cumplimiento de la legalidad en la gestión de los entes que audita. Las disposiciones legales y reglamentarias que puedan tener un efecto directo o indirecto en los estados financieros de la entidad incluyen normas sobre seguridad de la información y sobre protección de datos de carácter personal.

La consideración del cumplimiento por la entidad de las disposiciones legales y reglamentarias, de conformidad con la NIA 250 (Revisada), puede incluir la obtención de conocimiento de los procesos de TI de la entidad y de los controles de TI que la entidad ha implementado en virtud de disposiciones legales o reglamentarias. (*Anexo 5, párrafo 20, NIA-ES 315 Revisada)*

Para cumplir los requisitos de la *NIA-ES-SP 1250 Consideración de las Disposiciones Legales y Reglamentarias en la Auditoría de Estados Financieros*, un auditor puede, por ejemplo, considerar:

- Cumplimiento con el Esquema Nacional de Seguridad (ENS). Son cumplimientos relevantes relacionados con la gobernanza de la ciberseguridad, al menos, los siguientes:
  - De acuerdo con el ENS, debe formularse la **política de seguridad de la información (PSI)** que debe ser aprobada por el titular del órgano superior de la entidad. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización, así como, en su caso, a proveedores y terceros.
  - Deben haberse designado los **roles y responsabilidades en materia de seguridad de la información**. Los órganos superiores de la entidad deben nombrar al responsable de la información (que puede tratarse de una persona o un órgano colegiado), al responsable del servicio (que puede ser el mismo que el anterior), al responsable de la seguridad y al responsable del sistema. El procedimiento de nombramiento formal de los responsables mencionados debe constar en la política de seguridad de la información de la entidad.
  - Debe haberse implementado un **comité de seguridad TIC**.

  - Debe haberse realizado una **auditoría de seguridad** al menos hace dos años.

- Cumplimiento con la normativa de protección de datos de carácter personal. Son cumplimientos relevantes, al menos, los siguientes:
  - El nombramiento de **delegado de protección de datos** (DPD) y notificación a la Agencia de Protección de Datos, como exige la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - Elaboración de un **registro de actividades del tratamiento**.
  - Realización de un **análisis de riesgos** sobre los tratamientos de datos personales.
  - Realización de una **auditoría** en materia de protección de datos.

Ambas normas son muy importantes y su incumplimiento puede tener consecuencias relevantes en términos de vulnerabilidad frente a ataques a los sistemas de información o de vulneración de datos personales. Por esta razón **debe exigirse su cumplimiento con carácter generalizado**.

Será de aplicación la *GPF-OCEX 4320 Guía sobre la importancia relativa en las fiscalizaciones de cumplimiento de la legalidad*.

En los informes de auditoría financiera su incumplimiento deberá ser reportado en el apartado *Otros requerimientos legales y reglamentarios*[5].

4. 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, que empieza con la aprobación de las políticas de seguridad de la información, de acuerdo con artículo 12 del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, es del órgano competente de la entidad (normalmente el órgano de gobierno o el titular del órgano superior correspondiente).

En las entidades locales, esta responsabilidad principal recae en su presidente/a. Son los responsables de garantizar que el funcionamiento de la organización resulta conforme con las normas aplicables y de que existan unos adecuados controles sobre los sistemas de información y las comunicaciones. En las comunidades autónomas la responsabilidad principal recae en el órgano de gobierno autonómico. Son los máximos responsables de la implantación del ENS.

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[6].

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 TI ya asumen la responsabilidad de la gestión de los sistemas, que es incompatible con la responsabilidad sobre la seguridad de la información (artículo 11 del ENS).

La responsabilidad de la ejecución de las actividades establecidas por los responsables del gobierno de la entidad corresponde a la dirección. Ver a este respecto el apartado 3 de la *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría*.

[5] Véase la GPF-OCEX 1730 Preparación de informes de auditoría sobre los estados financieros.

[6] 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.

5. Elementos de la gobernanza de la ciberseguridad

Para lograr implantar un sistema de prevención proactiva de 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[7].

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 necesidades y condiciones necesarias para el establecimiento de una gobernanza adecuada.
- Debe formularse la **política de seguridad de la información (PSI), que debe ser aprobada por el titular del órgano superior correspondiente**. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización.
- 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**.
- 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 legal.
- La entidad debe **disponer de los recursos materiales y humanos** adecuados para atender a las necesidades identificadas e implementar las medidas de seguridad necesarias. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa[8]. La ciberseguridad requiere de una constante y adecuada dotación de recursos asignados a su mantenimiento y mejora.
- 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.
- 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 integrada, 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.** Todo el personal de la organización necesita poseer suficientes conocimientos en materia de ciberseguridad para enfrentarse y mitigar el riesgo al que esté expuesto. 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**.

[7] Aproximación al marco de gobernanza de la ciberseguridad, CCN 2022.

[8] Exposición de motivos del Real Decreto 311/2022.

Las entidades deben organizar sus estructuras de gobernanza atendiendo al **principio de proporcionalidad**, al que se alude varias veces en el Real Decreto 311/2022 que aprueba el ENS, teniendo en cuenta su propia complejidad, tamaño, riesgos a los que esté sometida, recursos con los que cuenta y el resto de las circunstancias aplicables.[9]

6. Modelo de gobernanza

La gestión de la seguridad de los sistemas de información exige establecer una organización interna de la seguridad. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

Cada entidad deberá establecer y aprobar su propio modelo de gobernanza de acuerdo con su estructura, dimensión y recursos disponibles, atendiendo al principio de proporcionalidad y deberá recogerlo en su Política de Seguridad de la Información.

En las guías del CCN se propone un modelo de gobernanza de la seguridad que facilita la toma de decisiones interna y articula la colaboración entre ellas. Está destinado a la gestión de los procesos relacionados con el Esquema Nacional de Seguridad y basado en bloques de responsabilidad. Habrá que adaptar este modelo a las posibilidades reales de decisión, gestión y operación de la seguridad de cada entidad.

Según el modelo, la gobernanza de la seguridad se articula a través de un Comité de Seguridad TIC, se gestiona a través de una Oficina de Seguridad TIC, y se implementa mediante Centros de Operaciones de Ciberseguridad (COCS) en colaboración con el departamento de TI. El COCS, realiza una vigilancia continua de los sistemas bajo su responsabilidad, junto a otros roles, y colabora con el departamento de TI, para asegurar la correcta operación e implementación de la seguridad.

A modo de ejemplo se representa gráficamente la estructura básica de ciberseguridad, propuesta en una reciente guía del CCN:

Fuente: Guía CCN-STIC 881

[9] De acuerdo con el "Principio 1: Proporcionalidad" del Código de buen gobierno de ciberseguridad.

7. El comité de seguridad TIC

La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[10] o comité de seguridad de la información, que se constituye como un órgano colegiado[11], algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad. Es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio.

El comité de seguridad TIC es el órgano especializado y permanente de una organización para la ciberseguridad y estará integrado por aquellas personas de la organización con responsabilidad en la toma de decisión en materia de seguridad y privacidad de la información, así como por aquellas designadas en representación de otros órganos o comités. Podrá integrar a vocales de otras áreas de la entidad que sean relevantes para la finalidad del comité, tales como la persona designada como Delegado de Protección de Datos o del Departamento Jurídico o de Recursos Humanos, entre otras.[12]

De acuerdo con lo dispuesto en el ENS, con los criterios generales expuestos en las guías del CCN consideramos que al definir la composición del comité de seguridad TIC y en su funcionamiento se deben tener en cuenta las siguientes consideraciones:

- **No es un comité meramente técnico**, sino que debe integrar vocales de cualquier área significativa necesaria para llevar a cabo sus objetivos.
- Debe ser un **órgano con poder de decisión ágil de toma de decisiones**. Un comité sin poder de decisión, o sin capacidad de influir en quien deba tomarlas, puede resultar inefectivo. Por este motivo se requiere que el órgano cuente con integrantes del nivel más alto de las organizaciones, además de contar con el apoyo necesario para implantar cuantas decisiones y acuerdos se tomen en las reuniones.
- Debe **reunirse periódicamente** con objeto de conocer el estado de la seguridad de la información de la entidad y tomar las decisiones pertinentes de forma oportuna.

  En algunas de las entidades se observa una baja o nula actividad del comité, pese a estar constituido formalmente, lo cual es equivalente a su no existencia. En entidades de gran tamaño y dada la complejidad que presentan sus sistemas de información, el comité debería reunirse al menos trimestralmente.[13]
- **El personal con roles asignados en materia de seguridad de la información o protección de datos deben disponer del suficiente tiempo de dedicación a la seguridad** para desempeñar sus funciones de manera efectiva.
- **El comité de seguridad TIC debe ejercer sus competencias sobre todos los sistemas de la entidad sin excepciones, incluidos aquellos que por su naturaleza son gestionados directamente por los servicios que explotan dichos sistemas.**

  Hay una peculiaridad en el caso de los ayuntamientos que se debe mencionar. En estos casos, en general, los departamentos de policía municipal gestionan de forma casi totalmente independiente sus propios sistemas de información, no integrándose en muchos casos en el marco general de ciberseguridad del ayuntamiento. No es tarea de los OCEX definir cómo deben estar organizados en un ayuntamiento u otra entidad sus sistemas de información, ni si los sistemas policiales y otros sistemas críticos deben estar totalmente integrados con los sistemas corporativos (que normalmente es la solución idónea) o es mejor que estén totalmente separados (lo cual entraña ciertos riesgos innecesarios). Esta es una decisión organizativa de la corporación.

[10] Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC, CCN, enero de 2021.

[11] Regulado por lo dispuesto en la Sección 3ª del Capítulo II del Título Preliminar, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

[12] Apartado 5.1 de "Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022", CCN.

[13] El Código de buen gobierno de la ciberseguridad recomienda que se reúna al menos dos veces al año, pero lo consideramos totalmente insuficiente.

No obstante, cualquiera que fuere la fórmula elegida para organizar los sistemas de información de una entidad, **su marco de ciberseguridad debe ser único**. Esto quiere decir que puede haber un único responsable de seguridad de la información con responsabilidades en el conjunto de sistemas de información de la entidad. O puede haber un responsable de la seguridad de la información de los sistemas de información policiales y/o sistemas críticos, pero en este caso deberán estar integrados también en el CSI para que sean copartícipes y corresponsables de las decisiones que se adopten.

Componentes

La guía CCN-STIC 201 indica que será cada administración la que establezca la composición de su comité de seguridad TIC en función de sus competencias, estructura y circunstancias. No obstante, las guías del CCN[14] establecen una serie de orientaciones sobre su composición y las responsabilidades de sus miembros, que deberían ser, al menos, los siguientes:

- **El presidente** del comité.

  En el caso de una entidad local debería ser el concejal o diputado responsable en materia TIC.

  En el caso de las universidades el CCN recomienda que sea el rector o una persona en la que delegue.

- El **secretario** del comité. En la Guía de seguridad de las TIC CCN-STIC-881, se propone que sea el secretario general de la entidad o una persona en la que delegue.

  Consideramos imprescindible la participación en el comité de seguridad TIC de los/as secretarios/as generales de las entidades, o alguien de su equipo, dado que sobre ellos recae la responsabilidad sobre la ejecución de muchas decisiones del comité.

  Al secretario le corresponderá:

  - Convocar las reuniones del Comité de Seguridad de la Información.
  - Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
  - Elaborar el acta de las reuniones.
  - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

- Responsable de seguridad de la información (**RSEG**).
- Responsable de la información.
- Responsable del sistema.
- Responsable de seguridad física.

  Este rol asume la responsabilidad sobre la seguridad física de la organización[15].

- Delegado de protección de datos (**DPD**), que participará con voz, pero sin voto, para no condicionar sus decisiones futuras y garantizar su independencia y ausencia de conflicto de intereses.

  Este rol es **incompatible** con el de responsable de seguridad.

- Responsable del cumplimiento legal.

El comité puede constituirse con miembros fijos y otros opcionales, por lo que además de los expuestos, podrá invitarse a intervenir en las reuniones cuantas personas sean necesarias de acuerdo con los asuntos a tratar.

La composición del comité de seguridad TIC debe constar en la PSI y sus miembros designados de acuerdo con el procedimiento en ella establecido.

[14] La Guía de seguridad de las TIC CCN-STIC-881 Guía de Adecuación al ENS para Universidades, de mayo de 2022 es muy específica sobre los componentes del CSI para el caso de las universidades, aunque muchos criterios son de aplicación general.

[15] CCN-STIC 201.

8. Roles en materia de seguridad de la información

El ENS (artículo 13.2) establece que la PSI deberá identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El **responsable de la información** determinará los requisitos de la información tratada.

b) El **responsable del servicio** determinará los requisitos de los servicios prestados.

c) El **responsable de la seguridad de la información** (RSEG) determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

d) El **responsable del sistema**, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo

El procedimiento de nombramiento formal de estos responsables debe constar en la política de seguridad de la información de la entidad.

Las características de los roles y sus responsabilidades en materia de ciberseguridad se detallan en la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*, además de ser una cuestión abordada por diversos documentos y guías del Centro Criptológico Nacional.

Para una correcta organización de la seguridad de la información debe tenerse en cuenta que:

- **Los roles en materia de seguridad deben estar formalmente establecidos.**
- **Los roles establecidos ejercerán sus funciones de manera efectiva.** La mera designación de roles para cumplir con la normativa no es suficiente.

  Las organizaciones deben garantizar que las personas designadas **tengan la disponibilidad de tiempo necesaria para realizar sus tareas** de manera efectiva.
- **Los roles estarán correctamente asignados, sin existir incompatibilidades con otras competencias.**

El responsable de seguridad de la información

El responsable de seguridad de la información (RSEG) puede ser un cargo unipersonal del nivel directivo de la organización o un órgano colegiado. No requiere desarrollar funciones de carácter técnico, su función es básicamente supervisora del cumplimiento efectivo de las decisiones del comité de seguridad TIC y de la normativa de seguridad. No obstante, de acuerdo con el *Código de buen gobierno de la ciberseguridad*, esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará **con la suficiente capacidad de decisión e influencia en la organización**.

De acuerdo con el artículo 11.2 y 13.3 del Real Decreto 311/2022, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos, no debiendo existir dependencia jerárquica entre ambos. Es decir, **ambos roles deben ser independientes.**

La *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*, establece "*…que la figura del Responsable de la Seguridad debe estar situada en una posición que le permita tener un acceso directo a los niveles directivos de la organización.*" Y además indica que "*…En el caso de entidades locales (Diputaciones, Cabildos o Ayuntamientos), debería depender del Secretario General, ...*"[16]

[16] De acuerdo con la guía CCN-STIC 201, el responsable de seguridad debería ser el secretario del Comité de Seguridad de la Información, pero no se ha seguido este mismo criterio en la guía CCN-STIC 881.

9. Normativa interna de ciberseguridad

Política de seguridad de la información *(medida de seguridad org.1)*

La política de seguridad de la información (PSI) es un documento de alto nivel que define, de acuerdo con el artículo 12 del ENS (2022), **el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta**. Constituye la expresión formal del compromiso y liderazgo de la alta dirección con la seguridad.

Se aprobará de conformidad con lo dispuesto en el artículo 12 del ENS, y se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

[*org.1.1*] Los objetivos o misión de la organización.

[*org.1.2*] El marco legal y regulatorio en el que se desarrollarán las actividades.

[*org.1.3*] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

[*org.1.4*] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

[*org.1.5*] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

El ENS indica los principios básicos y los requisitos mínimos de la PSI. Además, existen algunos aspectos que las organizaciones deben tener en cuenta, como son:

- Debe ser elaborada por el comité de seguridad TIC y aprobada por el presidente del ente local o el órgano superior de la entidad.
- Debe ser un documento breve, dejando detalles técnicos para las normas que la desarrollan.
- Debe ser revisada y actualizada periódicamente.
- Debe ser accesible (publicada y dada a conocer) a los empleados y colaboradores de la organización.

Un sistema de gestión continuada de la seguridad de la información requiere que la PSI se complete con *normativa interna*, desarrollada en documentos más precisos que materialicen los requisitos de la PSI (uso correcto de equipos, servicios, instalaciones, usos indebidos, responsabilidades del personal); y un conjunto de *procedimientos de seguridad* que describan, paso a paso, cómo deben realizarse tareas concretas (documentos que detallan cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos).

Esta normativa interna **debe diseñarse para ser aplicada**, no para cumplir una mera formalidad. El contenido del conjunto de políticas, normas y procedimientos aprobados debe ser una representación fidedigna y precisa del sistema de seguridad implantado por el ente local. La aprobación de un marco normativo que no represente la realidad del ente deviene en un uso estéril de recursos por su carencia de efectividad y en una falsa percepción de cumplimiento que puede conllevar el abandono de otras medidas más adecuadas.

Cada entidad debe establecer y aprobar su propia organización de seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en su Política de Seguridad de la Información[17].

Es importante tener en cuenta que, independientemente del modelo organizativo existente en una entidad, toda la normativa de ciberseguridad afectará, sin excepción, **a todos los departamentos y sistemas de información**. La organización de la seguridad sea la que sea, debe estar definida en la PSI aprobada por el órgano superior e incluirá todos los sistemas de información sin ninguna excepción.

[17] CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones

Normativa de seguridad *(medida de seguridad org.2)*

Se dispondrá de una serie de documentos que describan:

[*org.2.1*] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

[*org.2.2*] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Esta normativa deberá ser aprobada por quien se disponga en la PSI. Es de carácter obligatorio y deberá estar a disposición de todos los miembros de la organización (publicada en la intranet corporativa).

Es importante diferenciar entre norma y procedimiento. Una norma indica "qué debe hacerse". Los procedimientos detallan las acciones a realizar, es decir, el "cómo debe hacerse" y, cuando procede, quienes deben hacerlo.

Procedimientos de seguridad *(medida de seguridad org.3)*

Las entidades deben disponer de un conjunto de procedimientos aprobados que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

[*org.3.1*] Cómo llevar a cabo las tareas habituales.

[*org.3.2*] Quién debe hacer cada tarea.

[*org.3.3*] Cómo identificar y reportar comportamientos anómalos.

[*org.3.4*] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere.

Los procedimientos deberán ser aprobados por quien se disponga en la PSI.

10. Otros órganos relacionados con la gestión de la ciberseguridad

Las organizaciones, dependiendo de su tamaño y complejidad, pueden disponer, además del comité de seguridad TIC, de diversos órganos de gobierno relacionados con la gestión de la ciberseguridad, que pueden administrar funciones a distintos niveles, incluyendo el operativo, el ejecutivo/supervisión o el de gobierno. Algunos de estos órganos pueden ser:

- El comité de seguridad corporativa.
- El comité de gobernanza sobre las TI.
- La oficina de seguridad TIC.
- El centro de operaciones de seguridad.
- El equipo de respuesta a incidentes de seguridad.
- El comité de gestión de crisis.

La existencia de estos órganos responde, en general, a las exigencias de la normativa básica de aplicación, el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos. No obstante, puede ser de también de aplicación otra legislación sectorial y específica, como la de Ley de Protección de Infraestructuras Críticas (Ley PIC8/2011), que establecen sus propios requisitos de seguridad adicionales, incluyendo medidas organizativas.

Aunque la existencia de estos órganos puede no ser obligatoria en todas las circunstancias, dependiendo de la legislación que sea de aplicación en cada caso, sí resulta **imprescindible que**, en caso de existir, el **conjunto de estos órganos coordine adecuadamente sus actividades y existan mecanismos de comunicación y colaboración** entre los mismos.

Comité de seguridad corporativa

La seguridad de la información es una más de las áreas de seguridad de una organización. En organizaciones de tamaño significativo suele existir un Comité de Seguridad Corporativa (con su propio Secretario, al que suele denominarse Responsable de la Seguridad Corporativa). El responsable de la seguridad de la información será un miembro de este Comité, junto con otros responsables de seguridad de otras áreas o departamentos.[18]

Comité de gobernanza sobre las TI

Debería tener algún miembro común con el comité de seguridad TIC (como por ejemplo el responsable del sistema y el responsable de seguridad) de forma que sus actividades sean coherentes. Ver la guía *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría*.

Oficina de seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad, como elemento operativo, se podrá constituir una Oficina de seguridad TIC, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo:

- Adecuación al ENS, marco normativo y análisis y gestión de riesgos.
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.
- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.

Para su composición se propone:

- El Director de la Oficina de seguridad TIC, nombrado por el comité de seguridad TIC, que actuará como enlace con el mismo, que será el responsable de seguridad (RSEG), o la persona en quien delegue.
- Secretario de la Oficina de Seguridad TIC, nombrado por el Comité de Seguridad TIC, a propuesta de los miembros de la Oficina de Seguridad.
- Todos aquellos administradores especialistas de seguridad (AES) que el responsable de seguridad determine que sean necesarios.

Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por el comité de seguridad TIC[19]:

a) Gestión y operativa de la seguridad del proyecto de adecuación, implantación y gestión de la conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.

b) Redacción y presentación de propuestas al comité de seguridad TIC. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al comité.

c) Promover la mejora continua del SGSI.

Centros de operaciones de ciberseguridad (COCS)

De acuerdo con la guía CCN-STIC 201, la gobernanza de la seguridad en una organización se articula a través de un comité de seguridad TIC y se implementa mediante centros de operaciones de ciberseguridad que velan por la operación y correcta implementación de la seguridad mediante una vigilancia continua de los sistemas bajo su responsabilidad.

Bajo la responsabilidad y dirección del responsable de seguridad, el centro de operaciones de ciberseguridad presta sus servicios, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, especialmente los que manejan información clasificada, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

[18] Guía CCN-STIC 801.

[19] Ver un mayor detalle en CCN STIC-881.

En definitiva, los centros de operaciones de ciberseguridad articularán la respuesta a los incidentes de seguridad, sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración con competencias y de la función de coordinación de los CSIRT de referencia y del CCN-CERT, como coordinador nacional.

Asimismo, en función de la naturaleza y dimensiones de la organización, el COCS puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el responsable de seguridad.

El COCS puede llevar a cabo las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operaciones de seguridad sobre los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El equipo de respuesta a incidentes de seguridad

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el comité de seguridad TIC y funcionales del RSEG y posibles alertas recibidas del COCS.

Está compuesto por un equipo con capacidades de atención inmediata denominado primer nivel de atención y por un grupo de especialistas para aquellos incidentes no resueltos por el primer nivel que requieran un mayor grado de especialización.

Comité de gestión de crisis

Un ciberincidente grave provocará una crisis y esto implica la necesidad de tomar decisiones bajo mucha presión, en poco tiempo y con información probablemente incompleta.

Con independencia del tipo de ciberincidente que cause la crisis, se hace patente la componente de gestión que implica su resolución. Para ello, la organización afectada necesita haberse dotado de las capacidades y estructuras de gestión (comités/equipos) adecuadas que le han de permitir abordarla con garantías de éxito.

En resumen, la capacidad de gestionar una situación de crisis depende en gran medida de las estructuras o comités que se hayan establecido antes de que ocurra el desastre causado por un ciberincidente que sea un suceso de baja probabilidad y alto impacto.

El comité de crisis es el órgano encargado de la gestión de la crisis a alto nivel dentro de la organización, con una visión estratégica. Se encargará de tomar las decisiones y coordinar las acciones necesarias para la resolución de los incidentes que hayan sido calificados como crisis dentro de la entidad, determinando y/o validando las estrategias de análisis, de contención y mitigación que permitan recuperar las operaciones en el menor tiempo posible, minimizando los impactos sobre las partes interesadas.

11. Posibles deficiencias en materia de gobernanza

Entre otras se pueden citar las siguientes[20]:

En materia de normativa de seguridad

- Inexistencia de PSI formalmente aprobada por la corporación, o desactualizadas o no adaptadas a la realidad de las entidades, lo que impide que los principios que deben regir las actuaciones en materia de seguridad sean conocidos por toda la corporación.
- Inexistencia de normativa y procedimientos formalizados, lo que puede originar el riesgo de no realización de tareas importantes por no estar asignadas a responsables, dependiendo su ejecución de la buena voluntad de quienes los llevan a cabo.
- El contenido de los procedimientos no detalla de manera clara y precisa las tareas a realizar ni quiénes son los responsables de ejecutarlas, especificando únicamente el deber de realizar la acción, aspecto que corresponde a las normas de seguridad de rango superior, lo que genera procedimientos ineficaces.
- Existencia de procedimientos escritos que, aunque están definidos de manera correcta, han sido realizados por consultoras externas y tienen poca o nula adaptación al entorno de la entidad, dado que no reflejaban la realidad de las acciones llevadas a cabo en la práctica.
- Los procedimientos existentes, incluidos aquellos formalmente aprobados, no se encuentran actualizados y no representan con fidelidad los procesos de seguridad que describen.

En relación con el comité de seguridad TIC

- Existen entidades que no disponen de comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad.
- En otros casos, aunque el comité de seguridad de la información está formalmente constituido, no se reúne o no lo hace la periodicidad necesaria, lo que impide hacer un seguimiento del estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna.
- El comité de seguridad no dispone de los miembros adecuados, estando compuesto únicamente de miembros con cargos relacionados con los sistemas de información y la seguridad. La ausencia de miembros con el más alto poder de decisión en la organización y de vocales de las áreas significativas, convierte al comité en un órgano meramente técnico e impide un gobierno eficiente y la toma de decisiones estratégicas a nivel corporativo.

En relación con los roles de seguridad

- Existen entidades que no han asignado los roles y responsabilidades en materia de seguridad de la información.
- Existen entidades que no disponen de un delegado de protección de datos formalmente nombrado.
- Algunos de los roles se seguridad no ejercen sus funciones de manera que se garantice la necesaria independencia y la ausencia de conflicto de intereses.
- Algunos roles en materia de seguridad no disponen de la dedicación suficiente para las necesidades de la entidad. Los responsables de seguridad de manera general no ejercen sus funciones de manera exclusiva, incurriendo en una acumulación de competencias no directamente relacionadas con la seguridad de la información que impide que desarrollen sus funciones de forma efectiva.

En relación con el liderazgo y el compromiso con la ciberseguridad

- La falta de una cultura de ciberseguridad en la entidad, materializada en acciones formativas y campañas de concienciación dirigidas a los empleados.
- Inexistencia de implicación de los máximos responsables de la organización.

[20] Se ha tomado como referencia los más de 40 informes sobre ciberseguridad publicados por la Sindicatura de Cuentas de la Comunidad Valenciana en los que se señalan numerosas deficiencias en materia de gobernanza de la ciberseguridad.

- La carencia de planes estratégicos desarrollados e impulsados por el más alto nivel de la corporación en los que se establezcan acciones, objetivos y medidas concretas para alcanzar los niveles de seguridad exigidos por la normativa.
- Falta de comunicación o inadecuada comunicación de los procedimientos de seguridad y decisiones en materia de seguridad de la información al personal de la organización.
- La falta de recursos, tanto económicos como de personal, en los departamentos TIC, indispensable para implantar las medidas de seguridad necesarias y llevar a cabo proyectos transversales que afecten a toda la organización.

12. Cómo puede el auditor evaluar si existe una adecuada gobernanza de la ciberseguridad

Se podrá utilizar el programa de auditoría/cuestionario del Anexo, que tiene la siguiente estructura, y que deberá ser adaptada en cada caso:

1. *Políticas, normas y procedimientos sobre seguridad de la información (apartado 9 de la guía)*
2. *Comité de seguridad TIC, roles y responsabilidades*
3. *Compromiso de la dirección y de la alta dirección*
4. *Gestión de riesgos*
5. *Cumplimiento legal: ENS y protección de los datos personales*
6. *Recursos del departamento TIC y de seguridad*

13. Bibliografía

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 5311 Ciberseguridad, seguridad de la información y auditoría externa.
- GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad.
- GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica.
- GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría

CENTRO CRIPTOLÓGICO NACIONAL (CCN)

- Guía de seguridad de las TIC CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones, CCN, 2019.
- 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-881 Guía de Adecuación al ENS para Universidades, CCN 2022.
- Aproximación al marco de gobernanza de la ciberseguridad, CCN, 2022.

OTROS

- Código de buen gobierno de la ciberseguridad, Foro Nacional de Ciberseguridad, junio de 2023.
- 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.
- 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, 2012.
- Cybersecurity Program Audit Guide, US Government Accountability Office, septiembre de 2023.

Entidad auditada	**Programa/cuestionario para la evaluación de la gobernanza de la ciberseguridad**	**GPF-OCEX 5314 Anexo**

INSTRUCCIONES:

El presente programa/cuestionario tiene por finalidad realizar una evaluación sobre el **nivel de la gobernanza de la seguridad de la información** en la entidad.

Las contestaciones al cuestionario se referirán a la situación a fecha _____ del año _____ y podrán ser comentadas y verificadas por el equipo de auditoría en el curso del trabajo.

El cuestionario incluye preguntas relativas a diversos temas y se encuentran fundamentadas en normativa de obligado cumplimiento y metodologías de gestión de seguridad de la información de reconocido prestigio, particularmente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad.**
- Guía de Seguridad de las TIC **CCN-STIC 801**. Esquema Nacional de Seguridad Responsabilidades y Funciones.

La metodología y criterios de auditoría utilizados se encuentran recogido en la GPF-OCEX 5314.

La remisión del cuestionario cumplimentado, así como de la documentación que en caso necesario deba ser adjuntada al mismo, se realizará **únicamente por medios seguros**, dada la sensibilidad de la información tratada. Se remitirá …. ***(especificar método)***

Para cualquier duda, no dude en ponerse en contacto con los miembros del equipo de fiscalización (Correo electrónico: **_____**).

Le rogamos nos facilite el cuestionario cumplimentado en el plazo de _____ días.

CUMPLIMENTADO POR:

Nombre:

Cargo:

Fecha:

1. Políticas, normas y procedimientos sobre seguridad de la información

Respecto a la Política de Seguridad de la Información-PSI (Org.1)

Objetivo de auditoría: comprobar si la entidad tiene políticas sobre la seguridad de los sistemas de información (PSI) adecuadas, están aprobadas y actualizadas. Si la PSI está estructurada de forma que incluya, con claridad, al menos el contenido que señala el ENS.

Cuestionario:

1.1 ¿Dispone la entidad de una PSI aprobada?

Aportar documento formal conteniendo la PSI y documentación acreditativa de su aprobación.

En caso negativo, indicar se la entidad se ha adherido a la PSI de la que depende o está vinculada.

Aportar evidencia de su publicación, y de su difusión interna.

Indicar fecha de aprobación de la primera versión de la PSI

Indicar fecha de aprobación de la versión vigente de la PSI

Comprobaciones:

- Revisar las PSI para verificar si están aprobadas por el órgano superior correspondiente y publicadas, si están actualizadas, si tienen el contenido requerido por el ENS y si reflejan las necesidades de la entidad.
- Revisar el historial de control de cambios de las PSI para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.
- Si se define la estructura del comité de seguridad TIC, junto a otros comités técnicos o grupos de trabajo que puedan llegar a definirse (OTS, COCS…), detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Si se determinan en la PSI los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación: al menos, responsable de la información, responsable del servicio, responsable de seguridad y responsable del sistema.
- Se determinan los diferentes niveles de normativa de desarrollo de las PSI y los órganos competentes para aprobar las normas a cada nivel.

Respecto a la normativa de seguridad (Org.2)

Objetivo de auditoría: comprobar si la entidad dispone de normativa interna donde se determine el uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido.

Cuestionario:

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

- Aportar una relación de las normas aprobadas, indicando nombre, fecha de aprobación y órgano que la aprobó.
- Evidencia de su aceptación por empleados y colaboradores.

Comprobaciones:

- Revisar si las normas y procedimientos existen, están debidamente aprobadas, si se han comunicado adecuadamente a las partes interesadas y son accesibles.
- Revisar si las normas y procedimientos están adaptadas a las necesidades de la entidad o son puramente teóricas.
- Revisar el historial de control de cambios de normas y procedimientos para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.

Respecto a los procedimientos de seguridad (Org.3)

Objetivo de auditoría: comprobar si la entidad dispone de un conjunto de procedimientos documentados que determinan cómo realizar las tareas habituales y quiénes son sus responsables.

Cuestionario:

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

- Aportar una relación de los procedimientos aprobados, indicando nombre, fecha de aprobación y órgano que la aprobó.

Comprobaciones:

- Revisar si las normas y procedimientos existen, están debidamente aprobadas, si se han comunicado adecuadamente a las partes interesadas y son accesibles.
- Revisar si las normas y procedimientos están adaptadas a las necesidades de la entidad o son puramente teóricas.
- Revisar el historial de control de cambios de normas y procedimientos para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.

2. Comité de seguridad TIC, roles y responsabilidades

Objetivo de auditoría: Evaluar si las estructuras de gobierno de la ciberseguridad (comité de seguridad de las TIC y los distintos roles exigidos por la normativa) y sus responsabilidades están claramente definidas, si la entidad ha realizado los nombramientos en materia de seguridad de la información de acuerdo con lo previsto en las PSI y si las personas designadas disponen del tiempo necesario para llevar a cabo sus tareas de manera efectiva.

Cuestionario:

2.1 ¿Se ha constituido formalmente el Comité de Seguridad TIC?

- Aportar documentación acreditativa de la constitución.
- Aportar documento/s de nombramiento / asignación de roles y responsabilidades.

2.2 ¿Tiene el Comité de Seguridad TIC una actividad continuada y efectiva?

- Periodicidad de las reuniones: _____
- Aportar las actas de las reuniones celebradas en el año fiscalizado y el anterior.

2.3 ¿Existen otros órganos destinados a la gestión de la seguridad de la información?:

Oficina de seguridad TIC	SI/NO
Órgano de Auditoría Técnica (OAT)	SI/NO
Centro de Operaciones de ciberseguridad (COCS)	SI/NO

- Aportar documentación acreditativa de la constitución y funcionamiento de dichos órganos.

2.4 ¿Se han nombrado los roles en materia de seguridad de la información?

Responsable de la información	SI/NO
Responsable del servicio	SI/NO
Responsable de la seguridad de la información (RSEG)	SI/NO
Responsable del sistema	SI/NO

- Aportar documentación acreditativa de los nombramientos.

2.5 ¿Dispone el RSEG de dedicación suficiente a la gestión de la seguridad de la organización como para desempeñar sus funciones de manera adecuada?

¿Es conocida su responsabilidad por el resto de la organización?

Comprobaciones:

- Revisar las PSI para determinar si las funciones y responsabilidades del CIS y los distintos roles de la seguridad de la información han sido claramente definidas y comunicadas.
- Determinar si el CSI está integrado por los roles requeridos por el ENS y cumple con buenas prácticas.
- Revisar las actas de las reuniones para ver si el CSI está desempeñando de forma efectiva sus funciones (verificar la periodicidad de sus reuniones) y las responsabilidades definidas.
- Revisar si la corporación ha designado los roles y responsabilidades en materia de seguridad correctamente.
- Revisar si las personas con roles asignados ejercen de manera efectiva y disponen del tiempo necesario para realizar las tareas atribuidas.
- ¿Se dispone de un acta del Comité de Seguridad TIC donde se designen sus miembros, o las altas y bajas que se puedan llegar a producir?

3. Compromiso de la dirección y de la alta dirección

Objetivo de auditoría: evaluar las acciones relacionadas con la implicación de los miembros de la dirección y la alta dirección. Los miembros de la dirección y la alta dirección deben participar de forma activa en el establecimiento de políticas y objetivos estratégicos de la entidad, la gestión de riesgos y en la aplicación de medidas para mitigarlos. Debe existir un liderazgo reconocible.

Cuestionario:

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

- Aportar plan estratégico o documento equivalente.

3.2 ¿Los responsables de la gobernanza del Plan Estratégico TIC mantienen reuniones periódicas de revisión/seguimiento de cumplimiento del plan anterior?

- Aportar actas de las reuniones de revisión/seguimiento del plan anterior, indicadores de cumplimiento de los objetivos.

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

- Aportar plan estratégico o documento equivalente.

3.4 ¿Los responsables de la gobernanza del Plan Estratégico de Seguridad mantienen reuniones periódicas de revisión/seguimiento de cumplimiento de dicho plan?

- Aportar actas de las reuniones de revisión/seguimiento del plan anterior, indicadores de cumplimiento de los objetivos.

3.5 ¿El Comité de seguridad TIC incluye miembros de la dirección/alta dirección?

- ¿Participan de manera activa en sus reuniones?

3.6 ¿Realiza la alta dirección de la entidad acciones que promuevan la concienciación sobre la ciberseguridad y la difusión de la política de seguridad?

- Describir brevemente las actividades o formaciones llevadas a cabo en el último año.

3.7 ¿Existe un plan de formación y concienciación en materia de ciberseguridad?

- Describir brevemente las actividades o formaciones llevadas a cabo en el último año.
- Aportar plan de formación/concienciación y acreditación de su ejecución.

3.8 ¿Facilita la alta dirección los recursos necesarios para el buen funcionamiento del sistema de gestión de la seguridad de la información (SGSI) y según las necesidades identificadas?

- Proporcione una relación de informes de necesidad, o documento equivalente, remitidos a la dirección o la alta dirección e indique cuáles de los mismos han sido atendidos adecuadamente por la organización.

Procedimientos de auditoría:

- Analizar la información recibida y evaluar las acciones relacionadas con la implicación de los miembros de la dirección y la alta dirección y su participación activa en el establecimiento en la definición e implementación de políticas y objetivos estratégicos de la entidad, la gestión de riesgos y en la aplicación de medidas para mitigarlos.
- Identificar si existe un liderazgo reconocible.

4. Gestión de riesgos

Objetivo de auditoría: evaluar si la entidad ha realizado y documentado un análisis sobre los riesgos que afectan a sus sistemas de información y los ha clasificado por niveles de seguridad (alto, medio o bajo) de acuerdo con los requisitos del ENS (art. 40 y 41).

Cuestionario:

4.1 ¿Existe un sistema para la gestión de riesgos TI/ciberseguridad

- Aportar documentación sobre el análisis de riesgos realizado

4.2 ¿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?

- ¿Cómo se materializa esa participación?

Procedimientos de auditoría:

- Revisar la documentación del análisis de riesgos. Verificar que incluye los sistemas de información críticos de la entidad y que está actualizado.

5. Cumplimiento legal

Esquema Nacional de Seguridad

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

Cuestionario:

5.1 Además de las cuestiones incluidas en los apartados anteriores, informar y aportar la documentación justificativa sobre:

- Si la Entidad ha formalizado un documento con la **declaración de aplicabilidad**, que recoge las medidas de seguridad que son de aplicación en función del nivel y categoría del sistema, que además ha sido firmada por el responsable de seguridad.

  Aportar la declaración de aplicabilidad.

- Si la entidad ha realizado la **auditoría de cumplimiento del ENS** para los sistemas de categoría Media y Alta o autoevaluación para nivel básico.

  En caso afirmativo, indicar la empresa que ha realizado la auditoría y aportar el informe de auditoría y/o autoevaluación.

  Indicar si se ha realizado en el periodo revisado algún otro tipo de auditoría de seguridad.

- Los resultados de la auditoría y/o 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.
- Si la entidad no ha realizado informe de auditoría ENS (niveles medio y alto) ni autoevaluación (nivel básico) verificar si se ha realizado un Plan de adecuación al ENS.
- 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.

  Aportar el Informe INES
- 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.

Procedimientos de auditoría:

- Revisar la declaración de aplicabilidad y verificar que las medidas de seguridad se corresponden con los niveles de seguridad de los sistemas de información aprobados.
- Verificar que se ha elaborado y comunicado en informe sobre seguridad de la información para el ejercicio auditado (informe INES. Art. 32 ENS: Instrucción técnica de seguridad, Resolución de 7 de octubre de 2016 de la Secretaría de estado de las Administraciones Públicas).
- Verificar que se han realizado los informes de auditoría de seguridad requeridos por el ENS (Art. 31).

Protección de datos de carácter personal

Objetivo de auditoría: Evaluar si se da cumplimiento a los requisitos mínimos del RGPD y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.

Cuestionario:

5.2 ¿Existe un adecuado nivel de cumplimiento respecto al cumplimiento legal en materia de **protección de datos de carácter personal**?

- La entidad ha designado un Delegado de Protección de Datos (DPD) y su nombramiento ha sido comunicado a la AEPD.

  Aportar documento acreditativo del nombramiento y de la notificación a la AEPD.
- La entidad dispone del registro de actividades de tratamiento (RAT) con la información requerida por el RGPD

  Aportar RAT.
- La entidad ha realizado análisis de riesgo de los tratamientos de datos personales y evaluaciones de impacto para aquellos de riesgo alto.

  Aportar registro de los análisis de riesgo realizados en materia de protección de datos y evaluaciones de impacto.
- La entidad evalúa periódicamente la eficacia de las medidas técnicas y organizativas implantadas

  Aportar informes de auditoría para dar cumplimiento al requisito anterior.

Procedimientos de auditoría

- Verificar si se ha nombrado un delegado de protección de datos y se ha comunicado a la AEPD (art. 37 RGPD).
- Verificar si se ha elaborado y publicado en la web de la entidad el RAT (Art. 30 RGPD y 31 LOPDGDD)
- Verificar si se han realizado análisis de riesgos y evaluaciones de impacto sobre los datos personales tratados por la entidad (Art. 32 y 35 RGPD)
- Verificar que se han realizado auditorías sobre la protección de los datos personales en base al principio de responsabilidad proactiva del RGPD (art 32 RGPD)

6. Recursos del departamento TIC y de seguridad

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 tareas de seguridad, y si estos son adecuados al tamaño de la entidad.

Cuestionario:

6.1 ¿Dispone la entidad de los recursos humanos necesarios para cumplir adecuadamente con obligaciones con respecto a la seguridad de la información?

Informar 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. 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, NO dedicadas a la seguridad TIC.		
Número de personas contratadas a proveedores a tiempo completo que prestan servicio o asistencia al departamento TI dedicadas a la seguridad TIC.		

6.2 ¿Realiza la entidad las inversiones necesarias en proyectos o servicios para cumplir adecuadamente con obligaciones con respecto a la seguridad de la información?

Informar sobre:

(Con datos 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		

Procedimientos de auditoría

- Analizar el número de personal a tiempo completo (o equivalente) pertenecientes en al departamento/área/negociado de gestión de las TIC de la entidad, identificando cuántas de ellas se dedican a la SSI.

- Se revisará la dotación presupuestaria de los Capítulos 1, 2 y 6 del departamento TIC y a la SSI.
- Se revisará el total de ORN de los Capítulos 1, 2 y 6 del presupuesto.

7. Otros aspectos

Incluya a continuación información sobre otros proyectos o medidas implantadas o carencias identificadas que considere que deben ser contempladas para la evaluación de la gobernanza de la ciberseguridad.