

Prontuario de ciberseguridad para entidades locales

—
Centro Criptológico Nacional y
Federación Española de Municipios y Provincias

DICIEMBRE
2022

—
VERSIÓN 02



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS



Contenido

1. Introducción	3
2. Objeto del documento	4
3. La problemática de la ciberseguridad local	5
3.1. Amenazas y riesgos para las Entidades Locales	7
4. El cumplimiento del Esquema Nacional de Seguridad en las EE.LL.	11
5. Los responsables públicos y la ciberseguridad	13
5.1. Órganos necesarios	13
5.1.1. El alcalde	14
5.1.2. Los tenientes de alcalde	19
5.1.3. El Pleno	19
5.1.4. La Junta de Gobierno Local	21
5.2. Órganos complementarios	23
5.3. Funciones públicas de los habilitados nacionales: secretarios e interventores	23
5.3.1. Los secretarios	24
5.3.2. Los interventores	29
5.3.3. Los tesoreros	32
6. La prestación de servicios externos	34
7. Referencias	36
Anexo Tabla de Funciones y Responsabilidades	37

Introducción

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que un reto colectivo al que necesariamente hemos de enfrentarnos y en el que las entidades locales no pueden quedar al margen.

Por este motivo, resultando necesario incrementar el uso de los medios electrónicos por parte de nuestras entidades locales, como pone de manifiesto la reciente aprobación y publicación del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (BOE nº 77, de 31 de marzo de 2021), es imprescindible asimismo garantizar la protección de sus capacidades tecnológicas, la información tratada y los servicios prestados, puesto que, constituyendo el elemento más próximo a los intereses de los ciudadanos, su plena operatividad resulta imprescindible para el desarrollo de España.

Con este documento, dirigido a todo el sector público y, muy especialmente, a los órganos directivos de las entidades locales (ya se trate de cargos electos como de función pública), el Centro Criptológico Nacional y la Federación Española de Municipios y Provincias, en cumplimiento de sus responsabilidades y atendiendo a lo que venía

disponiendo el Real Decreto 3/2010, de 8 de enero, y, en la actualidad, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, norma a la que el presente documento está completamente adaptado, se espera contribuir a mejorar la ciberseguridad local española y mantener las infraestructuras y los sistemas de información de las administraciones de las entidades locales con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Confiando que este texto sea leído y tomado en consideración por todos aquellos que, al máximo nivel del gobierno de nuestros Ayuntamientos, Diputaciones y Cabildos, tienen la responsabilidad de hacer mejor, más eficiente y más segura la Administración Digital de nuestras entidades locales.

La gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentarnos y en el que las entidades locales no pueden quedar al margen.

2. Objeto del documento

El propósito del presente documento es doble. En primer lugar, mostrar de manera concisa y clara a los responsables de las entidades locales, ya se trate de cargos electos como de funcionarios, la **realidad de los riesgos y amenazas** que, para el normal desenvolvimiento de los procedimientos administrativos, las funciones involucradas en el desarrollo institucional provincial o municipal y la gestión y administración de las entidades locales, emanan del ciberespacio y; en segundo lugar, señalar las garantías ofrecidas por el **Esquema Nacional de Seguridad** (ENS, operado actualmente por Real Decreto 311/2022, de 3 de mayo, de obligada observancia por parte de todas las entidades locales), así como esbozar un catálogo de los requisitos y responsabilidades más significativas que aquellos responsables públicos deben tener en cuenta para garantizar la seguridad de la información tratada y los servicios prestados por la entidad local de que se trate, en cada una de sus respectivas competencias y atribuciones.

Para no hacer el documento en exceso prolijo o repetitivo, se han aunado las consideraciones que puedan resultar comunes a distintos tipos de cargos electos (presidentes de Diputación y alcaldes; diputados y concejales, etc.) en una única categoría, respetando las denominaciones y funciones que el ordenamiento jurídico contempla para el caso de los Ayuntamientos.

3. La problemática de la ciberseguridad local

El mundo en el que vivimos está cambiando rápidamente, y las Administraciones Públicas no son una excepción. Hoy en día, muchas personas dependen de internet para las interacciones y transacciones cotidianas. **El paisaje de la Administración Local está cambiando también.** Frente a la disminución presupuestaria y al incremento de las expectativas en la prestación de los servicios públicos, los responsables locales deben encontrar formas innovadoras de garantizar la sostenibilidad de tales servicios. La situación de los Ayuntamientos en su devenir digital varía mucho de unos a otros, pero todos ellos, en mayor o menor profundidad, han tomado medidas para que más servicios públicos locales puedan estar disponibles digitalmente, trasladando parte de su personal a su sostenimiento o a colaborar de forma innovadora con otras organizaciones, públicas o privadas, y esta tendencia sigue en aumento.

En la actualidad, las **entidades locales** (Diputaciones Provinciales, Cabildos insulares o los propios Ayuntamientos) están utilizando una **gama cada vez mayor de elementos tecnológicos**, desde aplicaciones móviles y servicios en la nube, hasta el uso generalizado de muy diversos tipos de dispositivos electrónicos.

Los responsables locales deben encontrar formas innovadoras de garantizar la sostenibilidad de tales servicios.

El **personal de la Administración Local** (desde los presidentes, alcaldes, diputados y concejales hasta el último de los funcionarios, pasando por los secretarios, los tesoreros, los interventores, etc.), **desarrolla** una buena parte de sus **actividades telemáticamente**: se comunican con los ciudadanos y las empresas locales, llevan a cabo su trabajo y revisan los informes y documentos para las reuniones, expiden resoluciones de actos administrativos, etc., todo ello de forma electrónica.

Aunque existen normativas, protocolos y orientaciones sobre el manejo y el intercambio de datos, especialmente los de carácter sensible o confidencial y la mayoría de los Ayuntamientos suelen disponer de ciertas herramientas de seguridad en los sistemas de información gestionadas por sus servicios de informática, no podemos confiarnos: los autores de los ataques, persiguiendo intenciones delictivas u hostiles, seguirán intentando violar la seguridad de las organizaciones para sustraer los datos que tratan y/o dañar sus sistemas.

Aunque **el nivel de amenaza varía según los Ayuntamientos**, todos ellos poseen información o infraestructura de interés para los ciberatacantes.

Los Ayuntamientos deben considerar que se trata de "cuándo" y no de "si" se producirá un ciberataque. Por lo tanto, todos deben revisar, actualizar y reforzar continuamente su enfoque de ciberseguridad.

La ciberseguridad no sólo es crucial para garantizar que los servicios se mantengan en funcionamiento, sino que también **es vital para garantizar que los ciudadanos confíen en los Ayuntamientos cuando les remiten sus datos**. Un ciberataque podría tener consecuencias muy graves, tanto en términos de interrupción de los servicios -muchos de los cuales sirven a los más vulnerables- como por el daño a la reputación del propio Ayuntamiento. En resumen: una ciberseguridad adecuada y proporcionada a los riesgos es esencial para garantizar el funcionamiento eficiente de todas las entidades locales y el mejor servicio al ciudadano.

Los responsables locales deben encontrar formas nuevas e innovadoras de garantizar la sostenibilidad de tales servicios.

3.1 Amenazas y riesgos para las Entidades Locales

En el proceso de transformación digital en el que está inmerso el conjunto de la sociedad, las entidades locales (Diputaciones Provinciales, Cabildos insulares o Ayuntamientos) no se están quedando atrás. Todos ellos han ido tomando diferentes medidas para que, cada vez más, los servicios públicos locales puedan estar disponibles en Internet: desde aplicaciones móviles y servicios en la nube, hasta el uso generalizado de dispositivos electrónicos.

El personal de la Administración Local (desde los presidentes, alcaldes, diputados y concejales, pasando por funcionarios, secretarios, tesoreros o interventores), desarrollan una buena parte de sus actividades telemáticamente: se comunican con los ciudadanos y las empresas locales, llevan a cabo su trabajo y revisan los informes y documentos para las reuniones, expiden resoluciones de actos administrativos, etc., todo ello de forma electrónica.

Aunque el nivel de amenaza varía según los ayuntamientos, todos ellos poseen información o infraestructura de interés para los ciberatacantes. Por lo tanto, todos deben revisar, actualizar y reforzar continuamente su enfoque de la ciberseguridad.

Asimismo, **la ciberseguridad también es vital para garantizar que los ciudadanos confíen en los Ayuntamientos** cuando les remiten sus datos.

Entre las principales amenazas se encuentran las siguientes:

Ciberdelincuencia

Suelen perseguir el beneficio económico. Sus principales herramientas y métodos utilizados incluyen:



Malware: software malicioso tal como virus, troyanos, gusanos o cualquier código o contenido que pueda tener un impacto adverso en organizaciones o individuos.



Ransomware: un tipo de malware que bloquea los sistemas o los datos de los ordenadores de sus víctimas, permitiéndoles el acceso una vez que se satisface un pago (extorsión).



Phishing: correos electrónicos que simulan proceder de un organismo público o de una persona, persiguiendo extraer información sensible de los ciudadanos, del propio Ayuntamiento o sus responsables o empleados.



Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, etc.



Explotación de vulnerabilidades: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de las vulnerabilidades organizativas o técnicas del sistema atacado.



Denegación de Servicio: interrupción o ralentización de un servicio por múltiples peticiones (normalmente aplicaciones web).



Acceso no autorizado a la información: sustracción de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.



Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Hactivismo

Ataque a sitios web o cuentas de redes sociales para publicitar una causa concreta. Los grupos hactivistas han utilizado con éxito los ataques de Denegación de Servicio para interrumpir los sitios web de varios Ayuntamientos.

Personas con información privilegiada

Divulgación, intencionadamente o no, de información o datos sensibles al dominio público. La mayoría de las veces se debe a un simple error humano o a la falta de concienciación sobre los riesgos.

Amenazas físicas y terrorismo

Daños por catástrofes de todo tipo (fuego, agua, corte del suministro eléctrico, etc.).

Espionaje

Obtención de información valiosa, por sí misma, o que pueda usarse como mecanismo de entrada para la realización de ulteriores ataques.

4. El cumplimiento del Esquema Nacional de Seguridad en las EE.LL.

Como es sabido, el objeto del **Esquema Nacional de Seguridad (ENS)**¹ es determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos por parte de las entidades del sector público (y de aquellas organizaciones del sector privado que les presten servicios), estando constituido por los **principios básicos** y los **requisitos mínimos** para una protección adecuada de la información tratada y los servicios prestados, de obligatoria observancia por las entidades de su ámbito subjetivo de aplicación, para asegurar el **acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación** de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

La figura siguiente muestra el ámbito subjetivo de aplicación del ENS en lo tocante al ejercicio de potestades administrativas y a la prestación de servicios públicos².

El objeto del Esquema Nacional de Seguridad (ENS)¹ es determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos por parte de las entidades del sector público.

1. Operado por Real Decreto 311/2022, de 3 de mayo.

2. Como es sabido, el RD 311/2022, de 3 de mayo, extiende también su ámbito de aplicación subjetivo a los sistemas de información de las organizaciones del sector privado que formen parte de la cadena de suministro de las entidades públicas y a aquellos otros sistemas que tratan información clasificada.

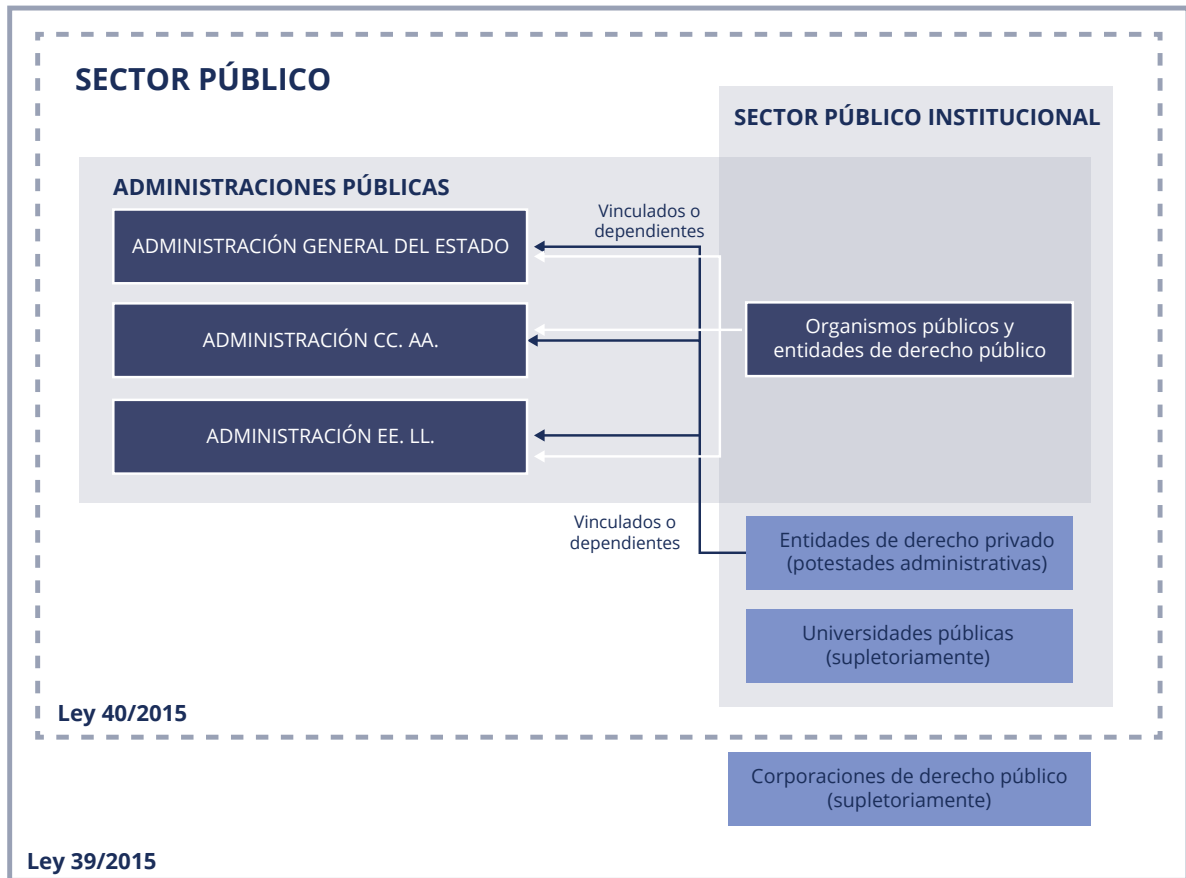


Figura 1. Aplicación del ENS

Consciente de la importancia de mantener la seguridad de los sistemas de información implicados en el desenvolvimiento de las funciones y competencias de las entidades públicas, el legislador dedica el artículo 31 y el Anexo III del ENS a materializar la exigencia de la realización de **auditorías de la seguridad** de los sistemas concernidos.

5. Los responsables públicos y la ciberseguridad

5.1 Órganos necesarios

Lo primero que hay que señalar es que, **el Gobierno y la administración municipal**, salvo en aquellos municipios que legalmente funcionen en régimen de Concejo Abierto, **corresponde al Ayuntamiento**, integrado por el **alcalde** y los **concejales**.

De conformidad con lo dispuesto en el art. 19 de la **Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL, en adelante**³, los concejales son elegidos mediante sufragio universal, igual, libre, directo y secreto, y el alcalde es elegido por los concejales o por los vecinos; todo ello en los términos que establezca la legislación electoral general.

El art. 35.2 del **Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales (ROF, en adelante)** califica como órganos necesarios:

El Gobierno y la administración municipal corresponde al Ayuntamiento, integrado por el alcalde y los concejales.

3. En Navarra sus entidades locales se rigen por la Ley Foral 6/1990, de la Administración Local de Navarra.



El alcalde



Los tenientes de alcalde



El Pleno



La Junta de Gobierno Local

En los municipios con población de derecho superior a 5.000 habitantes, así como, en los de menos, cuando así lo disponga su Reglamento orgánico o lo acuerde el Pleno de su Ayuntamiento.

5.1.1 El alcalde

El alcalde es el presidente de la Corporación y, entre otras **atribuciones**⁴ y, por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:



Dirigir el gobierno y la administración municipal y, en el marco del Reglamento orgánico, la **organización de los servicios administrativos de la Corporación**, lo que también comprende el gobierno de la seguridad de la información.

4. Recogidas en el art. 21 de la LBRL y el art. 41 del ROF.



Representar al Ayuntamiento, también ante las entidades públicas competentes en materia de ciberseguridad (como, por ejemplo, a la hora de ordenar la notificación de un incidente de seguridad con impacto significativo) o ante las entidades privadas (por ejemplo, exigiendo que los sistemas de información de los proveedores que prestan servicios a la entidad local sean conformes con lo dispuesto en el Esquema Nacional de Seguridad).



Convocar y presidir las sesiones del Pleno, de la Junta de Gobierno y de cualesquiera otros órganos municipales, así como **decidir los empates** con voto de calidad (como, por ejemplo, cuando el Pleno de la Corporación pueda debatir el contenido de la Política de Seguridad de la Información de la entidad local).



Hacer cumplir las Ordenanzas y Reglamentos municipales (como, por ejemplo, la Política de Seguridad de la Información de la entidad local o su Normativa Interna del Uso de los Medios Electrónicos).



Dirigir, impulsar e inspeccionar las obras y servicios cuya ejecución o realización hubiese sido acordada, recabando los asesoramientos técnicos necesarios (como, por ejemplo, cuando es necesaria o conveniente la contratación de proveedores tecnológicos externos para el suministro de productos o la prestación de servicios), lo que impactaría también en la contratación y concesión de obras, servicios y suministros cuya cuantía no exceda del 5% de los recursos ordinarios de su presupuesto, ni del 50% del límite general aplicable a la contratación directa, así como de todos aquellos otros que, excediendo de la citada cuantía, tengan una duración no superior a un año o no exijan créditos superiores a los consignados en el Presupuesto anual.



Desempeñar la jefatura superior de todo el personal, y acordar su nombramiento y sanciones, incluida la separación del servicio de los funcionarios de la Corporación y el despido del personal laboral (dirección e impulso que incluye, por ejemplo, la designación de los miembros del Comité de Seguridad de la Información o la designación de los responsables de la Información, los Servicios, el Sistema o la Seguridad, según dispone el Esquema Nacional de Seguridad).



El **ejercicio de las acciones judiciales y administrativas y la defensa del Ayuntamiento** en las materias de su competencia, incluso cuando las hubiere delegado en otro órgano y, en caso de urgencia, en materias de la competencia del Pleno, en este supuesto dando cuenta al mismo en la primera sesión que celebre para su ratificación.



La **aprobación de los proyectos de obras y de servicios** cuando sea competente para su contratación o concesión y estén previstos en el presupuesto (como, por ejemplo, velar porque los Pliegos de Prescripciones de los concursos públicos contengan los extremos necesarios para garantizar que los sistemas de información de que usa la entidad local -propios o externos- son conformes al ENS).



Ordenar la publicación, ejecución y hacer cumplir los acuerdos del Ayuntamiento (como, por ejemplo, la publicación en la sede electrónica de los Distintivos de Conformidad con el ENS de los que sea titular la entidad local).



Las demás que **expresamente le atribuyan las leyes** y aquellas que la legislación del Estado o de las comunidades autónomas asignen al municipio y no atribuyan a otros órganos municipales.

Conviene recordar que el alcalde puede **efectuar delegaciones en favor de la Junta de Gobierno Local**, como órgano colegiado, de forma que los acuerdos adoptados por esta en relación con las materias delegadas tendrán el mismo valor que las resoluciones que dicte el alcalde en ejercicio de las atribuciones que no haya delegado, sin perjuicio de su adopción conforme a las reglas de funcionamiento de la Junta de Gobierno⁵.

Además, el alcalde puede **delegar el ejercicio de determinadas atribuciones en los tenientes de alcalde**, cuando no exista Junta de Gobierno Local, sin perjuicio de las delegaciones especiales que, para cometidos específicos, pueda realizar en favor de cualesquiera Concejales, aunque no pertenecieran a la Junta de Gobierno Local.

Las denominadas **delegaciones genéricas** se referirán a una o varias áreas o materias determinadas (por ejemplo, aquellas relativas a la seguridad de los sistemas de información de la entidad), y podrán abarcar tanto la facultad de dirigir los servicios correspondientes como la de gestionarlos en general, incluida la facultad de resolver mediante actos administrativos que afecten a terceros.

Asimismo, el alcalde podrá efectuar **delegaciones especiales en cualquier concejal** para la dirección y gestión de asuntos determinados incluidos en las citadas áreas. En este caso, el concejal que ostente una delegación genérica tendrá la facultad de supervisar la actuación de los concejales con delegaciones especiales para cometidos específicos incluidos en su área⁶.

5. Art. 43.2 ROF.

6. Arts. 43.3 y 43.4 ROF.

Por la parte que pueda afectar a la seguridad de la información, dichas **delegaciones especiales** podrán ser⁷:



Relativas a un proyecto o asunto determinado.

En este caso, la eficacia de la delegación, que podrá contener todas las facultades delegables del alcalde, incluida la de emitir actos que afecten a terceros, se limitará al tiempo de gestión o ejecución del proyecto.



Relativas a un determinado servicio.

En este caso, la delegación comprenderá la dirección interna y la gestión de los servicios correspondientes, pero no podrá incluir la facultad de resolver mediante actos administrativos que afecten a terceros.

Todas las delegaciones anteriores serán realizadas mediante Decreto del alcalde que contendrá el ámbito de los asuntos a que se refiere la delegación, las facultades que se deleguen, así como las condiciones específicas de ejercicio de las mismas, en la medida en que se concreten o aparten del régimen general previsto en el ROF⁸.

En todo caso, las delegaciones que puede otorgar el alcalde a los miembros de la Junta de Gobierno Local, los tenientes de alcalde y las delegaciones especiales a los concejales, deberán adaptarse a las grandes áreas en que el Reglamento orgánico, en el caso de que hubiera sido aprobado por la Corporación, distribuya los servicios administrativos del Ayuntamiento⁹.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del ALCALDE (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

7. Art. 43.5 ROF.

8. Art. 44.1 ROF.

9. Art. 45 ROF.

5.1.2 Los tenientes de alcalde

Los tenientes de alcalde, que habrán sido nombrados por el alcalde¹⁰, sustituyen al alcalde, por el orden de su nombramiento y en los casos de vacante, ausencia o enfermedad, siendo libremente designados y removidos por este de entre los miembros de la Junta de Gobierno Local y, donde esta no exista, de entre los concejales¹¹.

El alcalde puede delegar el ejercicio de determinadas atribuciones en los miembros de la Junta de Gobierno Local y, donde esta no exista, en los tenientes de alcalde, sin perjuicio de las delegaciones especiales que, para cometidos específicos, pueda realizar en favor de cualesquiera concejales, aunque no pertenecieran a aquella¹².

5.1.3 El Pleno

El Pleno está integrado por todos los concejales y es presidido por el alcalde¹³.

Del Pleno, entre otras **atribuciones** y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:



El **control y la fiscalización de los órganos de gobierno** (como, por ejemplo, el control de los órganos de gobierno de la entidad local en relación con las acciones necesarias para garantizar la conformidad con el ENS).

10. Art. 21.2 LBRL.

11. Art. 23.2 LBRL.

12. Art. 23.4 LBRL.

13. Art. 22 LBRL.



La aprobación del Reglamento Orgánico y de las Ordenanzas. Al objeto de obtener el mayor consenso posible, también cabría incluir en estas competencias el debate y aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la entidad local.



La **aprobación de las formas de gestión de los servicios y de los expedientes de municipalización** (como puedan ser los servicios de administración digital dirigidos a los ciudadanos, para los que la seguridad de la información resulte esencial).



La **aprobación de la plantilla de personal y de la relación de puestos de trabajo**, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual (lo que también resulta de aplicación al personal de la entidad local directamente involucrado en tareas relativas a la seguridad de la información).



La **aprobación de los proyectos de obras y servicios** cuando sea competente para su contratación o concesión, y cuando aún no estén previstos en los presupuestos (como podría suceder, excepcionalmente, con la contratación de algún servicio relativo a la seguridad de la información).

De las competencias anteriores, **el Pleno puede delegar el ejercicio de sus atribuciones en el alcalde y en la Junta de Gobierno Local en los dos últimos casos señalados, exclusivamente.**

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del PLENO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.1.4 La Junta de Gobierno Local

La Junta de Gobierno Local está integrada por el alcalde, que la preside, y un número de concejales nombrados libremente por él como miembros de la misma, que no podrá superar al tercio del número legal de miembros de la Corporación¹⁴.

Es atribución propia e indelegable de la Junta de Gobierno Local la **asistencia permanente al alcalde** en el ejercicio de sus atribuciones.

La Junta de Gobierno será informada de todas las decisiones del alcalde, previamente a la adopción de la decisión, siempre que la importancia del asunto así lo requiera.

Es atribución propia e indelegable de la Junta de Gobierno Local la asistencia permanente al alcalde en el ejercicio de sus atribuciones.

14. Art. 23.1 LBRL.

De la Junta de Gobierno Local, entre otras **atribuciones** y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:



La **asistencia al alcalde** en el ejercicio de sus atribuciones¹⁵ (como sucede también con todo lo relativo a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local).



Las **atribuciones** que el alcalde o el Pleno **le delegue** o **le atribuyan** las leyes¹⁶.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas de la JUNTA DE GOBIERNO LOCAL (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

La siguiente figura muestra un esquema de las delegaciones reseñadas.

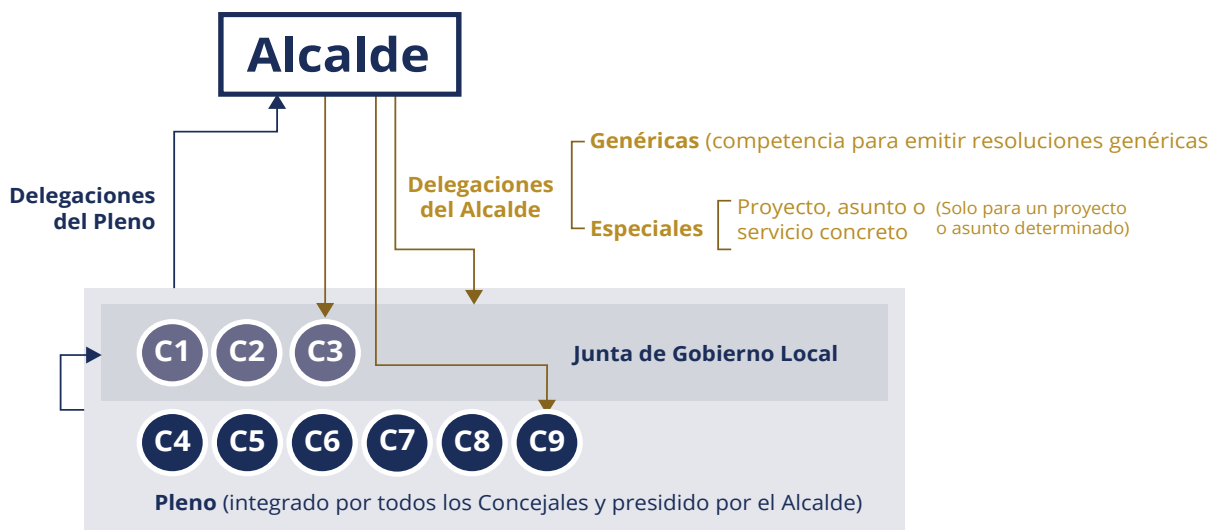


Figura 2. Esquema de las delegaciones

15. Art. 23.2.a) LBRL y art.53.1 ROF.

16. Art. 23.2.b) LBRL y art. 53.2 ROF.

5.2 Órganos complementarios

En función de la población del municipio, deberán existir otros **órganos complementarios**¹⁷:

- » **La Comisión especial de cuentas.**
- » **Las Comisiones informativas.**
- » **Los Consejos sectoriales.**
- » **Los concejales y diputados delegados.**
- » **Los órganos desconcentrados y descentralizados para la gestión de servicios.**

5.3 Funciones públicas de los habilitados nacionales: secretaríos e interventores

Son funciones públicas necesarias en todas las Corporaciones Locales, cuya responsabilidad administrativa está reservada a **funcionarios de Administración Local con habilitación de carácter nacional**, las siguientes¹⁸:



Secretaría

Comprensiva de la fe pública y el asesoramiento legal preceptivo.



Intervención-Tesorería

Comprensiva del control y la fiscalización interna de la gestión económico-financiera y presupuestaria, y la contabilidad, tesorería y recaudación.

¹⁷. Art. 119 ROF.

¹⁸. Art. 2 RJFAL (Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional).



Secretaría-Intervención

A la que corresponden las funciones de la fe pública y el asesoramiento legal preceptivo y las funciones de control y fiscalización interna de la gestión económica-financiera y presupuestaria, y la contabilidad, tesorería y recaudación.

Tales funcionarios tienen atribuida la dirección de los servicios encargados de su realización, sin perjuicio de las atribuciones de los órganos de gobierno de la Corporación Local en materia de organización de los servicios administrativos.

5.3.1 Los secretarios

En todas las entidades locales existirá un puesto de trabajo denominado **Secretaría**, al que corresponde la responsabilidad administrativa de las funciones de **fe pública** y **asesoramiento legal preceptivo** con el alcance y contenido previsto en el ordenamiento jurídico¹⁹.

De las **atribuciones** comprendidas en la función pública de la Secretaría y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:

19. Art. 7.1 RJFAL.

En cuanto a la **fe pública**²⁰:



Preparar los asuntos que hayan de ser **incluidos en el orden del día** de las sesiones que celebren el Pleno, la Junta de Gobierno y cualquier otro órgano colegiado de la Corporación en que se adopten acuerdos que vinculen a la misma, de conformidad con lo establecido por el alcalde o presidente de la misma, y la asistencia a este en la realización de la correspondiente convocatoria (incluyendo también todos aquellos asuntos relativos a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local).



Asistir y levantar acta de las sesiones de los órganos colegiados referidos en el punto anterior y publicarla en la sede electrónica de la Corporación de acuerdo con la normativa sobre protección de datos.



Transcribir en el Libro de Resoluciones, cualquiera que sea su soporte, las dictadas por la Alcaldía o Presidencia, por los miembros de la Corporación que resuelvan por delegación de las mismas, así como las de cualquier otro órgano con competencias resolutorias. Entre tales resoluciones estarán las relativas a la seguridad de la información de la entidad local.



Certificar todos los actos o resoluciones de la Presidencia y los acuerdos de los órganos colegiados decisorios, así como los antecedentes, libros y documentos de la Entidad Local, como los que puedan involucrar a actos o resoluciones relativas a la seguridad de la información de la entidad local.

20. Art. 3.2 RJFAL.



Anotar en los expedientes, bajo firma, **las resoluciones y acuerdos que recaigan**, así como **notificar dichas resoluciones** y acuerdos en la forma establecida en la normativa aplicable, incluyendo entre tales resoluciones y acuerdos aquellos que se refieran a acciones relativas a la seguridad de la información de la entidad.



Actuar como fedatario en la **formalización de todos los contratos, convenios y documentos análogos** en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la seguridad de la información de la entidad local.



Disponer que se publiquen, cuando sea preceptivo, los **actos y acuerdos** de la **entidad local** en los medios oficiales de publicidad, en el tablón de anuncios de la misma y en la sede electrónica, certificándose o emitiéndose diligencia acreditativa de su resultado si así fuera preciso, incluyendo todos los actos o Acuerdos relativos a la seguridad de la información de la entidad, como sería el caso de la publicación de los Distintivos de Conformidad con el ENS de los que la entidad local fuera titular.



Llevar y custodiar el Registro de Intereses de los miembros de la Corporación, el Inventario de Bienes de la Entidad Local y, en su caso, el Registro de Convenios, como todos aquellos Bienes (activos) y Convenios relativos a la seguridad de la información, propiedad o suscritos, respectivamente, por la entidad.



La **superior dirección de los archivos y registros de la Entidad Local**, incluyendo velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.

En cuanto al **asesoramiento legal**²¹:



La **emisión de informes previos** en aquellos supuestos en que así lo ordene el Presidente o Alcalde de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes **deberán señalar la legislación en cada caso aplicable** y la **adecuación a la misma** de los acuerdos en proyecto. (Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad).



La **emisión de informes previos** siempre que un **precepto legal** o **reglamentario** así **lo establezca** o la **emisión de informe previo** siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada, como podría ser el caso, entre otros, de la emisión de informes relativos a la modificación de Ordenanzas, Reglamentos o Estatutos rectores de Organismos de derecho público, sociedades mercantiles, fundaciones, etc., cuyos requisitos en materia de seguridad de la información hayan de modificarse.

21. Art. 3.3 RJFAL.



Informar en las sesiones de los órganos colegiados a las que asista y cuando medie requerimiento expreso de quien presida, acerca de los **aspectos legales del asunto que se discuta**, con objeto de colaborar en la corrección jurídica de la decisión que haya de adoptarse.



Acompañar al presidente o alcalde o a los miembros de la Corporación **en los actos de firma de escrituras** y, si así lo demandaren, en sus visitas a autoridades o asistencia a reuniones, a efectos de asesoramiento legal.



Asistir al presidente o alcalde de la Corporación, junto con el interventor, **para la formación del presupuesto**, a efectos procedimentales y formales, no materiales.



Emitir informes cuando así se establezca en la legislación sectorial.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del SECRETARIO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.3.2 Los interventores

En las Entidades Locales cuya Secretaría esté clasificada en clase primera o segunda, existirá un puesto de trabajo denominado **Intervención**²².

El control interno de la **gestión económico-financiera y presupuestaria** comprende, entre otras y por la parte que pudiera afectar a las actividades de la entidad local en materia de seguridad de la información:



La **función interventora**.



El **control financiero** en las modalidades de **función de control permanente** y la **auditoría pública**, incluyéndose en ambas el control de eficacia. El ejercicio del control financiero incluirá, en todo caso, las actuaciones de control atribuidas en el ordenamiento jurídico al órgano interventor, tales como:

1. El control de subvenciones y ayudas públicas.
2. El informe de los proyectos de presupuestos y de los expedientes de modificación de estos.
3. La emisión de informe previo a la concertación o modificación de las operaciones de crédito.
4. La emisión de informe previo a la aprobación de la liquidación del Presupuesto.

22. Art. 4 RJFAL.

5. La emisión de informes, dictámenes y propuestas que en materia económico-financiera o presupuestaria le hayan sido solicitadas por la Presidencia o la Alcaldía, o por un tercio de los concejales o diputados o cuando se trate de materias para las que legalmente se exija una mayoría especial, así como el dictamen sobre la procedencia de la implantación de nuevos Servicios o la reforma de los existentes a efectos de la evaluación de la repercusión económico-financiera y estabilidad presupuestaria de las respectivas propuestas.
6. Emitir los informes y certificados en materia económico-financiera y presupuestaria y su remisión a los órganos que establezca su normativa específica.

Por su parte, la **función de contabilidad** comprende, entre otras:



Llevar y desarrollar la contabilidad financiera y la de **ejecución del presupuesto** de la entidad local de acuerdo con las normas generales y las dictadas por el Pleno de la Corporación; formar la Cuenta General de la Entidad Local y formar, con arreglo a criterios usualmente aceptados, los estados integrados y consolidados de las cuentas que determine el Pleno de la Corporación.

**Coordinar las funciones o actividades contables**

de la **Entidad Local**, emitiendo las instrucciones técnicas oportunas e inspeccionando su aplicación.

**Organizar un adecuado sistema de archivo y conservación**

de toda la **documentación e información contable** que permita poner a disposición de los órganos de control los justificantes, documentos, cuentas o registros del sistema de información contable, por ellos solicitados en los plazos requeridos.

**Inspeccionar la contabilidad**

de los organismos autónomos, de las sociedades mercantiles dependientes de la Entidad Local, así como de sus entidades públicas empresariales, de acuerdo con los procedimientos que establezca el Pleno.

Competencias todas ellas que resultan también de aplicación a la gestión de aquellos expedientes tramitados por la entidad local en relación con la seguridad de la información.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del INTERVENTOR (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.3.3 Los tesoreros

En las Corporaciones Locales cuya Secretaría esté clasificada en primera o segunda clase existirá un puesto de trabajo denominado **Tesorería**.

La **función de tesorería** comprende, entre otras y por la parte que pudiera afectar a las actividades de la entidad local en materia de seguridad de la información²³:



La **titularidad y dirección** del órgano correspondiente de la entidad local.



El **manejo y custodia** de fondos, valores y efectos de la Entidad Local, de conformidad con lo establecido en las disposiciones legales vigentes.



La **dirección de los servicios de gestión financiera** de la Entidad Local y la propuesta de concertación o modificación de operaciones de endeudamiento y su gestión de acuerdo con las directrices de los órganos competentes de la Corporación.



La **elaboración y acreditación del periodo medio de pago a proveedores** de la entidad local, otros datos estadísticos e indicadores de gestión que, en cumplimiento de la legislación sobre transparencia y de los objetivos de estabilidad presupuestaria, sostenibilidad financiera, gasto público y morosidad, deban ser suministrados a otras administraciones o publicados en la web u otros medios de comunicación de la Entidad, siempre que se refieran a funciones propias de la tesorería.

23. Art. 5 RJFAL.

Por su parte, la **función de gestión y recaudación** comprende, entre otras:



La **jefatura** de los **servicios de gestión de ingresos y recaudación**.



El **impulso y dirección** de los **procedimientos de gestión y recaudación**.



La **tramitación de los expedientes de responsabilidad** que procedan en la gestión recaudatoria.

Competencias todas ellas que resultan también de aplicación a la gestión de aquellos expedientes tramitados por la entidad local en relación con la seguridad de la información.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del TESORERO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

6. La prestación de servicios externos

De conformidad con lo dispuesto en el ordenamiento jurídico vigente²⁴, cuando los operadores del sector privado presten servicios o provean soluciones a las entidades locales, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente **Declaración de Conformidad con el Esquema Nacional de Seguridad**, cuando se trate de sistemas de categoría BÁSICA, o la **Certificación de Conformidad con el Esquema Nacional de Seguridad**, cuando se trate de sistemas de categorías MEDIA o ALTA.

Es responsabilidad de las entidades locales contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, en el nivel y categoría de seguridad que corresponda en cada caso.

²⁴. Singularmente, la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

Además del Centro Criptológico Nacional (CCN) y la Entidad Nacional de Acreditación (ENAC), las entidades locales usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, podrán solicitar en todo momento a tales operadores, a través del CCN, los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones.

Para más información sobre la necesidad de que los sistemas de información usados por los proveedores tecnológicos de las entidades locales sean conformes con el ENS, puede consultarse la **Guía CCN-STIC 830** (<https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1674-ccn-stic-830-ambito-aplicacion-ens/file.html>) y la **Guía IC-01/19** (<https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/informes-cocens/371-ccn-cert-ic-01-19-criterios-generales-auditorias/file>).

7. Referencias

- ✿ RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- ✿ RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- ✿ Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- ✿ Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
- ✿ Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.
- ✿ Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- ✿ Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- ✿ Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- ✿ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ✿ Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información (ITS de Auditoría).
- ✿ Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (ITS de Conformidad).
- ✿ Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad (ITS de Informe del Estado de la Seguridad).
- ✿ Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad (ITS de Notificación de Incidentes de Seguridad).
- ✿ Guía CCN-CERT IC-01/19 Criterios Generales Auditorías.
- ✿ CCN-CERT IC-02/20 Guía para la contratación de auditorías de certificación del Esquema Nacional de Seguridad (ENS).
- ✿ Guía CCN-STIC 830 Ámbito de aplicación del Esquema Nacional de Seguridad.
- ✿ Guía Nacional de Notificación y Gestión de Ciberincidentes, aprobada por el Consejo Nacional de Ciberseguridad el 21 de febrero de 2020.
- ✿ FEMP: Guía Estratégica en seguridad para entidades locales: Esquema Nacional de Seguridad. Tomos I y II.
- ✿ Guía CCN-STIC 801 Responsabilidades y Funciones en el ENS.
- ✿ BP 01/21 Informe de Buenas Prácticas sobre Principios y recomendaciones básicas en Ciberseguridad.
- ✿ BP 21/01 Informe de Buenas Prácticas en Gestión de Incidentes de Ransomware.

Anexo: Tabla de Funciones y Responsabilidades

Leyenda

- A** – Aprobación y responsabilidad de las acciones emprendidas por la entidad local para satisfacer el requisito.
- ADP** – Aprobación por Delegación del Pleno.
- R** – Responsable de acometer (total o parcialmente) el requisito, dentro de las competencias o atribuciones del cargo.
- RDA** – Responsable de acometer y aprobar la función, por delegación del alcalde.

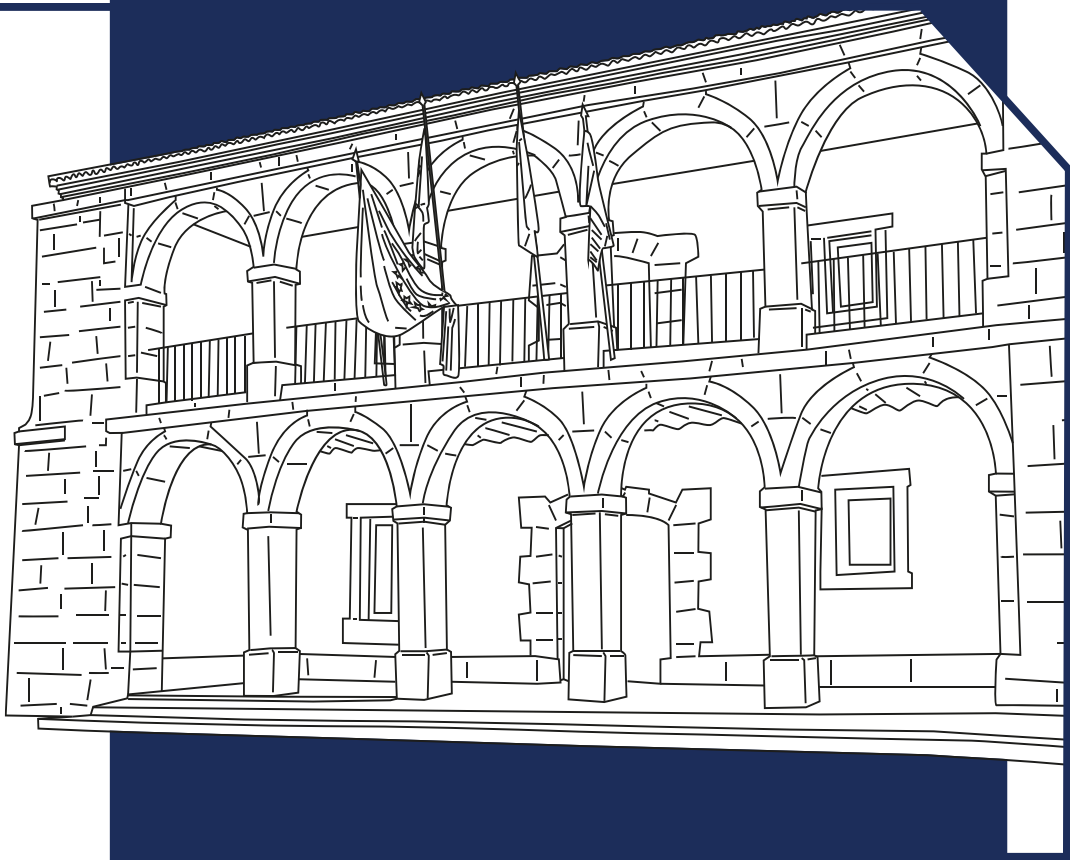
Notas

1. Cuando la responsabilidad R o RDA se repita en un mismo requisito, se entenderá que tal responsabilidad podría ejercerse, alternativamente, por cada uno de los responsables mencionados.
2. No se han incluido las funciones asignadas al Comité de Seguridad de la Información, y a los responsables de la Información, del Servicio, de la Seguridad y del Sistema, cuyas responsabilidades se encuentran recogidas en la Guía CCN-STIC 801.

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
1, 2, 5, 10, 32, 38	Velar por la conformidad general con el ENS de los sistemas de información de la entidad local.	A		RDA	RDA	R	R
Con carácter general	La superior dirección de los archivos y registros de la entidad local, incluyendo velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.					R	
ITS de Conformidad	Velar por que los sistemas de información de la entidad local posean las Declaraciones y/o Certificaciones de Conformidad con el ENS y que los Distintivos correspondientes se muestran en la sede electrónica de la entidad.	A		RDA	RDA	R	
ITS de Conformidad	Disponer que se publiquen, cuando sea preceptivo, los actos y acuerdos de la entidad local en los medios oficiales de publicidad, en el tablón de anuncios de la misma y en la sede electrónica, certificándose o emitiéndose diligencia acreditativa de su resultado si así fuera preciso, incluyendo todos los actos o Acuerdos relativos a la seguridad de la información de la entidad, como sería el caso de la publicación de los Distintivos de Conformidad con el ENS de los que la entidad local fuera titular.					R	
11, [op.acc.2]	Determinación de la composición del Comité de Seguridad de la Información y nombramiento del responsable de la Información, de los Servicios, de la Seguridad, del Sistema y su adecuada segregación.	A		RDA	RDA	R	
12	Velar por la existencia y adecuación de la Política de Seguridad de la Información y la Normativa Interna de la entidad.	R		RDA	RDA	R	
12, [org.1], [org.2]	Aprobación de la Política de Seguridad de la Información y de la Normativa Interna del Uso de los Medios Electrónicos de la entidad local.	ADP	A				
13	Velar por la organización e implantación del proceso de seguridad.	A		RDA	RDA	R	R
14, [op.pl.1]	Velar por la utilización de los principios de análisis y gestión de los riesgos en el proceso de seguridad de la información de la entidad y aprobar el Análisis de Riesgos para los sistemas de información de la entidad.	A		RDA	RDA	R	
15, 16	Aprobación de la plantilla de personal y de la relación de puestos de trabajo, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual	ADP	A	ADP			R
15, 16	Velar por la adecuada gestión del personal y su profesionalidad.	A		RDA	RDA	R	R
[op.exp.7] ITS de Notificación	Velar por el cumplimiento de la adecuada notificación de incidentes al Centro Criptológico Nacional.	A		RDA	RDA	R	
[op.ext]	Velar por que los sistemas de información de los proveedores externos que presten servicios a la entidad sean conformes con el ENS, posean los Acuerdos de Nivel de Servicio idóneos y se gestione adecuadamente su cumplimiento.	A		RDA	RDA	R	R
[op.ext]	Aprobación de los proyectos de obras y servicios, incluidos los relativos a la seguridad de la información, cuando sea competente para su contratación o concesión, y cuando aún no estén previstos en los presupuestos.	ADP	A	ADP		R	R
[op.ext]	Actuar como fedatario en la formalización de todos los contratos, convenios y documentos análogos en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la seguridad de la información de la entidad local.					R	
[op.cont]	Velar por la adecuada continuidad de los servicios en caso de impacto, incluyendo la aprobación del correspondiente Análisis de Impacto.	A		RDA	RDA	R	
[mp.if]	Velar por la protección de las infraestructuras físicas y lógicas de la entidad, incluyendo su acondicionamiento y abastecimientos y, en su caso, la disponibilidad de instalaciones alternativas, así como la identificación de las personas, especialmente cuando puedan tener acceso a los sistemas de información de la entidad.	A		RDA	RDA	R	R
[mp.per]	Velar por que el personal que trabaja en la entidad local esté debidamente concienciado y/o formado en materia de seguridad de la información.	A		RDA	RDA	R	R
[mp.info]	Velar por que la información tratada por la entidad, especialmente cuando se trate de datos personales, se custodie adecuadamente, de conformidad con las regulaciones que resulten de aplicación, calificándola de acuerdo con su naturaleza.	A		RDA	RDA	R	
[mp.info.4]	Velar por que se utilizan los procedimientos de firma electrónica, sello electrónico y sello de tiempo electrónico, atendiendo a los procedimientos administrativos de que se trate, de conformidad con la legislación vigente.	A		RDA	RDA	R	
[Anexo III], ITS de Auditoría	Velar por que se realice periódicamente una auditoría de conformidad con el ENS y, si procede, una auditoría externa de certificación, cada dos años o siempre que se hayan producido cambios en los sistemas de información afectados que induzcan a pensar que no son eficaces las medidas de seguridad adoptadas.	A		RDA	RDA	R	R
Con carácter general	Preparar los asuntos que hayan de ser incluidos en el orden del día de las sesiones que celebren el Pleno, la Junta de Gobierno y cualquier otro órgano colegiado de la Corporación en que se adopten acuerdos que vinculen a la misma, incluyendo también todos aquellos asuntos relativos a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local.					R	
Con carácter general	Transcribir en el Libro de Resoluciones, cualquiera que sea su soporte, las dictadas por la Alcaldía o Presidencia, por los miembros de la Corporación que resuelvan por delegación de las mismas, así como las de cualquier otro órgano con competencias resolutorias. Entre tales resoluciones estarán las relativas a la seguridad de la información de la entidad local.					R	
Con carácter general	Certificar todos los actos o resoluciones de la Alcaldía o Presidencia y los acuerdos de los órganos colegiados decisorios, así como los antecedentes, libros y documentos de la entidad, como los que puedan involucrar a actos o resoluciones relativas a la seguridad de la información de la entidad local.					R	
Con carácter general	Anotar en los expedientes, bajo firma, las resoluciones y acuerdos que recaigan, así como notificar dichas resoluciones y acuerdos en la forma establecida en la normativa aplicable, incluyendo entre tales resoluciones y acuerdos aquellos que se refieran a acciones relativas a la seguridad de la información de la entidad.					R	
Con carácter general	Llevar y custodiar el Registro de Intereses de los miembros de la Corporación, el Inventario de Bienes de la Entidad Local y, en su caso, el Registro de Convenios, como todos aquellos Bienes (activos) y Convenios relativos a la seguridad de la información de la entidad.					R	
Con carácter general	La emisión de informes previos en aquellos supuestos en que así lo ordene el Presidente o Alcalde de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes deberán señalar la legislación en cada caso aplicable y la adecuación a la misma de los acuerdos en proyecto. (Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad).					R	
Con carácter general	La emisión de informes previos siempre que un precepto legal o reglamentario así lo establezca o la emisión de informe previo siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada, como podría ser el caso, entre otros, de la emisión de informes relativos a la aprobación o modificación de Ordenanzas, Reglamentos o Estatutos rectores de Organismos de derecho público, sociedades mercantiles, fundaciones, etc., cuyos requisitos en materia de seguridad de la información hayan de modificarse.					R	
Con carácter general	Asistir al presidente o alcalde de la Corporación para la formación del presupuesto, a efectos procedimentales y formales, no materiales.					R	R

Prontuario de ciberseguridad para entidades locales

Centro Criptológico Nacional y
Federación Española de Municipios y Provincias



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS



centro criptológico nacional