



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

CERTIFICADO

LUCÍA MOLARES PÉREZ, CONCEJALA-SECRETARIA DE LA JUNTA DE GOBIERNO LOCAL, EN EL AYUNTAMIENTO DE POZUELO DE ALARCÓN (MADRID)

CERTIFICO: Que la Junta de Gobierno Local, en sesión Ordinaria celebrada 09-09-2026, al punto 6 **“APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CONFORME AL REAL DECRETO 311/2022, DE 3 DE MAYO. EXPTE. UNI/2026/138”** adoptó el siguiente acuerdo:

“El expediente ha sido examinado en la sesión de 4 de septiembre de 2026 por la Comisión General de Coordinación.

Vista la propuesta de la Segunda Teniente de Alcalde, Titular del Área de Gobierno de Economía, Hacienda y Digitalización, de fecha 3 de septiembre de 2026, que se transcribe:

“HECHOS

PRIMERO. - Con fecha 07-05-2026, mediante Resolución de la Directora General de Seguridad, Innovación, Administración Digital y Emprendimiento, expediente UNI/2026/58, se adjudicó a la empresa Ingeniería informática Net Computer ECUS, SL., contrato de servicio de consultoría técnica especializada para la implantación del ENS.

SEGUNDO. - Con fecha 22/07/2026 se emite informe técnico por el jefe de sección de innovación, mediante el que se informa lo siguiente:

“Este técnico informa favorablemente y considera necesaria la aprobación de la Política de Seguridad de la Información adjunta, por constituir una obligación legal derivada del artículo 12 del Real Decreto 311/2022 y del artículo 156.2 de la Ley 40/2015, y por ser el instrumento que permite dar cobertura documentada y verificable a los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad expuestos en los apartados anteriores”.

TERCERO. – Consta en el expediente la siguiente documentación:

- Documento con la Política de Seguridad de la Información
- Acta de constitución del Comité de Seguridad de la Información
- Informe técnico emitido por el Jefe de Sección de Innovación



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- Informe propuesta emitido por el Técnico de Administración General de la Unidad Jurídica de Seguridad

De los anteriores antecedentes de hecho resultan de aplicación los siguientes

FUNDAMENTOS DE DERECHO

PRIMERO. – El artículo 2 de la Ley 40/2015, de 1 de octubre, reguladora del Régimen Jurídico del Sector Público (LRJSP) establece que “las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.”

En este sentido, el artículo 156.2 LRJSP dispone que “el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.”

Por su parte el artículo 2.1 de la citada Ley determina que será de aplicación a las entidades que integran la Administración Local.

SEGUNDO. - El artículo 13.h) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) configura como derecho de las personas en sus relaciones con las Administraciones Públicas “a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.”

TERCERO. - El artículo 5.3 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo, aplicable al conjunto de las Administraciones Públicas, dispone que “los portales de internet dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.”

El Real Decreto 3/2010 fue derogado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

CUARTO. - El Real Decreto 311/2022, de 3 de mayo resulta de aplicación a las entidades locales, tal y como señala su artículo 2.1 por lo que atendiendo a lo dispuesto en el 12.2:



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

“cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente”.

QUINTO. - *En cuanto al órgano competente, el artículo 2.3.II del Reglamento señala que “la política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas”.*

Visto el contenido de la Política de Seguridad de la Información elaborada para el Ayuntamiento de Pozuelo de Alarcón en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en base a los anteriores antecedentes de hecho y fundamentos jurídicos, se propone a la Junta de Gobierno Local que adopte el siguiente

ACUERDO

ÚNICO. - *APROBAR la Política de Seguridad de la Información del Ayuntamiento de Pozuelo de Alarcón, conforme a lo dispuesto en el artículo 12.2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

ÍNDICE

<u>1. APROBACIÓN Y ENTRADA EN VIGOR</u>	3
<u>2. INTRODUCCIÓN</u>	3
<u>3. PRINCIPIOS Y DIRECTRICES</u>	4
<u>3.1 PREVENCIÓN</u>	4
<u>3.2 DETECCIÓN</u>	4
<u>3.3 RESPUESTA</u>	4
<u>3.4 RECUPERACIÓN</u>	5
<u>4. MISIÓN DEL AYUNTAMIENTO</u>	5
<u>5. ALCANCE</u>	5
<u>6. MARCO NORMATIVO</u>	5



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

7. MARCO DOCUMENTAL DE SEGURIDAD	6
8. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD	7
8.1 LA SEGURIDAD COMO UN PROCESO INTEGRAL Y MÍNIMO PRIVILEGIO	7
8.2 VIGILANCIA CONTINUA, REEVALUACIÓN PERIÓDICA E INTEGRIDAD, ACTUALIZACIÓN DEL SISTEMA Y MEJORA CONTINUA DEL PROCESO DE SEGURIDAD	7
8.3 GESTIÓN DE PERSONAL Y PROFESIONALIDAD	8
8.4 GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS, ANÁLISIS Y GESTIÓN DE RIESGOS	9
8.5 INCIDENTES DE SEGURIDAD, PREVENCIÓN, DETECCIÓN, REACCIÓN Y RECUPERACIÓN	9
8.6 EXISTENCIA DE LÍNEAS DE DEFENSA Y PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS	10
8.7 DIFERENCIACIÓN DE RESPONSABILIDADES, ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD	10
8.8 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS	10
8.9 PROTECCIÓN DE LAS INSTALACIONES	11
8.10 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD	11
8.11 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO Y CONTINUIDAD DE LA ACTIVIDAD	11
8.12 REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO	11
8.13 INFRAESTRUCTURAS Y SERVICIOS COMUNES	12
8.14 PERFILES DE CUMPLIMIENTO ESPECÍFICOS Y ACREDITACIÓN DE ENTIDADES DE IMPLEMENTACIÓN DE CONFIGURACIONES SEGURAS	12
8.15 SEGURIDAD EN EL TELETRABAJO	12
9. MODELO DE GOBERNANZA	13
9.1 ROLES O PERFILES DE SEGURIDAD	13
9.2 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	13
9.3 RESPONSABILIDADES ASOCIADAS AL ESQUEMA NACIONAL DE SEGURIDAD	14



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

<u>9.4 FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN</u>	16
<u>9.5 GABINETE DE GESTIÓN DE CRISIS DE CIBERINCIDENTES</u>	17
<u>9.6 PROCEDIMIENTOS DE DESIGNACIÓN</u>	19
<u>9.7 RESOLUCIÓN DE CONFLICTOS</u>	19
<u>10.DATOS DE CARÁCTER PERSONAL</u>	19
<u>11.TERCERAS PARTES</u>	19

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día de la propia firma por resolución de Alcaldía-Presidencia del Ayuntamiento de Pozuelo de Alarcón.

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

El Ayuntamiento de Pozuelo de Alarcón, en adelante Ayuntamiento, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

PRINCIPIOS Y DIRECTRICES

Los principios y directrices que se contemplan desde el Ayuntamiento a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

PREVENCIÓN

El Ayuntamiento con todos sus departamentos y áreas funcionales evita, o al menos en la medida de lo posible evita, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos tienen implementado las medidas mínimas de seguridad determinadas por este documento, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de esta política, el Ayuntamiento

- Autoriza los sistemas TI antes de entrar en operación.*
- Evalúa y monitoriza regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- *Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.*

3.2 DETECCION

Dado que los servicios y los sistemas se pueden degradar rápidamente debido a incidentes, se monitoriza la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a las o los responsables regularmente y en el momento en que se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3 RESPUESTA

El ayuntamiento debe:

- *Establecer mecanismos para responder eficazmente a los incidentes de seguridad.*
- *Designar el punto de contacto para las comunicaciones con respecto a incidentes detectados en los departamentos o en otros organismos relacionados con el Ayuntamiento.*

3.4 RECUPERACION

Para garantizar la disponibilidad de los servicios críticos, el Ayuntamiento debe desarrollar planes de continuidad de los sistemas TI como parte de su plan general de continuidad de negocio y actividades de recuperación.

MISIÓN DEL AYUNTAMIENTO

El Ayuntamiento, para la gestión de sus intereses y de las funciones y competencias que tiene atribuidas en diferentes normas o convenios, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

y aspiraciones de la población. Para ello pone a disposición de esta la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

MARCO NORMATIVO

El marco legal y regulatorio que afecta al desarrollo de las actividades y competencias del Ayuntamiento, en el ámbito del ENS, está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la ciberseguridad y seguridad de la información en general, así como a la protección de datos personales.

Las normas jurídicas que constituyen dicho marco se encuentran recogidas en un registro dispuesto al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

También forman parte del marco legal y regulatorio las restantes normas aplicables a la Administración Electrónica del Ayuntamiento, que sean desarrollo de las anteriores o estén relacionadas con ellas, comprendidas dentro del ámbito de aplicación de la presente Política.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Entre ellas, cabe destacar las instrucciones técnicas de seguridad, de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en la Disposición adicional segunda del Real Decreto por el que se regula el ENS.

El mantenimiento del precitado registro conteniendo el marco legal y regulatorio es responsabilidad del Ayuntamiento, pudiendo reflejarse asimismo como un anexo vinculado a esta política, aunque independiente, que no requerirá del mismo proceso formal de aprobación.

Así mismo, el Ayuntamiento, también será responsable de identificar las guías de seguridad elaboradas por el CCN en el ejercicio de sus competencias, referenciadas igualmente en la Disposición adicional segunda del Real Decreto por el que se regula el ENS, que serán de aplicación para facilitar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

MARCO DOCUMENTAL DE SEGURIDAD

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La presente Política se desarrollará mediante la documentación de seguridad que resulte necesaria, organizada, al menos, en los siguientes niveles:

- **Primer nivel:** Política de Seguridad de la Información.
- **Segundo nivel:** Normativas y procedimientos de seguridad.
- **Tercer nivel:** Procedimientos técnicos e instrucciones operativas.
- **Cuarto nivel:** Registros, evidencias, informes, actas, auditorías y demás documentación de soporte.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Toda la documentación deberá mantenerse actualizada, controlada, accesible para quienes deban aplicarla y alineada con el Esquema Nacional de Seguridad y con el marco organizativo del Ayuntamiento.

CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD

El Ayuntamiento para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.*
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- c) *En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.*
- d) *Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.*

Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario. Para ello se seguirán los principios de:

- ***Adaptabilidad:*** Ajuste a cambios tecnológicos, regulatorios y organizativos.
- ***Evaluación basada en evidencia:*** Revisión fundamentada en auditorías, incidentes y análisis de riesgos.
- ***Coordinación multidisciplinaria:*** Participación de responsables municipales para su correcta aplicación.
- ***Mejora Continua:*** Revisión periódica para optimizar su eficacia.
- ***Supervisión del CSI:*** El Comité de Seguridad de la Información revisará propuestas de actualización y garantizará su alineación con las directrices de la Comunidad de Madrid al mismo tiempo que supervisará el cumplimiento normativo asegurando la actualización de las medidas de seguridad. Dentro del proceso de supervisión, actualización y mejora continua se elevarán a la



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Alcaldía los informes de supervisión y mejora, el grado de cumplimiento y eficacia de las medidas.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información del Ayuntamiento dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación

El Ayuntamiento, dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Las medidas de detección irán dirigidas a descubrir la presencia de un ciber incidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “MODELO DE GOBERNANZA” del presente documento.

Autorización y control de los accesos

El Ayuntamiento, ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas, ya sea de manera física o lógica.

Protección de las instalaciones

El Ayuntamiento, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino

El Ayuntamiento, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

El Ayuntamiento, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

Seguridad en el teletrabajo

Debido a los problemas de inseguridad de Internet, no se debe transferir información de la organización por este medio a los domicilios particulares. En caso de teletrabajo, se solicitará autorización al Área de Informática para teletrabajar utilizando redes privadas virtuales (VPN). Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada está libre de virus o código malicioso.

Cuando los equipos o la información propiedad del Ayuntamiento de Pozuelo de Alarcón se encuentran fuera de las instalaciones, el responsable de su seguridad es quien los está utilizando, y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

Estas medidas se desarrollan con mayor detalle en la Norma de Teletrabajo Seguro del Ayuntamiento.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en el Ayuntamiento, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- **Responsable de Información y Servicios:** Titular de la Concejalía competente en materia de Administración Digital, con el apoyo de la Dirección General competente en materia de Administración Digital y/o seguridad.
- **Responsable de Seguridad de la Información del ENS:** Jefe de sección de Innovación
- **Responsable del Sistema del ENS:** Jefe de negociado de sistemas de información

Comité de Seguridad de la Información

El Ayuntamiento constituye un Comité de Seguridad de la Información, está formado por los siguientes miembros:

- **Presidencia:** Titular de la Concejalía competente en materia de Administración Digital.
- **Secretaría:** Responsable de Seguridad de la Información
- **Responsable de información:** Titular de la Concejalía competente en materia de Administración Digital, con el apoyo de la Dirección General competente en materia de Administración Digital y/o seguridad.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- **Responsable del servicio:** Titular de la Concejalía competente en materia de Administración Digital, con el apoyo de la Dirección General competente en materia de Administración Digital y/o seguridad.
- **Responsable de seguridad:** Jefe de sección de Innovación
- **Responsable del sistema:** Jefe de negociado de sistemas de información
- **DPD** (Con voz y sin voto)
- **Dirección General de Administración Digital y/o Seguridad:** miembro permanente y de apoyo directivo.

La formalización de estos puestos queda reflejada en el documento de constitución, composición y funciones del Comité de Seguridad, con los nombres designados a cada rol.

Puesto que el Comité de Seguridad de la Información es un órgano de gobernanza, coordinación, seguimiento y mejora continua del ENS, de carácter funcional y técnico, y no exclusivamente técnico, podrá recabar regularmente de personal técnico, propio o externo, así como de las unidades municipales afectadas, la información pertinente para la toma de decisiones, seguimiento o asesoramiento. A saber:

- responsables de otras áreas
 - direcciones generales
 - concejalías
 - órganos directivos
 - unidades municipales
 - entidades dependientes o proveedores
 - Asesoría jurídica

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Ayuntamiento y/o telemáticamente con periodicidad anual, previa convocatoria al efecto realizada por el Presidente de dicho Comité o cualquiera de sus miembros y/o, cuando haya un cambio relevante en el sistema de información.



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

El Comité de Seguridad de la Información, se encargará también, de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

Para asegurar su imparcialidad, el Delegado de Protección de Datos, actuará con voz y sin voto.

Atendiendo al alcance de los sistemas y servicios incluidos en el ENS, podrán participar en el Comité, como vocales funcionales o miembros de participación permanente, las personas titulares o representantes designados de aquellas unidades municipales directamente vinculadas a dicho alcance, en particular las relacionadas con el registro, padrón, gestión documental y archivo, gestión tributaria, atención a la ciudadanía y administración digital.

Asimismo, la Presidencia del Comité, por iniciativa propia o a propuesta del Responsable de la Información, del Responsable del Servicio o del Responsable de Seguridad, podrá convocar a responsables de otras áreas, concejalías, direcciones generales, órganos directivos, unidades municipales, entidades dependientes o terceros cuando resulte necesario para el ejercicio de las funciones del Comité. En tales casos, su colaboración, asistencia o, en su defecto, la designación de una persona representante con capacidad suficiente para informar y coordinar actuaciones tendrá carácter preceptivo.

Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad del ENS:

Funciones del responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.*
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Funciones del responsable de la Seguridad

- *Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.*
- *Promover la formación y concienciación en materia de seguridad de la información.*
- *Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.*
- *Determinar la categoría del sistema, en colaboración con el responsable del Sistema y/o Comité de Seguridad de la Información.*
- *Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.*
- *Gestionar las auditorías y revisiones, externas o internas, de la seguridad del sistema.*
- *Gestionar los procesos de certificación.*
- *Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.*
- *Podrá desplegar otras funciones derivadas de otras normas jurídicas de aplicación, siempre que concurren los requisitos de conocimiento, experiencia, independencia y en su caso titulación.*

Funciones del responsable del Sistema

- *Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.*
- *Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.*
- *Elaborar los procedimientos operativos necesarios.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- *Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.*
- *Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.*
- *Prestar al responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.*
- *Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.*
- *Llevar a cabo las funciones del administrador de la seguridad del sistema, en el caso de no estar designado explícitamente dicho rol.*
- *La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.*
- *La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.*
- *Aprobar los cambios en la configuración vigente del Sistema de Información.*
- *Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.*
- *Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.*
- *Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.*
- *Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Funciones del Comité de Seguridad de la Información

Las funciones propias de un Comité de Seguridad de la Información son las siguientes:

- *Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.*
- *Asesorar en materia de Seguridad de la Información.*
- *Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.*
- *Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:*
 - *Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.*
 - *Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.*
 - *Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.*
 - *Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.*
 - *Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- *Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.*
- *Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.*
- *Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.*
- *Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.*
- *Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.*
- *Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.*

Gabinete de Gestión de Crisis de Ciberincidentes

El Ayuntamiento podrá activar un Gabinete de Gestión de Crisis de Ciberincidentes como estructura específica de dirección y coordinación ante incidentes graves de ciberseguridad o crisis tecnológicas con impacto relevante en los servicios municipales, en la seguridad de la información o en la continuidad operativa.

El Gabinete de Gestión de Crisis de Ciberincidentes tendrá por finalidad coordinar la respuesta estratégica, organizativa y técnica ante este tipo de situaciones, facilitar la toma de decisiones urgentes, priorizar la recuperación de los servicios afectados y asegurar la adecuada coordinación entre las áreas implicadas.

Su activación podrá acordarse cuando concurra, entre otros, alguno de los siguientes supuestos:

- *incidentes graves de ciberseguridad con afectación significativa a sistemas o servicios municipales;*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  171O 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

- *interrupciones prolongadas o críticas de servicios electrónicos a la ciudadanía;*
- *incidentes con posible afectación masiva a datos personales o información sensible;*
- *ciberataques con impacto institucional, reputacional, operativo o de coordinación con terceros y autoridades.*

A título ejemplificativo, el Gabinete de Gestión de Crisis de Ciberincidentes podrá ser convocado en situaciones como un ataque de ransomware con cifrado de sistemas municipales, la caída prolongada de la sede electrónica o del registro, una intrusión con compromiso de credenciales privilegiadas, una brecha de datos personales de especial relevancia o cualquier incidente que exija decisiones extraordinarias de contención, comunicación, recuperación o continuidad.

El Gabinete de Gestión de Crisis de Ciberincidentes estará integrado, con carácter mínimo, por:

- *Presidencia: Alcaldía o persona en quien delegue.*
- *Titular de la Concejalía competente en materia de Administración Digital.*
- *Responsable de Seguridad.*
- *Responsable del Sistema.*
- *Responsable del Servicio.*
- *Responsable de la Información.*
- *Dirección General de Administración Digital y/o Seguridad.*

Podrán incorporarse, cuando la naturaleza del incidente lo requiera:

- *Comunicación, cuando el incidente requiera la gestión de la comunicación institucional o externa;*
- *Asesoría Jurídica, cuando resulten necesarias valoraciones o actuaciones de carácter jurídico;*
- *Delegado de Protección de Datos, cuando exista afectación a datos personales;*
- *Policía Local, cuando el incidente tenga implicaciones en seguridad física, accesos, edificios, videovigilancia o coordinación con emergencias;*
- *otras direcciones generales, concejalías, órganos directivos, unidades municipales, entidades dependientes o proveedores críticos.*

El funcionamiento detallado, criterios de activación, escalado, comunicación, recuperación, cierre y seguimiento del Gabinete de Gestión de Crisis de



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

Ciberincidentes se desarrollarán en la documentación interna y en los procedimientos de continuidad y gestión de incidentes que resulten de aplicación.

Procedimientos de designación

La designación de los Responsables identificados en esta Política ha sido realizada por Alcaldía-Presidencia del Ayuntamiento, y comunicada a las partes afectadas mediante notificación firmada por Secretaría.

Los roles de seguridad serán revisados cada cuatro años en el caso de que exista una vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

Resolución de conflictos

Si hubiera conflicto entre los responsables, será resuelto por el Comité de Seguridad de la Información.

DATOS DE CARÁCTER PERSONAL

El Ayuntamiento, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

TERCERAS PARTES

Cuando se preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento, definirá y aprobará los canales para la coordinación de la



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Ayuntamiento lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, 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.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

IMPORTANTE: *La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información, que propondrá, en caso de ser necesario, sus*



ÓRGANO O UNIDAD ADMINISTRATIVA Unidad del Órgano de Apoyo a la Junta de Gobierno Local	
PROCEDIMIENTO Gestión y ejecución de las sesiones de la Junta de Gobierno Local	
CÓDIGO DE VERIFICACIÓN DE DOCUMENTOS  1710 4G3H 500I 2E0D 03QC	
CÓDIGO DEL DOCUMENTO OAJ1AI02B0	CÓDIGO DEL EXPEDIENTE OAJ/2026/107

modificaciones o actualizaciones para su aprobación por el órgano competente en cada caso. Las modificaciones de la presente Política requerirán aprobación formal del órgano competente. Las modificaciones de la normativa, procedimientos, instrucciones y demás documentación de desarrollo del ENS podrán ser aprobadas por el responsable designado para cada área en el Comité de Seguridad.”

*Se acuerda en votación ordinaria y por unanimidad de los miembros presentes **APROBAR** la propuesta de resolución transcrita, en sus propios y literales términos.”*

Y para que así conste en el expediente, en cumplimiento de lo establecido en el artículo 51.2 del Reglamento Orgánico de Gobierno y Administración, y a reserva de los términos que resulten de la aprobación del acta, expido la presente de orden y con el Vº Bº de la Sra. Alcaldesa en Pozuelo de Alarcón a fecha de firma.

Vº Bº
ALCALDESA-PRESIDENTA

LA CONCEJALA-SECRETARIA
DE LA JUNTA DE GOBIERNO
LOCAL

PALOMA TEJERO TOLEDO
La Alcaldesa
09-09-2026 13:27:42

Paloma Tejero Toledo

MOLARES PÉREZ, LUCÍA EMILIA
Concejala Secretaria de la Junta de Gobierno Local
09-09-2026 12:36:23

Lucía Molares Pérez

Z