

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE FUENLABRADA

1. INTRODUCCIÓN

El Ayuntamiento de Fuenlabrada, se encuentra actualmente inmerso en un proyecto de transformación digital y de digitalización integral, participando en proyectos de alta tecnología en los que se hace uso de técnicas de minería de datos e inteligencia artificial, así como ante una ciudad en la que cada vez es mayor la presencia de soluciones de sensórica e inteligencia. Este Ayuntamiento, es consciente de que existe una acumulación tecnológica sin precedentes, y con ello de un empleo inusual de datos personales y conductuales que pueden poner en serio riesgo los derechos y libertades de ciudadanos, no sólo en términos de privacidad e intimidad, sino en término de todos los derechos que las regulaciones en materia de servicios y mercados digitales, así como de gobernanza de datos que les confieran.

El Ayuntamiento de Fuenlabrada, tiene un firme compromiso con la ética, la transparencia, y la ciberseguridad, así como con la protección efectiva de los colectivos más vulnerables, por lo que apuesta por favorecer la innovación en el ámbito de la seguridad y la protección de datos, para que no sea obstáculo en la economía digital.

Otro reto, es la implementación de espacios de datos, lo que en la administración se está consolidando como una herramienta esencial para la modernización y eficiencia de los servicios públicos y la denominada gobernanza basada en la evidencia.

Según la Secretaría de Estado de Digitalización e Inteligencia Artificial, un espacio de datos es un entorno donde se genera valor a partir del intercambio voluntario de datos en un marco de soberanía, confianza y seguridad.

Para su consecución, el Ayuntamiento de Fuenlabrada gestiona la Seguridad de la Información en un Sistema de Gestión de Seguridad de la Información único (en adelante el Ayuntamiento o el SGSI) y depende de los sistemas TIC y SI (Tecnologías de Información y Comunicaciones y Sistemas de Información) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información y los servicios.

La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 311/2022 de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	1/22





sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público 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 y recoge el Esquema Nacional de Seguridad en su artículo 156. Mientras que la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas el relativo 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.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento de Fuenlabrada, conocedor de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso "su propia Información" es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar 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 de los servicios prestados.

De este modo, todos los departamentos y/o áreas del Ayuntamiento de Fuenlabrada, que se encuentran dentro del ámbito del ENS, tienen presente 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 las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el Ayuntamiento de Fuenlabrada, sus Organismos Autónomos y empresas municipales (en adelante "Ayuntamiento de Fuenlabrada"), el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 8 del ENS.

Por otro lado, el Ayuntamiento de Fuenlabrada incluye el compromiso con el cumplimiento de la normativa de protección de datos que se desarrolla, entre otras, en el Reglamento (UE) 2016/679 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-), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, así como las directrices de las autoridades de control el Comité Europeo y la Agencia Española de Protección de Datos,

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	2/22





delimitando el ámbito de aplicación en consonancia con el Esquema Nacional de Seguridad y los roles y responsabilidades en la implantación de las diferentes medidas a adoptar, siguiendo lo recogido en la Disposición Adicional Primera de la LOPDGDD.

Además, el AYUNTAMIENTO propone un modelo de cumplimiento normativo desde el punto de vista organizativo, que sirva de evidencia de las buenas prácticas y medidas de diligencia debida como demostración de su firme compromiso con la garantía en la protección de los datos personales y la seguridad de la información.

2. MISIÓN DEL AYUNTAMIENTO DE FUENLABRADA

El Ayuntamiento de Fuenlabrada pone a disposición de la ciudadanía la realización de trámites y servicios online con el objetivo de impulsar su participación en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Potenciando por otro lado también, el uso de las nuevas tecnologías en el Ayuntamiento, la ciudad y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

Y todo ello porque es exigencia de la normativa de procedimiento administrativo común, así como de diversa normativa sectorial.

3. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Fuenlabrada, sus Organismos Autónomos y empresas municipales, 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 alcance del Esquema Nacional de Seguridad (ENS).

Todos los empleados públicos y cargos electos (miembros) del Ayuntamiento de Fuenlabrada, así como el personal de terceros relacionados con este, que se encuentren afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta "Política de Seguridad y Privacidad de la Información" y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información disponer los medios necesarios para que la información llegue al personal afectado.

4. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Fuenlabrada, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal. También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica derivadas de las anteriores.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	3/22





Las normas que constituyen dicho marco, se encuentran recogidas en un documento al efecto, según señala el correspondiente procedimiento de gestión de requisitos legales.

El Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información mantendrá dicho Marco Normativo actualizado, y en el mismo se incluirán, además, 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 del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en la “Disposición Adicional Segunda. Desarrollo del Esquema Nacional de Seguridad” del ENS.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Fuenlabrada derivadas de las anteriores y publicadas en la sede electrónica comprendida dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información y se mantendrá, en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad”.

Así mismo, el Comité también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

5. CUMPLIMIENTO DE PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE SEGURIDAD Y PROTECCION DE DATOS

El Ayuntamiento de Fuenlabrada para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad, que recogen 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.

5.1. Seguridad como un proceso integral y seguridad por defecto. Principio de mínimo privilegio.

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en el 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 falta de conocimiento, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	4/22





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

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- 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.
- 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.

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.

5.2. 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.

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, y el asesoramiento de la disponibilidad de la información y la continuidad operativa.

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.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	5/22





5.3. 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 y privacidad. 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 y privacidad 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.

5.4. 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 del ENS, 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.

5.5. Incidentes de seguridad, prevención, reacción y recuperación.

El Ayuntamiento de Fuenlabrada 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.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	6/22





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.

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

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.

5.6. Existencia de líneas de defensa y prevención ante otros sistemas interconectados

El Ayuntamiento de Fuenlabrada ha implementado una estrategia de protección basada en múltiples capas, 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 Ley General 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.

5.7. Función diferenciada y organización e implantación del proceso de seguridad

El Ayuntamiento de Fuenlabrada ha organizado su seguridad comprometiendo a todos los miembros de la corporación, mediante la designación de diferentes roles de seguridad y privacidad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

5.8. Autorización y control de los accesos

El Ayuntamiento de Fuenlabrada ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, mediante mínimo privilegio y exclusivamente en base

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	7/22





a la legitimación y a las funciones permitida, teniendo como referencia las competencias y responsabilidades de cada usuario.

5.9. Protección de las instalaciones

El Ayuntamiento de Fuenlabrada ha implementado mecanismo 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.

5.10. Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento de Fuenlabrada 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.

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

El Ayuntamiento de Fuenlabrada 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.

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 del ENS, 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 el ENS, 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.

5.12. Registros de actividad y detección de código dañino

El Ayuntamiento de Fuenlabrada ha habilitado registros de la actividad de los usuarios El Ayuntamiento de Fuenlabrada con el propósito de satisfacer el objeto del ENS, 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,

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	8/22





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, la exfiltración de datos personales, así como otros daños a las antedichas redes y sistemas de información.

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.

5.13. Infraestructuras y servicios comunes

El Ayuntamiento de Fuenlabrada 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 el ENS.

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

El Ayuntamiento de Fuenlabrada tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos que sean de aplicación.

5.15. Respeto a los principios de protección de datos personales

El Ayuntamiento tratará los datos personales bajo su responsabilidad conforme a los principios de protección de datos reconocidos, entre otros, en el artículo 5 del RGPD y demás normativa vigente, respetando también el Pacto Digital para la protección de las personas promovido por la Agencia Española de Protección de Datos (AEPD).

Además, el Ayuntamiento adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar que, de forma proactiva, cumple con la normativa de protección de datos respetando los derechos y libertades de las personas que, de una forma u otra, se relacionan con la entidad local. La gestión del riesgo se entiende como un elemento fundamental del modelo de responsabilidad proactiva propugnado por el RGPD debe facilitar el mantenimiento de un entorno controlado en el tratamiento de los datos personales, minimizando los riesgos hasta niveles aceptables por el Ayuntamiento. La reducción de estos niveles se realizará mediante la aplicación de medidas de seguridad, que deberán ser adecuadas a lo establecido en el Esquema Nacional de Seguridad, en cumplimiento de la Disposición Adicional Primera de la LOPDGDD.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	9/22





6. CONFIDENCIALIDAD Y PRIVACIDAD EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El desarrollo de la presente Política de Seguridad y del SGSI mediante el cual se da respuesta a la misma, así como a los requisitos del ENS y del RGPD, se realizará en el Ayuntamiento asegurando la debida confidencialidad y profesionalidad y, en todo caso, 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. La gestión de la seguridad de la información se realizará teniendo en cuenta igualmente en consideración, los principios y requisitos mínimos del ENS como son, entre otros: Profesionalidad (Art. 16), Autorización y control de los accesos (Art. 17), Mínimo privilegio (Art. 20), Gestión de la seguridad basada en los riesgos (Art. 17), Auditoría de la Seguridad (Art. 31).

En consecuencia, toda la información que se derive de las actividades de configuración, monitorización, evaluaciones de riesgo e impacto, auditoría, análisis, supervisión y seguimiento de la seguridad de la información se encontrará sujeta a la más estricta confidencialidad, proporcionalidad y necesidad, limitando su tratamiento de la información y el acceso a la misma a lo estrictamente necesario y al personal con competencias en materia de seguridad y privacidad para el cumplimiento de los objetivos de la presente Política de Seguridad.

7. ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa de la Organización de la Seguridad de la Información en el Ayuntamiento de Fuenlabrada se establece en la forma que se indica a continuación.

7.1. 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: Directores/as Generales o Responsables de los Departamentos/Servicios Municipales, y Directores Gerentes de los OO.AA y de empresas municipales dependientes del Ayuntamiento de Fuenlabrada a excepción de la DG de Innovación y Transformación Digital, cuyo Responsable de Información y Servicios será el Técnico de Desarrollo del área TIC. Borja Fernández Ruiz, dado que la Directora General de Innovación y Transformación Digital es la Delegada de Protección de Datos municipal. Responsable de Seguridad de la Información del ENS: Técnico de Sistemas del área TIC. Pilar Barreiro Álvarez
- Responsable del Sistema del ENS: Técnico de Sistemas del área TIC. José Martínez Castrejón

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	10/22





7.2. Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información

El Ayuntamiento de Fuenlabrada constituye un Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información, como órgano colegiado y está formado por los siguientes miembros:

- **Presidente:** Alcalde o Alcaldesa, o Concejal/a Delegado/a responsable de TIC o persona en quien delegue.
- **Secretario:** Responsable de Seguridad ENS.
- **Vocales:**
 - Responsable del Sistema ENS.
 - Secretaria General del Pleno del Ayuntamiento.
 - Responsables de Información y los Servicios convocados por la presidencia en función de los asuntos a tratar.
 - Responsables funcionales y responsables técnicos de aplicaciones convocados por la presidencia en función de los asuntos a tratar.
 - Delegado/a de Protección de Datos (DPD).

Puesto que el Comité de Seguridad y Privacidad de la Información no es un comité técnico, deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

- Grupos de trabajo especializados, internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de eventos formativos o de intercambio de experiencias.

El Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información celebrará sus sesiones en las dependencias del Ayuntamiento con periodicidad semestral, previa convocatoria al efecto realizada por el Presidente de dicho Comité, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

El Comité de Seguridad, Privacidad y Cumplimiento Normativo 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.

7.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad, Privacidad y Cumplimiento Normativo.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	11/22





Las sucesivas modificaciones a las funciones que en esta Política de Seguridad y Privacidad de la Información se asignan a los roles o perfiles de seguridad no requerirán la aprobación de una nueva Política de Seguridad y Privacidad de la Información, pudiendo ser aprobadas a propuesta del Comité de Seguridad, Privacidad y Cumplimiento Normativo descrito en la Política de Seguridad y Privacidad de la Información por el Alcalde-Presidente o Concejal Delegado en materia de STIC.

▪ **Funciones del Responsable de la Información, de los servicios**

- Establecer y aprobar los requisitos de seguridad y protección de datos aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de Mayo y RGPD, pudiendo recabar una propuesta al Responsable de Seguridad ENS y teniendo en cuenta la opinión del Responsable del Sistema ENS y Delegado/a de Protección de Datos.
- Informar sobre los derechos de acceso al Servicio y a la Información.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Poner en comunicación del Responsable de Seguridad ENS y Delegado/a de Protección de Datos, cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.
- Velar por la adecuada realización de sus funciones, dentro del marco de seguridad adecuado, ayudando a difundir el conocimiento y la cultura de seguridad y protección de datos necesarias para el correcto tratamiento de los datos.
- Colaborar en la definición y aprobación de las actividades de tratamiento de datos personales propias de su área de responsabilidad.
- Determinar los requisitos (de seguridad) de la información tratada y los servicios prestados.
- Efectuar las valoraciones a las que se refiere el artículo 40 del ENS (categorías de seguridad), así como, en su caso, su posterior modificación.
- Recibir información sobre los incidentes y de las actuaciones realizadas para su resolución.
- Determinación de los criterios para asignar y modificar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

▪ **Funciones del Responsable de Seguridad ENS:**

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	12/22





- Determinar las medias de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
- Supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportar sobre estas cuestiones.
- Formalización y aprobación de las medidas seleccionadas del Anexo II en la Declaración de Aplicabilidad, incluyendo las medidas compensatorias o complementarias de vigilancia y su correspondencia con las medidas del Anexo II antes citado.
- Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
- Determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Promover la realización del análisis de riesgos.
- 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.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información 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 revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Análisis de los informes de Auditoría de primera, segunda o tercera parte que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.
- Elevar al Comité de Seguridad, Privacidad y Cumplimiento Normativo la aprobación de cambios y otros requisitos del sistema.
- Aprobación explícita de los cambios que impliquen un riesgo de nivel ALTO con carácter previo a su implantación.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
- Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, normativas y procedimientos que incluirán las medidas técnicas y

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	13/22





organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.

- Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio.
- En lo que respecta a los incidentes de seguridad, contando con los responsables de la entidad, de la información y de los servicios:
 - o Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia, en particular con el CCN-Cert.
 - o Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
 - o Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
 - o Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
- Informar y coordinarse con el/la Delegado/a de Protección de Datos para verificar la posible exfiltración de datos y generación de brecha de datos personales. Identificar contexto, volumen de datos afectados, nivel de sensibilidad de los mismos, cantidad de personas afectadas, origen de esas personas y todo lo que conlleve a analizar e identificar el incidente de seguridad que haya ocasionado la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.
- Cuando el sistema trate datos personales, el Responsable de la Seguridad recogerá los requisitos de Centro Criptológico Nacional 9 CCN-STIC-801 Esquema Nacional de Seguridad - Responsabilidades y Funciones protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y con la evaluación de impacto en la protección de datos, si se ha llevado a cabo.
- Asimismo, el Responsable de la Seguridad actuará como Secretario del Comité de Seguridad, con las siguientes funciones derivadas:
 - o Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones del presidente del Comité.
 - o Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	14/22





- Elaborar el acta de las reuniones.
- Remitir el acta de las reuniones a los asistentes, recabando su firma.
- Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

■ **Las funciones del Responsable del Sistema ENS:**

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.
- En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos.
- Adoptar las medidas correctoras adecuadas derivadas de los informes de Auditoría de primera, segunda o tercera parte.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	15/22





- Adopción de medidas correctoras de las auditorías de primera, segunda o tercera parte, según las conclusiones trasladadas por el Responsable de la Seguridad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema que incluyen:
 - o La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
 - o La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
 - o La aplicación de los Procedimientos Operativos de Seguridad (POS).
 - o Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
 - o Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
 - o 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.
 - o Comprobar que los controles de seguridad establecidos son adecuadamente observados.
 - o Comprobar que son aplicados los procedimientos aprobados para manejar el sistema de información.
 - o Comprobar 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.
 - o Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

■ **Las funciones del Delegado de Protección de Datos.**

- Será responsabilidad del/la Delegado/a de Protección de Datos y el Responsable del Tratamiento velar por el cumplimiento de la Normativa de Protección de Datos, en particular, el Reglamento Europeo de 2016/679 de 27 abril de 2016, así como

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	16/22





cualquier otra legislación aplicable en el ámbito de datos de carácter personal que pueda surgir, siempre de acuerdo a lo dispuesto en el presente procedimiento.

- Implantación de las normas contenidas en el RGPD relativas a cumplimiento de normas jurídicas y de tratamiento de datos.
- Diseño e implantación de políticas de protección de datos y de medidas de seguridad adecuadas a los riesgos de los tratamientos.
- Auditoría continua de protección de datos.
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.
- Informar y asesorar al Ayuntamiento de Fuenlabrada y a los usuarios que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas del Ayuntamiento de Fuenlabrada en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera y actuará como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado/a de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
 - o Recabar información para determinar las actividades de tratamiento.
 - o Analizar y comprobar la conformidad de las actividades de tratamiento.
 - o Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
 - o Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

■ Las funciones de los Responsables funcionales de aplicaciones

- Operar los sistemas y tratar datos siguiendo las normas de sistemas y las pautas de seguridad y protección de datos.
- Identificar incidencias, definir mejoras funcionales, certificar los cambios funcionales en producción y desarrollo de pruebas de aceptación de implantaciones de servicios, o Sistemas.
- En materia de protección de datos:
 - o Colaborar en el mantenimiento del Registro de Actividades de Tratamiento (RAT), identificando nuevos tratamientos, sus riesgos y la necesidad de

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	17/22





realizar una evaluación de impacto, contando con el asesoramiento del Delegado/a de Protección de Datos.

- Identificar los prestadores que traten datos por cuenta del Ayuntamiento y determinar los contratos de encargados de tratamiento.
- Dar cumplimiento tramitando, con el asesoramiento del Delegado/a de Protección de Datos, a los derechos de protección de datos.
- Gestionarán el procedimiento de brechas de seguridad en protección de datos cuando afecte a un tratamiento de su área de competencia, contando con el responsable de seguridad, el de sistemas y con el asesoramiento de la Delegada de Protección de Datos.

■ Las funciones de los Responsables técnicos de aplicaciones

- Operar, mantener y documentar técnicamente el SI de acuerdo con las normas, y medidas técnicas y de seguridad.

7.4. Funciones del Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información

El Comité de Seguridad, Privacidad y Cumplimiento Normativo tendrá las siguientes funciones:

- Alinear las actividades de la organización en materia de seguridad de la información.
- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas informando regularmente del estado de la Seguridad de la Información.
- Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- 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.
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular,

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	18/22





deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de Seguridad de la Información.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información y Privacidad para su aprobación por el órgano competente y aprobar la Normativa de Seguridad de la información.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Representar frente a terceros (entidades privadas y otras Administraciones Públicas) la figura de Responsables de la Información ENS y Responsables de los Servicios ENS. Responsables Funcionales de Tratamiento en acciones transversales.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- 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.

7.5. Procedimientos de designación

La creación del Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política se realiza por resolución de la Alcaldía- Presidencia del Ayuntamiento de Fuenlabrada y comunicada a las partes afectadas.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

7.6. Resolución de conflictos

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

8. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Fuenlabrada solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	19/22





El Ayuntamiento de Fuenlabrada, ha implementado los mecanismos adecuados para garantizar la adecuación a la normativa vigente en materia de protección de datos. En particular el Ayuntamiento ha adoptado las medidas oportunas para adecuarse al Reglamento (UE) 2016/679 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) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, consistentes en el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se llevan a cabo, el análisis de riesgos de los tratamientos, la evaluación de impacto en los casos en los que sea requerido, el registro de actividades y el nombramiento del Delegado de Protección de Datos (Decreto nº 2021/8333 de 13 De Octubre de 2021).

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información aprobará el desarrollo de un sistema de gestión de la seguridad, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del Alcalde-Presidente o Concejäl delegado competente en materia de STIC del Ayuntamiento de Fuenlabrada.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Fuenlabrada, que se encuentran dentro del ámbito del ENS y RGPD, recibirán una concienciación adecuada en materia de seguridad de la información y protección de datos, a través de charlas, acciones formativas, comunicaciones, buenas prácticas definidas. Se establecerá un programa de concienciación continua para atender a todos los miembros del Ayuntamiento de Fuenlabrada, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC del Departamento TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Todos los empleados municipales, personal directivo y cargos públicos que presten servicios en la Ayuntamiento, tienen la obligación de conocer y cumplir las normas, protocolos, instrucciones o procedimientos en el tratamiento seguro de la información y de datos personales, actuando con secreto y confidencialidad, colaborando y evitando actuaciones

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	20/22





que puedan incrementar los riesgos a los que se encuentran expuestos los datos personales, asistiendo a las actividades de sensibilización o formación que se organicen.

El incumplimiento de las obligaciones podrá ser objeto de sanción disciplinaria o dar lugar al resarcimiento de daños y perjuicios de las personas afectadas o del propio Ayuntamiento, cuando se realice de forma dolosa contraviniendo las instrucciones municipales.

11. TERCERAS PARTES

Cuando el Ayuntamiento de Fuenlabrada preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad y Privacidad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Fuenlabrada utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y Privacidad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad y Privacidad.

De igual modo, teniendo en cuenta la obligación del Esquema Nacional de Seguridad, que indica que los prestadores del sector privado que presten servicios o provean soluciones a las entidades públicas, les es exigible el cumplimiento del Esquema Nacional de Seguridad; dicho prestador de servicios deberá 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 y Privacidad 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12. POLÍTICA DE USO ACEPTABLE

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	21/22





- Facilitar el acceso de forma deliberada a las instalaciones o los servicios a personas no autorizadas.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos o violar la privacidad de otros intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenamiento de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de destinatarios (que pueda llegar a saturar las comunicaciones).
- El uso de herramientas o servicios externos (incluyendo servicios cloud o de Inteligencia Artificial) no corporativas para el tratamiento o almacenamiento de información del Ayuntamiento.
- Facilitar acceso de forma deliberada a información de uso interno o confidencial a personas no autorizadas.
- No cumplir con la normativa de uso de sistemas de información corporativa.

13. DIFUSIÓN DE LA POLÍTICA

El Ayuntamiento de Fuenlabrada, a través del Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información, potenciará el conocimiento y difusión de la presente Política en los niveles adecuados, dado que interpreta este factor como crítico para asegurar su implantación eficaz y un cumplimiento efectivo.

Corresponde al Comité de Seguridad, Privacidad y Cumplimiento Normativo de la Información impulsar de forma efectiva la implantación de la Política de Seguridad y Privacidad de la Información. La distribución a las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad y Privacidad se realizará tan sólo en los casos que sean oportunos para salvaguardar la Política de Seguridad y Privacidad de la Información del Ayuntamiento de Fuenlabrada. Será responsabilidad del centro gestor o servicio promotor de expedientes de contratación realizar esta difusión y vigilancia de su cumplimiento.

CSV (Código de Verificación Segura)	IV76EXZC3YB3JOH4AT75IZ7UGM	Fecha	31/08/2026 13:52:12
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmado por	PILAR ARANZAZU HERRAEZ LOPEZ (Directora General)		
Firmado por	MARÍA DEL PILAR BARREIRO ÁLVAREZ (Jefe de Negociado)		
Url de verificación	https://sede.ayto-fuenlabrada.es/verifirmav2/code/IV76EXZC3YB3JOH4AT75IZ7UGM	Página	22/22

