AYUNTAMIENTO DE GETAFE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Y

PROTECCIÓN DE DATOS PERSONALES

PROPIEDADES DEL DOCUMENTO

FECHA DE CREACIÓN:	12/03/2025	**CALIFICACIÓN**	**PÚBLICO**

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR: Responsable del Sistema ENS Responsable de Seguridad	27/07/2025	
APROBADO POR: Alcaldesa de Getafe		

ÍNDICE:

TITULO I.- DISPOSICIONES GENERALES

Aprobación y entrada en vigor

Esta "Política de Seguridad de la Información y Protección de datos personales", en adelante Política, será efectiva desde la fecha de aprobación por la Alcaldesa y hasta que sea reemplazada por una nueva Política.

Introducción

El Ayuntamiento de Getafe 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.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos municipales 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; así como la mejora de la gobernanza y el cumplimiento normativo del ENS a través de un "escudo único" para la Administración y el uso de las herramientas del CCN-CERT destinadas al efecto.

De este modo, todas las unidades administrativas del Ayuntamiento de Getafe, 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 Getafe, el objetivo de la Seguridad de la Información es garantizar la seguridad 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, y en su caso, recuperar los servicios lo antes posible con la aplicación de las medidas que se relacionan a continuación.

Por otro lado, en el Título III de la presente Política, el Ayuntamiento de Getafe 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, 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.

Prevención

Para que la información, incluyendo los datos de carácter personal, y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional que se haya identificado como necesario, a través de una evaluación continua de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el Ayuntamiento:

- Certifica la gestión de cambios, el alcance funcional y el cumplimiento normativo y técnico de los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

El Ayuntamiento de Getafe establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el ENS (Reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Reacción

El Ayuntamiento de Getafe establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad y brechas o violaciones que afecten a la información incluyendo los datos de carácter personal.

- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en los diferentes departamentos o en otros organismos dependientes. Sin perjuicio de las atribuciones que el Delegado de Protección de Datos tiene en la colaboración con la autoridad de control cuando se vean afectados datos de carácter personal.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) y, cuando afecte a datos personales y suponga un riesgo para los derechos y libertades de las personas afectadas, a la Agencia Española de Protección de Datos (AEPD), a los propios afectados, sin perjuicio de que cuando dichos incidentes puedan ser constitutivos de un delito se ponga en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado y/o los juzgados y tribunales.

Recuperación

Para garantizar la disponibilidad de los servicios, el Ayuntamiento dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Misión del Ayuntamiento

El Ayuntamiento de Getafe pone a disposición de la ciudadanía la realización de trámites online con el objetivo de impulsar 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 eficacia de la acción pública.

En este sentido, la consagración del derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios electrónicos, obliga al Ayuntamiento, en todas sus áreas y servicios, a cumplir sus objetivos utilizando sistemas de información que garanticen la seguridad de la información, por lo que las decisiones a adoptar en materia de seguridad tendrán en cuenta los principios y requisitos mínimos de seguridad establecidos en el Esquema Nacional de Seguridad.

Alcance

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Getafe, 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.

Además, en dichos sistemas se tratan datos de carácter personal extendiendo también su alcance a estos, en la medida que es necesario dar cumplimiento con el principio de proactividad, disponiendo de una Política que detalle el marco de actuación municipal en la materia.

Marco normativo

El marco normativo que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Getafe comprende el Real Decreto que regula el Esquema Nacional de Seguridad, en adelante ENS, y todas aquellas normas jurídicas estatales y autonómicas 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.

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

También podrán formar parte del referido marco, aquellas normas aplicables a la Administración Electrónica del Ayuntamiento, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en la Sede Electrónica comprendida dentro del ámbito de aplicación de la presente Política.

El Ayuntamiento de Getafe también será responsable de identificar las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

Se incluyen también en la normativa aplicable a esta Política las normas reguladoras de la protección de datos personales vigentes, entre otras, el Reglamento UE General de Protección de Datos y la Ley Orgánica que lo complementa.

TITULO II.- DEL ESQUEMA NACIONAL DE SEGURIDAD

Cumplimiento de los artículos de seguridad

El Ayuntamiento de Getafe, para lograr el cumplimiento del Real Decreto por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y 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.

Seguridad como un proceso integral y mínimo privilegio

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de Getafe, 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 que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente 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 mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) 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.

e) 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.

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

Se referencia en este requisito el apartado de Obligaciones del personal.

Gestión de la seguridad basada en los riesgos y 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.

Se referencia en este requisito el apartado Gestión de riesgos.

Incidentes de seguridad, prevención, reacción y recuperación

El Ayuntamiento de Getafe ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de Getafe, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

El Ayuntamiento de Getafe, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en los diferentes departamentos o en otros organismos dependientes.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, el Ayuntamiento de Getafe, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa y prevención ante otros sistemas interconectados

El Ayuntamiento de Getafe ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento de Getafe, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de Organización de la seguridad del presente documento.

Autorización y control de los accesos

El Ayuntamiento de Getafe, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

El Ayuntamiento de Getafe, 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, el Ayuntamiento de Getafe, tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad (apartado 6.3).

Se tendrá en cuenta lo definido en el apartado de Terceras partes de la presente Política.

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

El Ayuntamiento de Getafe, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias del Ayuntamiento de Getafe. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que

toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad y detección de código dañino

El Ayuntamiento de Getafe, ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del Esquema Nacional de Seguridad, 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.

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.

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 de Getafe 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.

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

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

Organización de la seguridad

Criterios utilizados para la Organización de la Seguridad de la Información

El Ayuntamiento de Getafe, teniendo en cuenta lo establecido en el Esquema Nacional de Seguridad y las pautas establecidas en la Guía *CCN-STIC-801 "Responsabilidades y Funciones en el ENS"*, para organizar la seguridad de la información emprenderá las siguientes acciones:

- **Designará roles de seguridad**: Responsables de los Servicios, Responsables de Información, Responsable de Seguridad de la Información, Responsable del Sistema y Delegado de Protección de Datos.
- **Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información**. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información y Protección de datos. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

Roles y Órganos de Seguridad de la Información del Ayuntamiento de Getafe

En el Ayuntamiento de Getafe los roles y órganos de seguridad de la información, serán los siguientes:

- Responsables de los Servicios y Responsables de la Información ENS: Los jefes y responsables de los diferentes órganos y unidades administrativas.
- Delegado/a de Protección de Datos.
- Responsable de Seguridad de la Información ENS: Jefatura de Sección de Informática.
- Responsable del Sistema ENS: Técnico/a del Servicio de Informática
- Comité de Seguridad de la Información y Protección de Datos:
    - Presidente: Alcaldesa o Concejal en quien delegue.
    - Secretario/a: Responsable de Seguridad de la Información ENS.
    - Vocales:
        - Jefe/a de la Oficina de la Junta de Gobierno.
        - Secretario/a General del Pleno.
        - Jefe/a de Servicio de Administración Electrónica y Transparencia.
        - Jefe/a de Servicio de Personal.
        - Responsable del Sistema ENS.
        - Jefa/a de Asesoría Jurídica.
        - Delegado/a de Protección de Datos.
        - Los Responsables de Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar.

El Comité de Seguridad y Protección de datos, se reunirá con carácter ordinario, al menos una vez cada doce meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

El Secretario/a del Comité levantará actas de las reuniones del Comité de Seguridad y Protección de datos. A las sesiones del Comité de Seguridad y Protección de datos podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

Responsables de la Información y los Servicios

Serán funciones de los Responsables de Información y de los Servicios:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información y Protección de datos los requisitos de seguridad aplicables al Servicio (niveles de seguridad del servicio) y la Información (niveles de seguridad de la información), dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad. Pudiendo recabar una propuesta al Responsable de Seguridad ENS y teniendo en cuenta la opinión del Responsable del Sistema ENS.
- Dictaminar respecto a 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 de la Información ENS, 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. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información y Protección de datos, en su próxima reunión.

Responsable de Seguridad de la Información ENS

Serán funciones del Responsable de Seguridad de la Información ENS:

- 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.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información y Protección de datos.
- Participará 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
- Elevar al Comité de Seguridad y Protección de datos la aprobación de cambios y otros requisitos del sistema.

Responsable del Sistema ENS

Serán funciones del Responsable del Sistema ENS:

- 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. Elaborando los procedimientos operativos necesarios.
- 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.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad de la Información ENS y/o Comité de Seguridad de la Información y Protección de datos.
- Participará 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:
    - 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.
    - Informar al Responsable de Seguridad de la Información ENS de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique el Responsable del Sistema ENS 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.

Delegado de Protección de Datos

La persona designada como Delegada de Protección de Datos ejercerá las funciones contenidas en la normativa vigente en protección de datos personales o seguridad de la información, así como aquellas otras atribuciones de las autoridades de control, emanadas de

sus dictámenes, informes o criterios interpretativos. En todo caso, la Delegada participará y podrá asesorar o supervisar, con total independencia cuando lo considere oportuno, en todas las actuaciones del Ayuntamiento relacionadas con el área de su competencia, integrándose también en el Comité de Seguridad y Protección de Datos. Las funciones se definen en el TITULO III de la presente Política.

Funciones y obligaciones del Comité de Seguridad de la Información y Protección de Datos

Serán funciones del Comité de Seguridad de la Información y de Protección de Datos en relación al Esquema Nacional de Seguridad:

- Aprobar y coordinar las propuestas de los Responsables de Información y Servicios sobre los niveles de seguridad de la información y de los servicios y asumir las funciones de los Responsables de Información y Servicios en las actuaciones en que se considere necesario.
- Atender las inquietudes, 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 a la Dirección.
- Asesorar en materia de Seguridad de la Información, siempre y cuando le sea requerido.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asumir temporalmente ciertas funciones de Delegado/a de Protección de Datos en caso de vacante o baja de éste.
- 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 (Privacy by Design). 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.
    - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación el Órgano Superior.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el 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 RGPD que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

Procedimientos de designación

La creación del Comité de Seguridad de la Información y Protección de datos, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta política, se realizará por la Alcaldía del Ayuntamiento de Getafe o Concejalía en quien delegue.

El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

Datos de carácter personal

El Ayuntamiento 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. Estas medidas operativas estarán recogidas en los documentos y normativas internas corporativas, de acuerdo con la normativa vigente y el contenido del TITULO III de la presente Política.

Obligaciones del personal

Todos los miembros del Ayuntamiento de Getafe, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas 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.

Gestión de riesgos

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad de la Información ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información y Protección de datos.

El Comité de Seguridad de la Información y Protección de datos dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información y Protección de datos procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en el ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

Desarrollo de la política de seguridad de la información

Esta Política será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información y Protección de datos, su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

Corresponde a la Alcaldía del Ayuntamiento de Getafe la aprobación de los documentos de las Políticas y normativa de alto nivel, siendo el Comité de Seguridad de la Información y Protección de datos el órgano responsable de la aprobación de los restantes documentos y de su difusión para que la conozcan las partes afectadas.

Del mismo modo, esta Política complementa las políticas de seguridad del Ayuntamiento de Getafe en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros del Ayuntamiento de Getafe que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet municipal, en soporte papel, esta documentación será custodiada por el Servicio de Informática.

Terceras partes

Cuando el Ayuntamiento de Getafe preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad 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 Getafe utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña 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.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas 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. Se destaca la obligación por parte de los proveedores de cumplir con los procedimientos de gestión de incidentes de seguridad, conforme a ENS, siguiendo la guía de referencia del CCN-CERT de Gestión de Ciberincidentes.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información ENS 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.

TITULO III.- DE LA PROTECCIÓN DE DATOS PERSONALES EN EL AYUNTAMIENTO DE GETAFE

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.

Medidas de cumplimiento normativo

El Ayuntamiento desarrolla y mantiene actualizado un sistema de gestión de la protección de datos que incluye, entre otras medidas, las siguientes:

a) La aprobación y mantenimiento de esta Política.

b) La identificación de los tratamientos de datos de carácter personal para su integración en el Registro de Actividades del Tratamiento que se mantendrá actualizado y publicado en la web municipal para conocimiento de cualquier persona, en aplicación del principio de transparencia.

c) Implantación y actualización de la gestión de los riesgos, incluyendo la realización de evaluaciones de impacto cuando sea preciso.

d) Supervisión periódica y actualización de la información para que las personas afectadas conozcan de forma transparente, con un lenguaje entendible y accesible, los tratamientos de sus datos personales tratados responsabilidad del Ayuntamiento, con independencia de la forma o medio de recogida.

e) El Ayuntamiento evitará las transferencias internacionales de datos fuera del Espacio Económico Europeo o países considerados por las autoridades de control con suficientes garantías. En caso de que, excepcionalmente, realizase una transferencia de datos fuera de estos territorios, cumplirá con las garantías de la normativa de protección de datos e informará de forma pormenorizada a las personas afectadas.

f) Cuando el Ayuntamiento preste servicios de forma indirecta, con independencia de la relación jurídica con el prestador, en todo caso, se tendrá en cuenta si van a tratar datos personales para instruirles, mediante un contrato de encargado del tratamiento, de cómo deben actuar.

Roles y responsabilidades en el cumplimiento de la normativa de protección de datos

El Ayuntamiento para la adecuada gestión de las obligaciones de la normativa de protección de datos personales y de su sistema de gestión, atribuye las siguientes responsabilidades y funciones:

Alcaldía

Son funciones de la Alcaldía, las siguientes:

- La aprobación de esta Política y sus modificaciones.
- El ejercicio de acciones judiciales o administrativas en defensa del Entidad local como responsable del tratamiento.

- La dirección y representación de la Entidad local en materia de protección de datos personales ante las autoridades de control.
- Aprobación del Registro de Actividades del Tratamiento y, en su caso, la modificación o supresión de las actividades de tratamiento.
- La aprobación/firma de las resoluciones y/o comunicaciones relacionadas con la respuesta al ejercicio de derechos u otras peticiones realizadas por las personas afectadas por el tratamiento de sus datos personales.
- La notificación a la AEPD y/o las personas afectadas aquellos incidentes de seguridad, en su caso;
- La firma de los contratos o actos jurídicos vinculantes de Encargado del Tratamiento con entidades o personas físicas o jurídicas que presten servicios cuando traten datos personales.
- La designación, cese o remoción de la persona designada como Delegado/a de Protección de Datos, así como su registro en la AEPD.
- Dictar las instrucciones, normas o protocolos internas para el adecuado cumplimiento de la normativa de protección de datos.

El Comité de Seguridad de la Información y Protección de datos

Además de las funciones que tiene atribuidas en el apartado 7 de esta Política, en relación con la protección de datos personales aprobará inicialmente y elevará a su aprobación definitiva las propuestas sobre:

- Las instrucciones, normas o protocolos internos para el cumplimiento de la normativa de protección de datos.

Además, será informado de las brechas de seguridad que afecten a datos personales, así como de su incidencia

Responsables funcionales de las aplicaciones

Además de las funciones del apartado 7, les corresponde:

- Colaborar en el mantenimiento del Registro de Actividades de Tratamiento (RAT), identificando nuevos tratamientos, sus riesgos y la necesidad de 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

Asesoría jurídica municipal

A la Asesoría jurídica municipal le corresponde la tramitación de los expedientes ante la AEPD u otra autoridad de control, incluidos los sancionadores, así como la presentación de recursos administrativos o judiciales relacionados con el cumplimiento de la normativa de protección de datos.

Delegada de Protección de Datos

Serán funciones de la persona designada como Delegada de Protección de Datos, además de las recogidas en el apartado 7, las siguientes sin perjuicio de las que le atribuya la normativa en la materia:

- Informar y asesorar al Ayuntamiento de Getafe 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 Getafe 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- 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:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
    - 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.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- 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.
- Colaborar con la Asesoría Jurídica en el ejercicio de las competencias de ésta.

Obligaciones del personal

Todas las personas integrantes del Ayuntamiento de Getafe, con independencia de su relación jurídica, prestarán su colaboración en las actuaciones de implementación de la normativa de protección de datos además de cumplir con las obligaciones del Título I y II de la presente Política.

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 de datos personales, actuando con secreto y confidencialidad, colaborando y evitando actuaciones 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 cumplimiento 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.

DISPOSICIONES ADICIONALES

Modificaciones de la Política

EDICIÓN	FECHA	MODIFICACIONES RESPECTO A LA EDICIÓN ANTERIOR
01	30/04/19	Edición inicial
02	15/12/22	Segunda Edición
03	12/03/25	Tercera Edición. Revisión y adaptación al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante Real Decreto por el que se regula el Esquema Nacional de Seguridad)

LA ALCALDESA DE GETAFE

El documento ha sido firmado por la Alcaldesa, Dña. Sara Hernández Barroso, en fecha 13 de noviembre de 2025.