

AYUNTAMIENTO DE GETAFE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

	Política de Seguridad	Identificador: ENS-02-POL-01
		Versión: 01
		Fecha: 30/04/2019
		Página 1 de 13

ÍNDICE:

1. APROBACIÓN Y ENTRADA EN VIGOR	3
2. INTRODUCCIÓN	3
2.1. Prevención	3
2.2. Detección	4
2.3. Respuesta	4
2.4. Recuperación	4
3. MISIÓN DEL AYUNTAMIENTO	4
4. ALCANCE	5
5. MARCO NORMATIVO	5
6. ORGANIZACIÓN DE LA SEGURIDAD	6
6.1. Criterios utilizados para la Organización de la Seguridad de la Información	6
6.2. Roles y Órganos de Seguridad de la Información del Ayuntamiento de Getafe	6
6.3. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad	7
6.3.1. Responsables de la Información y los Servicios	7
6.3.2. Responsable de Seguridad ENS	7
6.3.3. Responsable del Sistema ENS	8
6.3.4. Delegado de Protección de Datos	9
6.4. Funciones y obligaciones del Comité de Seguridad de la Información	10
6.5. Procedimientos de designación	11
7. DATOS DE CARÁCTER PERSONAL	11
8. OBLIGACIONES DEL PERSONAL	11
9. GESTIÓN DE RIESGOS	11
10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	12
11. TERCERAS PARTES	12
12. Modificaciones	13

1. Aprobación y entrada en vigor

Texto aprobado el día 30 de abril de 2019 por Resolución de la Alcaldesa del Ayuntamiento de Getafe.

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

2. Introducción

El Ayuntamiento de Getafe depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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 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.

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 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 recuperar los servicios lo antes posible, según lo establecido en el Artículo 7 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1. Prevención

Para que la información 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 haya identificado como necesario, a través de una evaluación 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:

- Autoriza los sistemas antes de entrar en operación.

	Política de Seguridad	Identificador: ENS-02-POL-01
		Versión: 01
		Fecha: 30/04/2019
		Página 3 de 13

- 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.

2.2. 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 Artículo 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3. Respuesta

El Ayuntamiento de Getafe establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- 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).

2.4. 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.

3. 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.

Al potenciar el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía se persigue fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

	Política de Seguridad	Identificador: ENS-02-POL-01
		Versión: 01
		Fecha: 30/04/2019
		Página 4 de 13

4. Alcance

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Getafe relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el Ayuntamiento de Getafe. Todos ellos tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. Marco normativo

El marco normativo en que se desarrollan las actividades del Ayuntamiento, y, en particular, la prestación de sus servicios electrónicos, está integrado por las siguientes normas:

- a) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica y Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- b) 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.
- c) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- d) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- e) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- f) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- g) Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- h) Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- i) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- j) Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- k) Ley 59/2003, de 19 de diciembre, de firma electrónica.
- l) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- m) Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

	Política de Seguridad	Identificador: ENS-02-POL-01
		Versión: 01
		Fecha: 30/04/2019
		Página 5 de 13

- n) Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- o) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- p) Ordenanza reguladora de la Administración Electrónica del Ayuntamiento de Getafe aprobada por Pleno el 5 de julio de 2012, publicada en el BOCM el 1 de septiembre de 2012.

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

6. Organización de la seguridad

6.1. Criterios utilizados para la Organización de la Seguridad de la Información

El Ayuntamiento de Getafe, teniendo en cuenta lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica 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 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. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

6.2. 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 administrativos
- Delegado de Protección de Datos: Comité de Seguridad de la Información, siendo interlocutor de la AEPD el Jefe de Servicio de Administración Electrónica y Transparencia.
- Responsable de Seguridad de la Información ENS: Director del Servicio de Informática.
- Responsable del Sistema ENS: Técnico del Servicio de Informática
- Comité de Seguridad de la Información:
 - Presidente: Alcaldesa o Concejales en quien delegue.
 - Secretario/a: Responsable de Seguridad de la Información ENS
 - Vocales:

- Jefa de la Oficina de la Junta de Gobierno.
- Secretario General del Pleno.
- Jefe de Servicio de Administración Electrónica y Transparencia.
- Responsable del Sistema

Los Responsables de Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez cada seis 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. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

6.3. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

6.3.1. 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 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 3/2010, de 8 de enero. 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 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, en su próxima reunión.

6.3.2. Responsable de Seguridad ENS

Serán 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.
- 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 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, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema
- Gestionar los procesos de certificación
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

6.3.3. Responsable del Sistema ENS

Serán funciones del Responsable del Sistema:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. 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 y/o Comité de Seguridad 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.
- 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 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.

6.3.4. Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informará y asesorará 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.
- Supervisará 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.

- Ofrecerá el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperará 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 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.

6.4. Funciones y obligaciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad de la Información:

- 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 (hasta el nombramiento de Delegado de Protección de Datos) las funciones 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.

6.5. Procedimientos de designación

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

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

7. 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 estarán recogidas en los documentos y normativas de seguridad de seguridad que se encuentran bajo la custodia del Servicio de Informática.

8. 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.

	Política de Seguridad	Identificador: ENS-02-POL-01
		Versión: 01
		Fecha: 30/04/2019
		Página 10 de 13

9. 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.

El Comité de Seguridad de la Información 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 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 los anexos I y II del Real Decreto 3/2010, de 8 de enero 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 (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

10. 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, 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 alto nivel (Políticas). Siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable 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.

11. 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 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.

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.

12. Modificaciones

EDICIÓN	FECHA	MODIFICACIONES RESPECTO A LA EDICIÓN ANTERIOR
01	30/04/2019	Edición Inicial