AYUNTAMIENTO DE TOLEDO

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. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizar la protección de los datos de carácter personal y facilitar preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

Por su parte, 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.

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, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que deberá ser aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1.

El Ayuntamiento de Toledo, con objeto de impulsar la máxima coordinación de actuaciones en esta materia y para garantizar los adecuados niveles de seguridad de la información en su ámbito y el establecimiento de criterios comunes, ha creado, mediante Resolución de la Junta de Gobierno Local de 24 de enero de 2018, el Comité Municipal de Seguridad de la Información, adscrito al Área de Gobierno de Hacienda, Patrimonio y Régimen Interior, como órgano colegiado competente para elaborar las propuestas de creación, modificación y actualización de la Política de Seguridad de la Información del Ayuntamiento de Toledo. Ejerciendo la citada competencia, el Comité Municipal de Seguridad de la Información ha redactado la Política de Seguridad del Ayuntamiento de Toledo, basada en los principios y directrices del Real Decreto 3/2020, de 8 de enero, y en las guías del Centro Criptológico Nacional CCN-STIC 805 “Política de Seguridad”, CCN-STIC 801 “Responsabilidades y funciones” y CCN-STIC 883 “Implantación del ENS en Entidades Locales”.

La presente Resolución, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información del Ayuntamiento de Toledo, propuesta por el Comité de Seguridad de la Información, así como establecer la estructura organizativa para implantarla y gestionarla. En virtud de lo anterior y en cumplimiento del artículo 11 del Real Decreto 3/2010, de 8 de enero, dispongo:

Primero: Aprobar la Política de Seguridad de la Información del Ayuntamiento de Toledo en los términos del Anexo que se incorpora en el presente acuerdo.

ANEXO

Política de Seguridad de la Información del Ayuntamiento de Toledo

Artículo 1. Objeto

La Política de Seguridad de la Información (en adelante, PSI), identifica responsabilidades y funciones, y establece el marco organizativo y normativo para la protección adecuada de la información y los servicios gestionados por medio de las Tecnologías de la Información y de las Comunicaciones, y se desarrolla en base a los principios definidos en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).

Artículo 2. Alcance

La seguridad comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones y debe entenderse como un proceso continuo de adaptación y mejora que debe ser controlado, gestionado y monitorizado.

La PSI se aplicará a todos los sistemas de información gestionados por el Ayuntamiento de Toledo y será de obligado cumplimiento para todas las personas que accedan tanto a los sistemas de información como a la propia información, con independencia de cuál sea su destino, adscripción o relación con el Ayuntamiento.

Artículo 3. Misión y objetivos del organismo

El Ayuntamiento de Toledo, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población del municipio de Toledo.

Para ejercer las competencias municipales el Ayuntamiento de Toledo hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

Artículo 4. Marco normativo

El Ayuntamiento de Toledo, en el ámbito de la administración electrónica, desarrolla sus funciones en el marco normativo relativo a la protección de datos de carácter personal europea y nacional, al procedimiento administrativo común, el régimen jurídico del sector público y a la demás normativa sobre administración electrónica que le resulta de aplicación.

En particular, constituyen el núcleo del marco normativo en lo relativo a administración electrónica, entre otras, las siguientes normas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y las modificaciones previstas en Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y el 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).
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Reglamento (UE) 910/2014 del Parlamento Europeo y el Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

Artículo 5. Principios y directrices de seguridad

Seguridad integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

Gestión de riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

Prevención, reacción y recuperación

La seguridad del sistema debe contemplar aspectos de prevención, detección, respuesta y recuperación, de manera que las amenazas existentes no se materialicen, o en caso de

materializarse no afecten gravemente a la información que maneja, o comprometa los servicios que presta.

El Ayuntamiento de Toledo debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, sus órganos directivos deben implementar las medidas mínimas de seguridad determinadas por el ENS, por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y por el RLOPD para tratamientos automatizados.

Así mismo deberán tenerse en cuenta las medidas especificadas en el artículo 32 del Reglamento UE 2016/679, que deberán garantizar un nivel de seguridad adecuado al riesgo para tratamientos automatizados, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, en particular:

a) Para garantizar el cumplimiento de la Política de Seguridad, los órganos directivos responsables deben:

- Autorizar los sistemas o los servicios antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.

b) Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, los órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

c) Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

Con el fin de garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Líneas de defensa

El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

- Ganar tiempo para una reacción adecuada.

- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

- Minimizar el impacto final sobre el mismo.

Reevaluación periódica

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

La seguridad como función diferenciada

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, siendo el Responsable de la Información quien determinará los requisitos de la información tratada, el Responsable del Servicio quien determinará los requisitos de los servicios prestados, y el Responsable de Seguridad quien determinará las decisiones técnicas para satisfacer los requisitos de seguridad de la información y de los servicios.

Autorización y control de acceso

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Adquisición de productos

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que 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.

Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles o móviles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

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

a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. 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.

Registro de actividad.

Con la finalidad exclusiva de lograr el cumplimiento del 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, se registrarán las actividades 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.

Artículo 6. Organización de seguridad

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI está compuesta por los siguientes agentes:

a) El Comité Municipal de Seguridad de la Información.
b) El Responsable de Seguridad.
c) El Responsable de la Información.
d) El Responsable del Servicio.
e) El Responsable del Tratamiento de Datos Personales.
f) El Responsable del Sistema.
g) El Delegado de Protección de Datos de carácter personal.

Artículo 7. El Comité Municipal de Seguridad de la Información.

Creado por Resolución de la Junta de Gobierno Local del Ayuntamiento de Toledo de 24 de enero de 2018 y publicado en el Boletín Oficial de la provincia de Toledo de 8 de junio de 2018, como órgano colegiado para el seguimiento, asesoramiento, coordinación y control en materia de seguridad de la información, adscrito al Área de Gobierno de Hacienda, Patrimonio y Régimen Interior. Su composición y régimen de funcionamiento se describen en la citada Resolución.

El Comité Municipal de Seguridad de la Información (en adelante, el Comité) tiene como finalidad velar por la seguridad de la información, asegurando el carácter armónico e integrador

de todas las actuaciones en esta materia y facilitando las actuaciones conjuntas de los diversos órganos afectados.

Para el cumplimiento de la finalidad descrita, en el ámbito de esta PSI, el Comité llevará a cabo las funciones siguientes:

a) Velar por el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad de la información para el personal del Ayuntamiento.

b) Elevar a la Junta de Gobierno de la Ciudad para su aprobación las resoluciones necesarias para el desarrollo de la PSI.

c) Elaborar las propuestas de modificación y actualización permanente de la PSI.

d) Elaborar y aprobar la normativa de seguridad derivada de segundo nivel (Normas de Seguridad de la Información).

e) Difundir los acuerdos aprobados por el Comité a toda la organización municipal.

f) Promover inversiones de carácter horizontal para garantizar la disponibilidad de recursos para atender a las diferentes necesidades de seguridad de la información.

g) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

h) Establecer una valoración de referencia para los diferentes tipos de información y servicios gestionados por el Ayuntamiento.

i) Establecer un criterio de riesgo aceptable para la seguridad de la información y los servicios.

j) Analizar los informes facilitados por el Responsable de Seguridad relativos al resultado de los análisis de riesgos, de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.

Artículo 8. El Responsable de la Información, del Servicio y del Tratamiento de Datos Personales.

El Comité será el máximo Responsable de la Información y del Servicio en el ámbito de esta PSI.

Como Responsable de la Información y Servicio determinará los requisitos de seguridad de la información tratada, según los parámetros del Anexo I del ENS para la categorización de los sistemas.

Asimismo, como Responsable de la Información, el Comité asumirá el papel de Responsable del Tratamiento de Datos Personales, y las funciones que para este rol especifica la normativa en vigor sobre tratamiento de datos personales. Como Responsable del

Tratamiento determinará los requisitos de seguridad de los tratamientos de datos personales, atendiendo a los riesgos para los derechos y libertades de los interesados.

Artículo 9. El Responsable de Seguridad.

El Responsable del Servicio Municipal de Informática del Ayuntamiento de Toledo asumirá las funciones de Responsable de la Seguridad. Su forma de designación y renovación serán las propias del puesto de trabajo integrado en la organización municipal. Asumirá las siguientes funciones:

a) Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los Responsables de la Información, de los Servicios y de los Tratamientos de Datos Personales.

b) Elaborar y aprobar la normativa de seguridad de tercer nivel (Procedimientos de seguridad) y difundir la misma entre los miembros de la organización.

c) Velar e impulsar el cumplimiento del cuerpo normativo definido en la PSI.

d) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas de acuerdo al análisis de riesgos.

e) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

f) Promover la mejora continua en la gestión de la seguridad de la información.

g) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

h) Coordinar la realización de análisis de riesgos periódicos sobre los sistemas de información bajo su responsabilidad.

i) Gestionar los incidentes de seguridad de la información que se produzcan, informando de los más relevantes al Comité.

j) La coordinación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.

k) La elaboración de un informe de revisión anual sobre el estado de la seguridad.

Artículo 10. El Responsable del Sistema.

El Centro Municipal de Informática ejercerá las funciones correspondientes al Responsable del sistema, que consistirán en:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Artículo 11. El Delegado de Protección de Datos de carácter personal.

El Delegado de Protección de Datos que haya sido designado por el Ayuntamiento de Toledo atendiendo a los requisitos de designación, cualificación y posición especificados en el Reglamento (UE) 2016/679, 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, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ejercerá las funciones indicadas en la citada normativa.

Artículo 12. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En su defecto, será el Comité quien resuelva.

En la resolución de estos conflictos, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 13. Gestión de Riesgos

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos, de conformidad con lo dispuesto en el artículo 6 del ENS, y en la reevaluación periódica.

El análisis de riesgos se realizará:

a) Regularmente, al menos una vez al año.
b) Cuando cambien sustancialmente la información manejada o los servicios prestados.
c) Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del ENS.
d) Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del ENS.

Para la armonización de los análisis de riesgos, el Comité establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, así como un nivel aceptable de riesgos residual.

El Responsable de la Información y el Servicio es el propietario de los riesgos sobre la Información y los servicios respectivamente, y como tal debe aceptar los riesgos residuales sobre los sistemas con anterioridad a su puesta en producción.

Artículo 14. Desarrollo Normativo

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento en el ámbito de la PSI, y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel se fundamente en las de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de Seguridad de la Información.
b) Segundo nivel normativo: Normas de Seguridad de la Información. Desarrollan y detallan la PSI, centrándose en un área o aspecto determinado de la seguridad de la información.
c) Tercer nivel normativo: Procedimientos de Seguridad de la Información. Especifican la implementación técnica de procedimientos de seguridad basados en las Normas de Seguridad de la Información.

Todos estos niveles prestarán especial atención a las exigencias derivadas del ENS, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Artículo 15. Proceso de revisión de la política de seguridad

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización municipal, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la organización.

Artículo 16. Difusión y formación

El Ayuntamiento de Toledo deberá adoptar las medidas necesarias para promover la difusión y concienciación en materia de seguridad de la información. Así mismo se realizarán acciones formativas periódicas en materia de seguridad de la información.