POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE MADRID Y SUS ORGANISMOS AUTÓNOMOS

1. Objetivo.

La Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos autónomos, en adelante la Política de Seguridad de la Información, identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

La Política de Seguridad de la Información es el instrumento en que se apoyan el Ayuntamiento de Madrid y sus Organismos autónomos para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el Ayuntamiento de Madrid.

2. Alcance.

Esta Política de Seguridad de la Información será de obligado cumplimiento para todos los órganos superiores y directivos del Ayuntamiento de Madrid y sus Organismos autónomos, así como para terceras partes a las que el Ayuntamiento de Madrid y sus Organismos autónomos presten servicios, cedan información, o de las que utilicen servicios o manejen información.

Esta Política estará disponible para consulta de todos ellos a través de la Sede Electrónica del Ayuntamiento de Madrid y del Boletín Oficial del Ayuntamiento de Madrid.

3. Principios y directrices.

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

Prevención.

El Ayuntamiento de Madrid 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 Esquema Nacional de Seguridad (en adelante, ENS) regulado mediante Real Decreto 3/2010, de 8 de enero, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política de Seguridad de la Información, 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.

Detección.

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, estos órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

Respuesta.

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

Recuperación.

Para 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.

4. Marco normativo.

El marco normativo de las actividades del Ayuntamiento de Madrid en el ámbito de esta Política de Seguridad de la Información está integrado por las siguientes normas:

a) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.
b) Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
c) Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.
d) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
e) Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
f) Ley 22/2006, de 4 de julio, de Capitalidad y de Régimen Especial de Madrid.
g) Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio.

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) Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
j) Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
k) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
l) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de carácter personal.
m) 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.
n) 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.
o) Decreto del Alcalde, de 17 de enero de 2005, por el que se regula la Atención al Ciudadano en el Ayuntamiento de Madrid.
p) Decreto de 1 de septiembre de 2010 del Delegado del Área de Gobierno de Hacienda y Administración Pública por el que se crean la Sede Electrónica y el Registro Electrónico del Ayuntamiento de Madrid.
q) Normas aplicables a la Administración Electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información.

5. Estructura.

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel: Política de Seguridad de la Información.
b) Segundo nivel: Instrucciones de Seguridad de la Información.
c) Tercer nivel: Procedimientos de Seguridad de la Información.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos del Ayuntamiento de Madrid y sus Organismos autónomos, sin necesidad de revisar su estrategia de seguridad.

El personal del Ayuntamiento de Madrid y de sus Organismos autónomos tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Instrucciones y los Procedimientos de Seguridad de la información estarán disponibles en la Intranet del Ayuntamiento de Madrid.

5.1. Primer nivel: Política de Seguridad de la Información.

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto y aprobada por la Junta de Gobierno.

5.2. Segundo nivel: Instrucciones de Seguridad de la Información.

El segundo nivel desarrolla la Política de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información.

Las Instrucciones de Seguridad de la Información serán aprobadas por el titular del Área de Gobierno competente en materia de tecnologías de la información y comunicaciones municipales a propuesta del Comité Municipal de Seguridad de la Información del Ayuntamiento de Madrid, y desarrollarán, al menos:

a) Gestión de activos de información inventariados, categorizados y asociados a un responsable.
b) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
c) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
d) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que sea transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
e) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
f) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información.
g) Gestión de los incidentes de seguridad implantando los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
h) Gestión de la continuidad implantando los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

5.3. Tercer nivel: Procedimientos de Seguridad de la Información.

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobados por el Responsable de Seguridad de la Información o por los Responsables de la Información o los de los Servicios, según su ámbito de competencia.

Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

6. Organización de la seguridad.

La organización de la seguridad en el Ayuntamiento de Madrid queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

6.1. Junta de Gobierno.

La Junta de Gobierno de la Ciudad de Madrid, mediante la aprobación del presente Acuerdo, asegura el compromiso de las autoridades del Ayuntamiento de Madrid en la aplicación del ENS.

Este compromiso se manifiesta mediante la aprobación de la Política de Seguridad de la Información, así como de todas aquellas modificaciones o actualizaciones de la misma que el Comité Municipal de Seguridad de la Información pueda proponer, en el ámbito de sus competencias.

6.2. Comité Municipal de Seguridad de la Información: composición, funciones y responsabilidades.

La composición, funciones y responsabilidades del Comité son establecidas en el Decreto de 25 de noviembre de 2014 de la Alcaldesa, de creación y regulación del Comité Municipal de Seguridad de la Información.

6.3. Responsable de Seguridad de la Información.

Es el Gerente del Organismo Autónomo Informática del Ayuntamiento de Madrid, que será el encargado de establecer las medidas necesarias para cumplir los requisitos de seguridad establecidos por los responsables de la información y de los servicios manejados por el sistema.

Teniendo en cuenta la complejidad organizativa y funcional de los medios electrónicos utilizados por el Ayuntamiento de Madrid y sus Organismos autónomos, en ejercicio de la potestad de autoorganización de la Administración municipal, el Responsable de Seguridad de la Información podrá asignar diversos cometidos a unidades orgánicas o empleados públicos, o especializar funciones por razones técnicas u organizativas. Esta asignación no supondrá en ningún caso una delegación de las competencias que le corresponden.

Sus responsabilidades y, en su caso, de las unidades o empleados especializados, son las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Analizar y elevar al Comité Municipal de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.
c) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.

d) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
e) Elaborar informes periódicos de seguridad para el Comité Municipal de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.
f) Realizar o promover auditorias periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
g) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

6.4. Grupo de Seguridad de la Información.

El Grupo de Seguridad de la Información se constituye en el seno del Comité Municipal de Seguridad de la Información como grupo de trabajo de apoyo técnico y administrativo al mismo. Su composición y funciones se establecen en el artículo 9 del Decreto de 25 de noviembre de 2014, de la Alcaldesa, por el que se crea y regula el Comité Municipal de Seguridad de la Información.

6.5. Responsable de la Información.

Es cada titular de la Dirección General o Gerente del Organismo Autónomo responsable de la información afectada por la presente Política de Seguridad de la Información, y que tiene la potestad de establecer los requisitos de la información en materia de seguridad en su ámbito de actuación. Sus responsabilidades son las siguientes:

a) Determinar los niveles de seguridad de la información tratada y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
b) Realizar, junto a los Responsables del Servicio y contando con la participación del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
c) Aceptar los riesgos residuales respecto de la información calculada en el análisis de riesgos.
d) Realizar el seguimiento y control de los riesgos.

El Responsable de la Información remitirá al Responsable de Seguridad el resultado de las tareas realizadas en el ámbito de estas responsabilidades, al menos una vez al año o a petición del mismo, reportando el resultado en formato adecuado para una integración de la información.

6.6. Responsable del Servicio.

Es cada titular de la Dirección General o Gerente del Organismo Autónomo responsable de cada servicio electrónico afecto a la presente Política de Seguridad de la Información, y que tiene la potestad de establecer los requisitos del servicio en materia de seguridad en su ámbito de actuación. Sus responsabilidades son las siguientes:

a) Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
b) Realizar, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
c) Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
d) Realizar el seguimiento y control de los riesgos.
e) Suspender, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

El Responsable del Servicio remitirá al Responsable de Seguridad el resultado de las tareas realizadas en el ámbito de estas responsabilidades, al menos una vez al año o a petición del mismo, reportando el resultado en formato adecuado para una integración de la información.

6.7. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad de la Información, elevándose para su resolución al Comité Municipal de Seguridad de la Información en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

7. Datos de carácter personal.

El Ayuntamiento de Madrid trata datos de carácter personal. La relación de ficheros creados e inscritos en la Agencia Española de Protección de Datos (AEPD) están publicados en la dirección de Internet: https://www.agpd.es;. Todos los sistemas de información del Ayuntamiento de Madrid se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal detallados en su correspondiente Documento de Seguridad.

8. Gestión de riesgos.

El Análisis de Riesgos, evaluando las amenazas y los riesgos a los que están expuestos la información, los servicios y sistemas del Ayuntamiento de Madrid y sus Organismos autónomos, se realizará:

a) Regularmente, al menos una vez al año.
b) Cuando cambie la información manejada.
c) Cuando cambien los servicios prestados.

d) Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.
e) Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.

Para la armonización de los Análisis de Riesgos, el Comité Municipal de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité Municipal de Seguridad de la Información, asimismo, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. Terceras partes.

Cuando el Ayuntamiento de Madrid utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité Municipal de Seguridad de la Información establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Madrid preste servicios a otros organismos o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan 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 exigirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

10. Revisión.

El Comité Municipal de Seguridad de la Información revisará anualmente la Política de Seguridad de la Información o cuando exista un cambio significativo que obligue a ello. La propuesta de revisión, en su caso, será aprobada por la Junta de Gobierno de la Ciudad de Madrid y difundida para que la conozcan todas las partes afectadas.