III. ADMINISTRACIÓN LOCAL

AYUNTAMIENTO DE

59 MADRID

ORGANIZACIÓN Y FUNCIONAMIENTO

Área de Gobierno de Vicealcaldía

Acuerdo de 7 de julio de 2022, de la Junta de Gobierno de la Ciudad de Madrid, por el que se aprueba la Política de Seguridad de la Información del Ayuntamiento de Madrid y de sus Organismos Públicos, y se modifica el Acuerdo de 5 de septiembre de 2019, de organización y competencias de la Coordinación General de la Alcaldía.

El Ayuntamiento de Madrid utiliza los medios que en cada momento ponen a su disposición las Tecnologías de la Información y de las Comunicaciones (TIC) para alcanzar sus objetivos.

Los sistemas TIC deben estar protegidos contra amenazas accidentales o deliberadas con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad 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 órganos superiores y directivos responsables de la información, los sistemas y los servicios electrónicos deben aplicar las medidas mínimas de seguridad exigidas por el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (en adelante, ENS), 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.

Según el artículo 8 ENS la seguridad de la información debe contemplar los aspectos de prevención, detección, respuesta y conservación, para conseguir que las amenazas sobre la misma no se materialicen y no afecten a los servicios que se prestan.

Los diferentes órganos superiores y directivos responsables deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema de información, 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 su financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos que incluyan sistemas TIC.

El Ayuntamiento de Madrid, 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 el Decreto del Alcalde de 17 de noviembre de 2021, el Comité Municipal de Seguridad de la Información, como órgano colegiado competente para elaborar las propuestas de modificación y actualización de la Política de Seguridad de la Información del Ayuntamiento de Madrid y de sus Organismos Públicos (en adelante, la Política de Seguridad de la Información), evaluando su idoneidad con una periodicidad mínima anual y proponiendo a la Junta de Gobierno del Ayuntamiento de Madrid su aprobación y revisión cuando proceda.

El Comité Municipal de Seguridad de la Información, de carácter interdepartamental, está adscrito a la Coordinación General de Alcaldía, órgano competente en materia de tecnologías de la información y comunicaciones municipales.

La Política de Seguridad de la Información, que se aprueba mediante el presente acuerdo, contiene los principios y directrices para la gestión de la seguridad de la información y el modelo organizativo para la gestión de dicha política.

En la misma, se incluyen los siguientes aspectos:

a) El objetivo y alcance de la Política de Seguridad de la Información.
b) El marco normativo aplicable en el ámbito de la Seguridad de la Información.
c) Los niveles aplicables en esta materia.
d) El modelo organizativo para la gestión de la Política de Seguridad de la Información.
e) Los roles, responsabilidades y funciones de los órganos municipales relacionados con la seguridad de la información.

BOCM-20220722-59

Finalmente, el acuerdo tiene también por objeto modificar el Acuerdo de 5 de septiembre de 2019 de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias de la Coordinación General de la Alcaldía, para delegar en la Coordinación General de la Alcaldía la competencia para dictar instrucciones específicas en materia de seguridad de la información.

En su virtud, de conformidad con lo dispuesto en los artículos 17.1.b) y h), y 17.2 de la Ley 22/2006, de 4 de julio, de Capitalidad y de Régimen Especial de Madrid, y en el artículo 19 del Reglamento Orgánico del Gobierno y de la Administración del Ayuntamiento de Madrid, de 31 de mayo de 2004, a propuesta de la titular de la Coordinación General de la Alcaldía, que eleva la Secretaria de la Junta de Gobierno, y previa deliberación de la Junta de Gobierno de la Ciudad de Madrid, en su reunión de 7 de julio de 2022,

ACUERDA

Primero.—Aprobar la Política de Seguridad de la Información del Ayuntamiento de Madrid y de sus Organismos Públicos que se inserta como anexo.

Segundo.—La Junta de Gobierno mantendrá permanentemente actualizada en la sede electrónica del Ayuntamiento de Madrid la Política de Seguridad de la Información del Ayuntamiento de Madrid y de sus Organismos Públicos acordando, en su caso, las modificaciones que estime oportunas.

Tercero.—En relación al gobierno de situaciones de cibercrisis previstas en el apartado 7 de la Política de Seguridad de la Información del Ayuntamiento de Madrid, hasta que el Plan Territorial de Emergencia Municipal del Ayuntamiento de Madrid incluya los riesgos de seguridad previstos en dicha política, el gobierno de las situaciones de cibercrisis se realizará por el Comité Municipal de Seguridad de la Información, que será expresamente convocado a tales efectos por su presidente.

Conforme a lo establecido en el artículo 9 del Decreto de 17 de noviembre de 2021, del Alcalde, por el que se crea el Comité Municipal de Seguridad de la Información, a dichas sesiones asistirán, junto a los miembros natos:

a) La persona titular de la Coordinación General de la Alcaldía.
b) La persona titular de la Dirección General de Emergencias y Protección Civil.
c) La persona titular de la Dirección General de Comunicación.
d) La persona titular de la Asesoría Jurídica.

Cuarto.—Queda sin efecto el Acuerdo de 24 de mayo de 2017, de la Junta de Gobierno de la Ciudad de Madrid, por el que se aprueba la Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos Públicos.

Asimismo, quedan sin efecto cuantas disposiciones se opongan, contradigan o resulten incompatibles con lo establecido en el presente acuerdo.

Quinto.—Modificar el Acuerdo de 5 de septiembre de 2019, de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias de la Coordinación General de la Alcaldía, en los términos que se indican a continuación:

En el apartado 3.º, se añade una nueva letra f) en el punto 2.8, que queda redactada en los siguientes términos:

"f) Dictar instrucciones en materia de seguridad de la información".

Sexto.—Se faculta al titular de la Coordinación General de la Alcaldía para resolver las dudas que pudieran surgir en la interpretación y aplicación del presente acuerdo.

Séptimo.—Se faculta al titular de la Coordinación General de la Alcaldía para dictar las resoluciones que sean necesarias para el desarrollo y la ejecución del presente acuerdo.

Octavo.—El presente acuerdo surtirá efectos desde la fecha de su adopción, sin perjuicio de su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID, en el "Boletín Oficial del Ayuntamiento de Madrid" y en la sede electrónica del Ayuntamiento de Madrid.

Noveno.—Del presente acuerdo se dará cuenta al Pleno, a fin de que quede enterado.

BOCM-20220722-59

ANEXO

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

1. *Objetivo*

1.1. La Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos Públicos (en adelante, la Política de Seguridad de la Información), identifica responsabilidades y establece principios y directrices para proteger la confidencialidad, integridad y disponibilidad de los servicios y activos de la información del Ayuntamiento de Madrid y de sus organismos públicos independientemente de su soporte de almacenamiento.

1.2. La Política de Seguridad de la Información es el instrumento en que se apoyan el Ayuntamiento de Madrid y sus organismos públicos para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones.

1.3. 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. *Ámbito de aplicación*

La Política de Seguridad de la Información será de obligado cumplimiento para todos los órganos superiores y directivos del Ayuntamiento de Madrid y sus organismos públicos, así como para todo su personal y para terceros a los que el Ayuntamiento de Madrid y sus organismos públicos presten servicios, cedan información, o de las que utilicen servicios o manejen información.

3. *Marco normativo*

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

a) 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.
b) Reglamento (UE) 910/2014 del parlamento europeo y del 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.
c) Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales, tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
d) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
e) Ley 6/2020, de 11 de noviembre, Reguladora de Determinados Aspectos de los Servicios Electrónicos de Confianza.
f) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
g) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
h) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
i) Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
j) Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público.
k) Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.
l) Ley 22/2006, de 4 de julio, de Capitalidad y de Régimen Especial de Madrid.
m) Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
n) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

BOCM-20220722-59

ñ) 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.
o) Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información.
p) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el reglamento de actuación y funcionamiento del sector público por medios electrónicos.
q) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información.
r) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
s) 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.
t) Ordenanza de Atención a la Ciudadanía y Administración Electrónica del Ayuntamiento de Madrid, de 26 de febrero de 2019.

4. *Principios y directrices*

Los principios y directrices que deben de contemplarse a la hora de garantizar la seguridad de la información y asegurar que el Ayuntamiento de Madrid cumpla sus objetivos utilizando sistemas de información, están dirigidos por el marco normativo indicado y se desarrollan en este apartado.

4.1. Alcance estratégico.

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Ayuntamiento para conformar un todo coherente y eficaz.

4.2. 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.

4.3. Seguridad por defecto.

Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4.4. 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.

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

4.5. Proporcionalidad.

El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

4.6. 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 los servicios que se prestan.

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 la normativa de seguridad vigente en materia de seguridad de la información y protección de datos de carácter personal.

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 de la Información, los órganos directivos responsables deben: autorizar los sistemas o los servicios antes de entrar en operación; evaluar regularmente la seguridad, incluyendo evaluacio-

BOCM-20220722-59

nes de los cambios de configuración realizados de forma rutinaria, y 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 10 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 la 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.

4.7. 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:

a) Ganar tiempo para una reacción adecuada.
b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
c) Minimizar el impacto final.

4.8. 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.

4.9. 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 la seguridad quien determinará las decisiones técnicas para satisfacer los requisitos de seguridad de la información y de los servicios.

5. *Estructura*

5.1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en los tres niveles indicados a continuación, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior:

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 públicos, sin necesidad de revisar su estrategia de seguridad.

5.2. El personal del Ayuntamiento de Madrid y de sus organismos públicos 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.

5.3. Niveles del cuerpo normativo sobre seguridad de la información:

5.3.1. 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.

BOCM-20220722-59

5.3.2. 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.

De conformidad con el apartado 3.º.2.8 f) del Acuerdo de 5 de septiembre de 2019, de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias de la Coordinación General de la Alcaldía, las instrucciones de seguridad de la información serán aprobadas por la persona titular de la Coordinación General de la Alcaldía, a propuesta del Comité Municipal de Seguridad de la Información del Ayuntamiento de Madrid, y desarrollarán, al menos las siguientes materias:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.
b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.
c) 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.
d) 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.
e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se 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.
f) 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.
g) 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.
h) Gestión de los incidentes de seguridad implantando los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
i) 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.

5.3.3. 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 aprobadas por el responsable de la seguridad 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 organizativo específico o a un sistema determinado.

6. *Organización de la Seguridad de la Información*

La organización de la seguridad de la información en el ámbito descrito por la Política de Seguridad de la Información queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la siguiente estructura organizativa.

6.1. Junta de Gobierno.

La Junta de Gobierno de la Ciudad de Madrid, mediante la aprobación de la Política de Seguridad de la Información, así como de todas sus modificaciones o actualizaciones, expresa el compromiso del Ayuntamiento de Madrid en la aplicación del ENS.

6.2. Comité Municipal de Seguridad de la Información.

6.2.1. La composición, funciones y responsabilidades del Comité Municipal de Seguridad de la Información (en adelante, el Comité) son establecidas en el Decreto de 17 de

BOCM-20220722-59

noviembre de 2021, del Alcalde, por el que se crea el Comité Municipal de Seguridad de la Información y se regula su composición y funcionamiento.

6.3. Responsable de la seguridad.

6.3.1. De conformidad con los artículos 3 y 15.1.l) y m) de los Estatutos del Organismo Autónomo Informática del Ayuntamiento de Madrid, de 29 de junio de 2004, corresponde al titular de la Gerencia del Organismo Autónomo Informática del Ayuntamiento de Madrid ser responsable de la seguridad del Ayuntamiento de Madrid y sus organismos públicos y 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.

6.3.2. En el ejercicio de las citadas competencias, el responsable de la seguridad desarrollará las siguientes funciones:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Velar por la independencia en la toma de decisiones y separación de funciones en materia de seguridad de la información.
c) Analizar y elevar al Comité toda la documentación relacionada con las instrucciones de seguridad de la información para su aprobación.
d) 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.
e) Promover la mejora continua en la gestión de la seguridad de la información.
f) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
g) Impulsar la formación y concienciación en materia de seguridad de la información.
h) Elaborar informes periódicos de seguridad para el Comité, que incluirán los incidentes más relevantes de cada período.
i) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
j) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.
k) Nombrar responsables de seguridad delegados, tal y como se definen en el apartado 6.6.
l) Proponer al responsable de un sistema de información o servicio su detención si se aprecian deficiencias graves de seguridad.

6.4. Responsable de la información.

6.4.1. Son responsables de la información los titulares de los órganos directivos del Ayuntamiento de Madrid y de sus organismos públicos responsables de la información afectada por la Política de Seguridad de la Información, en sus respectivos ámbitos de competencias.

6.4.2. Corresponde al responsable de la información establecer los requisitos de la información en materia de seguridad, y en particular:

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 41 ENS.
b) Realizar, junto a los responsables del servicio y el responsable de la 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.
e) Proponer al responsable de un sistema de información o servicio su detención si se aprecian deficiencias graves de seguridad que afecten a la información de la que es responsable.

6.5. Responsable del servicio.

6.5.1. Son responsables del servicio los titulares de los órganos directivos del Ayuntamiento de Madrid y de sus organismos públicos responsables de cada servicio electrónico afecto a la Política de Seguridad de la Información, en sus respectivos ámbitos de competencias.

6.5.2. Corresponde al responsable del servicio establecer los requisitos del servicio en materia de seguridad, y en particular:

BOCM-20220722-59

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 41 del ENS.
b) Realizar, junto a los responsables de la información y el responsable de la 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 la prestación de un servicio electrónico o el manejo de una determinada información, cuando se encuentre afectada por deficiencias graves de seguridad.

6.6. Responsable de seguridad delegado.

6.6.1. El responsable de la seguridad podrá nombrar responsables de seguridad delegados.

6.6.2. Corresponde a los responsables de seguridad delegados ejercer, en el ámbito de competencias para el que haya sido nombrado, las funciones del apartado 6.3.2, salvo la letra k), entendiendo las referencias realizadas al Comité en las letras c) y h) son para el responsable de la seguridad.

6.7. Responsable del sistema.

6.7.1. Son responsables del sistema los titulares de los órganos directivos del Ayuntamiento de Madrid y de sus organismos públicos que gestionen la operación de sistemas de información en el Ayuntamiento de Madrid, en sus respectivos ámbitos de competencias.

6.7.2. Corresponde al responsable del sistema:

a) Desarrollar, operar y mantener los sistemas de información en el ámbito de su competencia.
b) Verificar el correcto funcionamiento de los sistemas de información en su ámbito de competencia, incluyendo sus especificaciones, instalación y monitorización de su correcto funcionamiento.
c) Definir su arquitectura y la gestión de la misma, estableciendo sus criterios y perfiles de uso.
d) Aplicar las medidas de seguridad necesarias, de acuerdo con la política, las instrucciones y los procedimientos de seguridad de la información del Ayuntamiento de Madrid.
e) Proponer mejoras en las medidas de seguridad existentes al responsable de la seguridad.
f) Detener el sistema de información cuando se encuentre afectado por deficiencias graves de seguridad.
g) Definir, elaborar y supervisar la ejecución de planes paliativos respecto de la prestación de un servicio o tratamiento en caso de que sea necesaria su detención.

6.8. Resolución de conflictos.

6.8.1. 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, este será resuelto por el órgano competente de conformidad con lo previsto en los acuerdos de la Junta de Gobierno de organización y competencias y los estatutos del correspondiente organismo público, dando cuenta al Comité.

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

7. *Gobierno de situaciones de cibercrisis*

El gobierno a nivel corporativo de las situaciones de cibercrisis, entendidas como aquellas en las que se produzcan ciberincidentes que tengan un impacto crítico en la seguridad de los sistemas de información concernidos, se realizará conforme a lo previsto en el Plan Territorial de Emergencia Municipal del Ayuntamiento de Madrid.

8. *Datos de carácter personal*

8.1. El Ayuntamiento de Madrid realiza tratamientos de datos de carácter personal. La relación de actividades de tratamiento se encuentra publicada en el Registro de Activi-

BOCM-20220722-59

dades de Tratamiento del Ayuntamiento, que está disponible para su consulta en la sede electrónica del Ayuntamiento de Madrid.

8.2. Todos los sistemas de información del Ayuntamiento de Madrid se ajustarán a los requisitos de seguridad definidos por los responsables de tratamiento de los datos de carácter personal que dichos sistemas manejen, de acuerdo con lo exigido por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre; la Ley Orgánica 7/2021, de 26 de mayo; y las directrices y normas dictadas por el Delegado de Protección de Datos del Ayuntamiento de Madrid.

8.3. Intervienen en esta materia los responsables y encargados de tratamiento, así como el Delegado de Protección de Datos, con las obligaciones y responsabilidades recogidas en la legislación que les resulta de aplicación.

9. *Concienciación y formación*

9.1. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

9.2. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos.

El personal del Ayuntamiento de Madrid recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

9.3. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

10. *Gestión de riesgos*

10.1. El análisis y gestión de riesgos, evaluando las amenazas y los riesgos a los que están expuestos la información, los servicios y sistemas del Ayuntamiento de Madrid y de sus organismos públicos, será la base para determinar las medidas de seguridad que se deben adoptar.

10.2. El análisis de riesgos se realizará regularmente, al menos una vez al año, así como en estos supuestos:

a) Cuando cambie la información manejada.
b) Cuando cambien los servicios prestados.
c) Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el anexo I ENS.
d) Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el anexo I ENS.

10.3. 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.

Asimismo, el Comité dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. *Servicios e información de terceros*

11.1. Cuando el Ayuntamiento de Madrid utilice servicios o maneje información de terceros, les hará partícipes de la Política de Seguridad de la Información.

El Comité establecerá canales para el reporte y la coordinación de los respectivos comités de seguridad de dichos terceros y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

11.2. Cuando el Ayuntamiento de Madrid preste servicios a otros organismos o ceda información a terceros, les hará partícipes de la Política de Seguridad de la Información y de las instrucciones y procedimientos que atañan a dichos servicios o información, quedando sujetos a las obligaciones que en ellos se establezcan, sin perjuicio de que puedan desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias y se exigirá que el personal de dichos terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en la Política de Seguridad de la Información.

BOCM-20220722-59

11.3. Cuando algún aspecto de la Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte, de conformidad con lo dispuesto en los puntos 10.1 y 10.2, será necesario que el responsable de la seguridad emita un informe en el que se precisen 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 para poder continuar con la utilización del servicio o el manejo de la información.

12. *Revisión*

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

Madrid, a 7 de julio de 2022.—La Directora de la Oficina del Secretario de la Junta de Gobierno, Carmen Toscano Ramiro.

(03/14.544/22)

BOCM-20220722-59