Política de Seguridad de la Información

Ayuntamiento de Málaga

Mayo 2019

Índice

1 APROBACIÓN Y ENTRADA EN VIGOR ... 3
2 OBJETIVOS Y MISIÓN DEL AYUNTAMIENTO ... 3
3 OBJETIVOS Y MISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ... 3
4 ALCANCE ... 4
5 MARCO NORMATIVO ... 4
6 REVISIÓN DE LA POLÍTICA ... 5
7 ORGANIZACIÓN DE LA SEGURIDAD ... 5
7.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES ... 6
7.1.1 Junta de Gobierno Local ... 6
7.1.2 Junta Rectora del CEMI ... 6
7.1.3 Comité Municipal de Seguridad de la Información (MSI) ... 6
7.1.4 Comité de Seguridad de Tecnologías de Información y Comunicación (STIC) ... 7
7.2 ROLES: FUNCIONES Y RESPONSABILIDADES ... 8
7.2.1 Responsable de la información ... 8
7.2.2 Responsable del servicio ... 8
7.2.3 Responsable del tratamiento ... 8
7.2.4 Delegado de Protección de Datos ... 8
7.2.5 Presidente del Comité MSI ... 8
7.2.6 Gerente de la organización municipal ... 9
7.2.7 Coordinador de los Comités STIC/MSI ... 9
7.2.8 Responsable del área de Recursos Humanos y Calidad ... 9
7.2.9 Responsable del área Jurídica ... 9
7.2.10 Responsable de Seguridad de la Información ... 9
7.2.11 Responsable de los Sistemas CEMI ... 9
7.2.12 Responsable de Clientes CEMI ... 10
7.3 PROCEDIMIENTOS DE DESIGNACIÓN DE LOS COMITÉS ... 10
8 ANÁLISIS Y GESTIÓN DE RIESGOS ... 10
9 DIRECTRICES PAR LA CONTRATACIÓN Y/O USO DE SERVICIOS DE “COMPUTACIÓN EN NUBE” 10
9.1 DESCRIPCIÓN DE MODELOS DE DESPLIEGUE Y TIPOS DE SERVICIO ... 10
9.1.1 Modelos de despliegue: ... 10
9.1.2 Tipos de servicio: ... 11
9.1.3 Despliegue del servicio ... 11
9.2 Confidencialidad del servicio ... 11
9.3 RESPONSABILIDADES Y OBLIGACIONES ... 12
9.4 PRIVACIDAD Y PROTECCIÓN DE DATOS ... 12
9.5 SEGUIMIENTO Y FINALIZACIÓN DEL SERVICIO ... 12
9.6 MEDIOS ALTERNATIVOS ... 12
9.7 USO DE SERVICIOS GRATUITOS DE “COMPUTACIÓN EN NUBE” ... 12
10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ... 13
10.1 Instrumentos de desarrollo ... 13
10.2 Aprobación de las normas de seguridad ... 13
10.3 Sanciones previstas por incumplimiento ... 13
11 SEGURIDAD DE LA INFORMACIÓN ... 13
12 DATOS DE CARÁCTER PERSONAL ... 14
13 OBLIGACIONES DEL PERSONAL ... 14
14 TERCERAS PARTES ... 14

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Junta de Gobierno Local del Ayuntamiento de Málaga, el día 24 de mayo de 2019.
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.
La entrada en vigor de la presente Política de Seguridad de la Información del Ayuntamiento de Málaga supone la derogación de cualquier otra que existiera a nivel de los diferentes departamentos municipales.

2 OBJETIVOS Y MISIÓN DEL AYUNTAMIENTO

El Ayuntamiento de Málaga, 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 Málaga.

El Ayuntamiento de Málaga ejerce sus competencias, en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Andalucía.

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

3 OBJETIVOS Y MISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Ayuntamiento de Málaga ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, en el ámbito de la administración electrónica, reconociendo así como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Ayuntamiento de Málaga.

El marco de gestión de seguridad de la información abarca igualmente la protección de datos de carácter personal y tiene en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD, así como lo contemplado en la legislación de carácter nacional en dicha materia.

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por el Ayuntamiento de Málaga.
2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

3. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
4. Proteger los recursos de información del Ayuntamiento de Málaga y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Esta Política de Seguridad asegura un compromiso manifiesto de las máximas Autoridades del Ayuntamiento de Málaga, para la difusión, consolidación y cumplimiento de la presente Política.

4 ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para todos los Departamentos Municipales del Ayuntamiento de Málaga, entendiendo por Departamentos Municipales a sus Áreas y Distritos, sus Organismos Autónomos y Agencias Públicas, Sociedades Mercantiles con mayoría de capital social municipal y demás entes que decida la Junta de Gobierno Local; a sus recursos y a los procesos afectados por el ENS, RGPD y LOPDGDD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

5 MARCO NORMATIVO

Se toma como referencia, sin carácter exhaustivo, la siguiente legislación:

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- 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.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 27/2013, de 27 de diciembre, de Racionalización y Sostenibilidad de la Administración Local.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

- Real Decreto 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad del Ayuntamiento de Málaga en el ámbito de sus competencias y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por la Corporación igualmente en el ejercicio de sus competencias.

6 REVISIÓN DE LA POLÍTICA

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.

La Política será propuesta y revisada por la Junta Rectora del Centro Municipal de Informática (en adelante CEMI) con el apoyo del Comité de Seguridad de Tecnologías de la Información y Comunicación (en adelante Comité STIC), aprobada por la Junta de Gobierno Local y difundida por el Comité Municipal de Seguridad de la Información (en adelante Comité MSI) para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá a la Junta de Gobierno Local para resolución de los mismos, previo informe propuesta del Comité MSI.

7 ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información del Ayuntamiento de Málaga son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Para una mejor respuesta a incidentes de seguridad, el Ayuntamiento de Málaga mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, definidas y documentadas.

7.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

Tomando como base esta política, el documento de organización de la seguridad detalla la gestión interna del Comité de Seguridad de Tecnologías de la Información y Comunicación (STIC) y del Comité Municipal de Seguridad de la Información (MSI), identificando a todos sus miembros y detallando las atribuciones de cada responsable así como los mecanismos de coordinación y resolución de conflictos.

7.1.1 Junta de Gobierno Local

En materia de seguridad de la información, la Junta de Gobierno Local del Ayuntamiento de Málaga tiene las siguientes funciones:

- Aprobar la Política de Seguridad de la Información del Ayuntamiento de Málaga y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad y el Reglamento General de Protección de Datos, por delegación de la Alcaldía-Presidencia.
- Aprobar el desarrollo organizativo propuesto por el Comité Municipal de Seguridad de la Información (Comité MSI), o por la Junta Rectora del CEMI, por delegación de la Alcaldía-Presidencia.
- Nombramiento y cese de los integrantes del Comité MSI.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta de la Junta Rectora del CEMI y/o Comité MSI.
- Nombrar al Delegado de Protección de Datos de la organización municipal, a propuesta del Presidente del Comité MSI, previo informe de la Dirección General de Recursos Humanos, Calidad y Seguridad.

7.1.2 Junta Rectora del CEMI

La Junta de Gobierno Local, a fecha 9 de noviembre de 2013, delega en la Junta Rectora del CEMI las competencias en materia de seguridad de la información, y en concreto las siguientes:

- Elaborar y proponer la política de seguridad de la organización municipal, para su posterior aprobación por la Junta de Gobierno Local.
- Velar por que la seguridad de la información sea parte del proceso de planificación de la organización municipal.

Para realizar la tarea encomendada a la Junta Rectora del CEMI en materia de seguridad de la información, ésta realiza las siguientes funciones:

- Nombramiento y cese de los integrantes del Comité de Seguridad de Tecnologías de Información y Comunicación (Comité STIC).

7.1.3 Comité Municipal de Seguridad de la Información (MSI)

El comité MSI tiene las siguientes funciones:

- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Elaborar y proponer a la Junta de Gobierno Local el desarrollo organizativo que permita el cumplimiento de los esquemas nacionales de seguridad e interoperabilidad, así como del Reglamento General de Protección de Datos.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

- Recabar informes regulares del estado de seguridad de la información de la organización municipal y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la Junta de Gobierno Local y al Comité STIC.
- Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de los distintos departamentos municipales.
- Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica del Ayuntamiento de Málaga.
- Llevar a cabo acciones de concienciación, formación y motivación del personal municipal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos municipales, usuarios y ciudadanos y la protección de su información.

El funcionamiento de este Comité supone el desempeño de los siguientes roles:

- Presidente del Comité MSI
- Gerente de la organización municipal
- Responsable del área de recursos humanos
- Responsable del área jurídica
- Coordinador del Comité MSI
- Responsable de seguridad de la información
- Responsable de los Clientes CEMI

7.1.4 Comité de Seguridad de Tecnologías de Información y Comunicación (STIC)

Dentro del CEMI se crea el Comité STIC que eleva a la Junta Rectora todas sus propuestas.

El Comité STIC tiene las siguientes funciones:

- Proponer a la Junta Rectora del CEMI la revisión de la Política de Seguridad de la Información del Ayuntamiento de Málaga, para su ulterior elevación a la Junta de Gobierno Local.
- Proponer a la Presidencia del Comité MSI las instrucciones de servicio y circulares que permitan la implantación de los esquemas nacionales de seguridad e interoperabilidad, en el ámbito de la organización municipal.
- Proponer criterios de seguridad: redactar, revisar y evaluar las normas técnicas y pautas de seguridad así como los procedimientos de notificación de incidentes de seguridad.
- Evaluar e informar sobre los riesgos de seguridad en los activos TIC.
- Velar por el alineamiento de las actividades de seguridad de la información y los objetivos de la organización municipal, llevando a cabo acciones orientadas a la mejora continua de los procesos de seguridad de la información.
- Velar por que la seguridad de la información sea parte del proceso de planificación de la organización municipal.

Estará formado por los siguientes roles:

- Coordinador del Comité STIC
- Responsable de Seguridad de la Información

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

- Responsable de los Sistemas CEMI

El coordinador del Comité STIC podrá incorporar a los técnicos y asesores que considere oportunos para el desarrollo de sus competencias.

7.2 ROLES: FUNCIONES Y RESPONSABILIDADES

Tomando como base esta política, existirá un documento de organización de la seguridad, en el que se recojan las funciones de los diferentes responsables, así como los mecanismos de nombramiento y cese de los mismos.

7.2.1 Responsable de la información

De acuerdo con lo especificado en el ENS, le corresponde la potestad de establecer los requisitos de la información en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de la información.

Dicha potestad se ejercitará por el Director General / Gerente / máximo responsable ejecutivo del Área o ente instrumental, de conformidad con lo que establezcan las instrucciones de servicio y circulares dictadas por el Presidente del Comité MSI, y previo informe del Responsable de Seguridad de la Información y del Responsable del Sistema.

El Responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección, siendo el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

7.2.2 Responsable del servicio

De acuerdo con lo especificado en el ENS, le corresponde la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de los servicios.

Dicha potestad se ejercitará por el Director General / Gerente / máximo responsable ejecutivo del Área o ente instrumental, de conformidad con lo que establezcan las instrucciones de servicio y circulares dictadas por Presidente del Comité MSI, y previo informe del Responsable de Seguridad de la Información y del Responsable del Sistema.

7.2.3 Responsable del tratamiento

De acuerdo con lo especificado en el RGPD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Este rol, que recae sobre el Ayuntamiento de Málaga, será desempeñado por el Director General/Gerente o máximo responsable ejecutivo del departamento municipal correspondiente.

7.2.4 Delegado de Protección de Datos

Tiene asignadas las funciones contempladas en el art. 39 del Reglamento General de Protección de Datos.

La designación para el desempeño de este rol se efectuará por la Junta de Gobierno Local.

7.2.5 Presidente del Comité MSI

Preside el Comité Municipal de Seguridad de la Información y, por delegación de la Alcaldía-Presidencia, será el responsable de aprobar las instrucciones de servicio y circulares que permita el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad, en el ámbito de la organización municipal.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

Propone a la Junta de Gobierno Local el nombramiento del Delegado de Protección de Datos para toda la organización municipal, dando cuenta del mismo al Comité MSI.

Es el responsable de la determinación de la categoría del sistema y de que se realice el análisis y gestión de riesgos, aplicado a los sistemas de tratamiento de la información.

Este rol recae en el Concejal que tenga delegadas la funciones en materia de Nuevas Tecnologías.

7.2.6 Gerente de la organización municipal

Pertenece al Comité Municipal de Seguridad de la Información y será el responsable de la coordinación general de los distintos departamentos municipales para la eficaz aplicación de la política de Seguridad de la Información. Este rol recae sobre el Coordinador General Gerente del Ayuntamiento.

7.2.7 Coordinador de los Comités STIC/MSI

Será el responsable de coordinar las acciones del Comité STIC y del Comité MSI así como de impulsar la implementación y cumplimiento de la presente política. En nombre del Comité MSI recabará de los responsables de los departamentos municipales informes regulares del estado de seguridad de la información. Es el responsable de elaborar el ciclo de vida de seguridad de los servicios TIC del CEMI (especificación, arquitectura, desarrollo, operación y cambios) así como de definir la topología de los sistemas de información del CEMI. Este rol recae sobre el Gerente del CEMI. La misma persona ejerce este rol en los dos comités siendo el nexo de unión entre ambos.

7.2.8 Responsable del área de Recursos Humanos y Calidad

Pertenece al Comité Municipal de Seguridad de la Información y cumplirá la función de implicar a todo el personal de la organización municipal en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados municipales y de la capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el titular de la Dirección General de Personal, Organización y Calidad.

7.2.9 Responsable del área Jurídica

Pertenece al Comité de Seguridad Municipal de la Información y asesorará en material legal en lo que se refiere al diseño e implementación de las políticas y medidas que se establezcan en relación a la seguridad de la información. Y, específicamente en cuanto se refiere al cumplimiento de la legislación sobre seguridad de la información de cuantos contratos, convenios, acuerdos, ordenanzas y similares sea parte el Ayuntamiento de Málaga. Este rol recae sobre el titular de la Asesoría Jurídica de la organización municipal.

7.2.10 Responsable de Seguridad de la Información

Cumplirá funciones relativas a la seguridad de los sistemas de información del Ayuntamiento de Málaga, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en el Ayuntamiento de Málaga. Es el equivalente al "*Responsable de Seguridad*" enunciado en el Esquema Nacional de Seguridad (RD 3/2010). Este rol recae sobre el Responsable del Proceso de Gestión de la Seguridad de la Información del CEMI. Es la misma persona en ambos Comités.

7.2.11 Responsable de los Sistemas CEMI

Pertenece al Comité STIC y cumplirá la función de cubrir los requerimientos de seguridad informática establecidos en los sistemas y recursos de tecnología en el ámbito de los sistemas del Centro Municipal de Informática (CEMI). Este rol es el equivalente al "*Responsable del*

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

Sistema" enunciado en el Esquema Nacional de Seguridad (RD 3/2010). Este rol es desempeñado por el Responsable de la Explotación de los Sistemas de Información del CEMI.

7.2.12 Responsable de Clientes CEMI

Cumplirá funciones de representación de los departamentos municipales a los que el CEMI presta servicios TIC (clientes CEMI), velando por la seguridad de la información y servicios TIC suministrados a dichos departamentos municipales. Este rol es desempeñado por el Responsable de la Gestión de Clientes del CEMI.

7.3 PROCEDIMIENTOS DE DESIGNACIÓN DE LOS COMITÉS

Corresponde a la Junta de Gobierno Local el nombramiento y el cese de los componentes del Comité Municipal de Seguridad de la Información, para el ejercicio de las competencias definidas en la presente política. La Presidencia del Comité recaerá en el Concejal que tenga delegadas las competencias en materia de Nuevas Tecnologías, y actuará como Coordinador el Gerente del CEMI. La Junta de Gobierno Local podrá revisar los nombramientos del Comité Municipal de Seguridad de la Información cuando estime oportuno.

Corresponde a la Junta Rectora del CEMI el nombramiento y el cese de los componentes del Comité STIC, a propuesta del Gerente del CEMI, quien desempeñará el rol de Coordinador de este Comité. La Junta Rectora del CEMI podrá revisar los nombramientos del Comité STIC a solicitud del Gerente del CEMI, o tras la baja voluntaria o forzosa de cualquiera de sus miembros.

8 ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El nivel de riesgo máximo aceptable, se establecerá en base a la metodología elegida, Magerit.

El nivel máximo de riesgo aceptable se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen.

9 DIRECTRICES PAR LA CONTRATACIÓN Y/O USO DE SERVICIOS DE "COMPUTACIÓN EN NUBE"

9.1 DESCRIPCIÓN DE MODELOS DE DESPLIEGUE Y TIPOS DE SERVICIO

9.1.1 Modelos de despliegue:

Nube pública. Aquella que está preparada para el uso abierto al público en general. La infraestructura y los recursos están en manos de terceros y los servicios pueden ser utilizados y compartidos por usuarios de múltiples organizaciones.

Nube privada. Aquella preparada para el uso exclusivo de una sola organización y que puede ser gestionada por la propia entidad, por un tercero o alguna combinación de los dos. Una nube privada puede ser interna, si está ubicada en las instalaciones del cliente o externalizada, si los servidores se encuentran alojados en un tercero.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

Nube comunitaria. Aquella que está preparada para ser compartida entre varias organizaciones que tienen unas políticas similares (seguridad, privacidad, cumplimientos normativos...). Puede ser gestionada por las propias organizaciones participantes o por un tercero, y también pueden ser internas, si están implementadas en las instalaciones de uno de los participantes de la comunidad o externalizadas si los servidores se encuentran alojados en un tercero.

Nube híbrida. Aquella en la que la infraestructura es una composición de dos o más tipos de nube (privada, comunitaria o pública), que mantienen su propia identidad pero que son unidas por una tecnología estandarizada que permite la portabilidad de las aplicaciones y de los datos.

9.1.2 Tipos de servicio:

IaaS (Infraestructura como un servicio) es el nivel más bajo de servicio. Se encarga de entregar una infraestructura de procesamiento completa al usuario, normalmente mediante una plataforma de virtualización. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red.

PaaS (Plataforma como un servicio) es un nivel intermedio que se encarga de entregar una plataforma de procesamiento completa a la organización cliente. El consumidor no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.

SaaS (Software como un servicio) es aquel en el que el proveedor de "computación en la nube" es el encargado de ofrecer al consumidor el software como un servicio a través de Internet. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como por ejemplo un navegador web; el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza.

9.1.3 Despliegue del servicio

La selección del modelo de despliegue de este tipo de servicios vendrá condicionada por la categorización de la información gestionada por el Sistema, en su parámetro de confidencialidad según clasificación ENS, siendo los requisitos mínimos los dispuestos en la siguiente tabla:

Infraestructura	N/A	Bajo	Medio	Alto
Nube pública	X	X		
Nube comunitaria externalizada	X	X	X	
Nube comunitaria interna	X	X	X	X
Nube privada externalizada	X	X	X	
Nube privada interna	X	X	X	X

9.2 CONFIDENCIALIDAD DEL SERVICIO

El proveedor deberá comprometerse a mantener la confidencialidad en el tratamiento de la información proporcionada por el AYUNTAMIENTO. Esto implica, además del cumplimiento legal en materia de protección de datos, que el proveedor firme el acuerdo de confidencialidad vigente en la organización municipal, así como a implantar unos controles de acceso adecuados a la normativa ENS.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

9.3 RESPONSABILIDADES Y OBLIGACIONES

Al proveedor de servicios contratados se le exigirá el cumplimiento de, al menos, las siguientes responsabilidades:

- Garantizar el cumplimiento de las medidas de seguridad, previstas en el ENS, RGPD y LOPDGDD, que sean requeridas para los sistemas objeto de prestación del servicio.
- Realización de mantenimiento y actualización de sistemas, de acuerdo al tipo de servicio contratado.
- Notificar todos los incidentes que pueden comprometer la seguridad del servicio o de la información al AYUNTAMIENTO.
- Realizar la entrega de informes de monitorización de servicios.
- Realizar auditorías que demuestren el adecuado cumplimiento normativo.
- Garantizar el correcto funcionamiento de los servicios contratados cumpliendo con los niveles de servicio fijados en los Acuerdos de Nivel de Servicios (SLAs).
- Mantener el principio de confidencialidad durante y tras la finalización de la relación contractual.

9.4 PRIVACIDAD Y PROTECCIÓN DE DATOS

El proveedor asumirá el rol de encargado del tratamiento, siendo, en todo momento, la organización municipal la Responsable del Tratamiento.

El encargado del tratamiento no podrá subcontratar con un tercero la realización de servicios que incluyan el tratamiento de los datos provistos por el cliente, salvo aquellos supuestos en los se disponga de autorización expresa por parte del Responsable del Tratamiento.

En caso de que el proveedor de servicios de "computación en la nube" emplee centros de procesamiento de datos emplazados en terceros países, fuera del Espacio Económico Europeo o a estados que no proporcionen un nivel adecuado de protección, se considerará que dicho servicio implicará la realización de transferencias internacionales de datos, por lo que éstas deberán ser tratadas de acuerdo a lo establecido en el RGPD y la LOPDGDD.

9.5 SEGUIMIENTO Y FINALIZACIÓN DEL SERVICIO

Se deberán definir mecanismos para facilitar el adecuado seguimiento y monitorización del servicio. Para esto el proveedor deberá poner a disposición del AYUNTAMIENTO las herramientas que permitan verificar la correcta prestación del servicio de acuerdo a lo estipulado contractualmente, así como definir procedimientos para la coordinación y comunicación entre cliente y proveedor ante desviaciones, incidentes, peticiones o cambios en el servicio.

Los contratos deberán incluir las condiciones de finalización del servicio y la recuperación de los activos de información.

9.6 MEDIOS ALTERNATIVOS

La prestación de servicios de "computación en la nube" por parte de un tercero, exige que se deban tener medios alternativos para aprovisionar el servicio en caso de caída del mismo. Esta medida es aplicable para todos los sistemas cuya disponibilidad haya sido categorizada con nivel ALTO, según el ENS.

9.7 USO DE SERVICIOS GRATUITOS DE "COMPUTACIÓN EN NUBE"

El uso de estos servicios deberá ser autorizado por el CEMI y, en cualquier caso, la responsabilidad del cumplimiento respecto a ENS, RGPD, LOPDGDD o de cualesquiera otras normas de obligado cumplimiento, así como del correcto tratamiento de los datos en términos generales desde el punto de vista de su seguridad, recaerá siempre sobre el departamento

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

municipal responsable de la información, con independencia de la existencia de acuerdos, seguros u otras medidas compensatorias.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

10.1 INSTRUMENTOS DE DESARROLLO

La Política de Seguridad de la Información del Ayuntamiento de Málaga se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán los siguientes instrumentos:

- Normas técnicas de seguridad: Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- Guías de seguridad: Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos. Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.
- Procedimientos operativos de seguridad (POS): Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.
- Instrucciones técnicas (IT): Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas.

La normativa técnica de seguridad estará disponible en la intranet municipal a disposición de todos los miembros de la organización municipal que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

10.2 APROBACIÓN DE LAS NORMAS DE SEGURIDAD

En toda la organización municipal, la aprobación de las normas técnicas de seguridad se hará de acuerdo a lo dispuesto en la presente política, a excepción de la Empresa Malagueña de Transportes (EMTSAM) y de la Empresa Municipal de Aguas de Málaga (EMASA), cuyos respectivos Consejos de Administración serán quienes ejerzan las competencias de desarrollo y aprobación del marco normativo que implante la presente política de seguridad en sus correspondientes ámbitos competenciales.

10.3 SANCIONES PREVISTAS POR INCUMPLIMIENTO

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la normativa sobre régimen disciplinario de los empleados públicos, así como, en su caso, a lo prevenido en el Acuerdo de Funcionarios y Convenio Colectivo vigentes en cada momento.

11 SEGURIDAD DE LA INFORMACIÓN

Se desarrollará una Clasificación de la Información del Ayuntamiento de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu

Dicha clasificación será aprobada por el Presidente del Comité MSI, a propuesta del gerente del CEMI.

12 DATOS DE CARÁCTER PERSONAL

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento municipal se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Las medidas de protección de los datos de carácter personal se establecerán a partir de los resultados del Análisis de Riesgos y de la Evaluación de Impacto prevista en el Reglamento General de Protección de Datos y LOPDGDD.

Todos los sistemas de información del Ayuntamiento de Málaga se ajustarán a los niveles de seguridad requeridos por esta normativa.

13 OBLIGACIONES DEL PERSONAL

Todos los miembros de la organización municipal y las empresas y personas terceras que realicen servicios de cualquier clase contratados por el Ayuntamiento de Málaga o que de alguna manera se presten bajo el control y/o la dirección del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, que será trasladada a través de los Departamentos Municipales quienes deberán disponer los medios necesarios para que ésta llegue a los afectados.

Se establecerá un programa de concienciación continua dirigido a todos los miembros del Ayuntamiento de Málaga, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

14 TERCERAS PARTES

Cuando el Ayuntamiento de Málaga 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 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 Málaga utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar 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.

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 de la Información 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, así como del responsable del tratamiento previsto en el RGPD y LOPDGDD, antes de seguir adelante.

C/ Concejal Muñoz Cerván, 3, Edificio 4 ■ 29003 ■ Málaga ■ 951 92 60 50 ■ CIF P-2900011-D ■ www.malaga.eu