IV. Administración Local

Cartagena

2238 Aprobación definitiva del Reglamento de Política de Seguridad de la Información en el Excmo. Ayuntamiento de Cartagena.

Visto que con fecha de 24 de noviembre de 2016 se acordó, por el Excmo. Ayuntamiento Pleno, la aprobación inicial del "Reglamento que regula la Política de Seguridad de la Información del Excmo. Ayuntamiento de Cartagena" y que con fecha de 9 de enero de 2017, se publicó Edicto en el BORM en el que se anunciaba el trámite de información pública por plazo de treinta días del citado Reglamento, sin que se hubiesen presentado alegaciones, es por lo que, habiendo transcurrido el plazo establecido al efecto, de conformidad con lo dispuesto en el artículo 49 de la Ley 7/1985, de 2 de abril, de Bases de Régimen Local, por medio del presente, se acompaña el texto íntegro del "Reglamento que regula la Política de Seguridad de la Información del Excmo. Ayuntamiento de Cartagena", para su entrada en vigor de conformidad con los plazos establecidos en los artículos 70.2 y 65.2 de la citada Ley 7/1985, de 2 de abril, entendiéndose definitivamente adoptado el acuerdo de aprobación hasta entonces provisional.

Cartagena, 21 de febrero de 2017.—El Concejal Delegado del Área de Hacienda e Interior, Francisco Aznar García.

REGLAMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL EXCELENTÍSIMO AYUNTAMIENTO DE CARTAGENA

Exposición de motivos

Mediante el presente "Reglamento de Política de Seguridad de la Información", el Excmo. Ayuntamiento de Cartagena se dota de un marco de gestión de la seguridad de la información, 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, anticipándose a sus necesidades, y preservando sus derechos.

El presente "Reglamento de 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 Cartagena.

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 Excmo. Ayuntamiento de Cartagena, que se concretan en lo dispuesto en el artículo 6 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, es decir, el servir con objetividad

los intereses públicos que les están encomendados y actuar de acuerdo con los principios de eficacia, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al derecho.

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.

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 Cartagena 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.

El presente "Reglamento de Política de Seguridad de la Información" asegura un compromiso manifiesto de las máximas autoridades del Ayuntamiento de Cartagena, para la difusión, consolidación y cumplimiento del mismo.

En este contexto, el presente Reglamento viene informado por lo preceptuado en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, reforzado por artículo 156 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, que insiste en la necesidad de su cumplimiento.

Del mismo modo, el presente "Reglamento de Política de Seguridad de la Información" es coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

En este sentido, se ha tomado en consideración, en lo que procede, el 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).

Por último, la redacción del presente "Reglamento de Política de Seguridad de la Información" viene informado por las Políticas de Seguridad de la Información promulgadas por otras administraciones, habiendo servido como base del mismo con carácter general la Política codificada por el Ministerio de Hacienda y Administraciones Públicas y, con un mayor enfoque hacia la Administración Municipal, las aprobadas por otros Ayuntamientos.

Por tanto, en virtud de lo previsto en la citada normativa, y haciendo uso de la potestad de autorregulación de la Administración Municipal, se promulga el presente Reglamento de Política de Seguridad de la Información.

Artículo 1. Objeto y ámbito de aplicación

1. Constituye el objeto del presente "Reglamento de Política de Seguridad de la Información", en adelante RPSI, la articulación de las condiciones generales de seguridad en el ámbito del Ayuntamiento de Cartagena, así como del marco organizativo y tecnológico de la misma, con el fin de sentar las bases para establecer los mecanismos normativos y procedimentales necesarios para hacer de la gestión de la seguridad una actividad continuada, al mismo nivel que las demás actividades que constituyen el normal funcionamiento del Ayuntamiento, y como base para una ejecución fiable de éstas, tanto a nivel interno como para la ciudadanía.

2. El RPSI será de obligado cumplimiento para todos los órganos administrativos del Ayuntamiento de Cartagena, cualesquiera organismos públicos y entidades de derecho público vinculados al mismo o dependientes de él y las entidades de derecho privado vinculadas a éste o dependientes del mismo, que quedarán sujetas a lo dispuesto en las normas del RPSI que específicamente se refieran a ellas, y, en todo caso, cuando ejerzan potestades administrativas, siendo aplicable a los activos empleados por el Ayuntamiento en la prestación de los servicios de la Administración Electrónica.

3. El RPSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Ayuntamiento y sus entidades vinculadas o dependientes, con independencia de cuál sea su destino, adscripción o relación con el mismo.

Artículo 2. Marco legal y regulador.

El marco normativo en que se desarrollan las actividades del Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

a) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica.

b) Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

c) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

d) Ley Orgánica 15/1999 de diciembre, de 13 de diciembre, de Protección de Datos de Carácter Personal.

e) 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.

f) Ley 59/2003, de 19 de diciembre, de firma electrónica.

g) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

h) Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

i) 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).

Del mismo modo, forman parte del marco regulador las normas aplicables a la Administración Electrónica del Ayuntamiento de Cartagena que desarrollen o complementen las anteriores en el uso de su potestad de autorregulación y que se encuentren dentro del ámbito de aplicación del la RPSI, tal y como se definen en el artículo 13 del mismo; así como la normativa comunitaria en la materia.

Artículo 3. Principios de la seguridad de la información.

1. Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles con capacidad de toma de decisiones, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Ayuntamiento para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará el Responsable de la Información, que propone los requisitos de seguridad de la información tratada; el o los Responsables del Servicio, que cumplen y hacen cumplir los requisitos de seguridad en los sistemas y servicios de su competencia; el o los Responsables del Sistema, que tienen la responsabilidad sobre la seguridad física y lógica y la prestación de los servicios en los ámbitos de competencia que se determinan en el presente RPSI; y el Responsable de Seguridad, que determina, las decisiones para satisfacer los requisitos de seguridad. El Comité de Dirección de Seguridad de la Información sirve de vínculo entre todos ellos, con las funciones que se codifican en el presente RPSI.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

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

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado, con la periodicidad que determine el Comité de Dirección de Seguridad de la Información (en adelante CDSI).

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto, atendiendo a lo preceptuado en el Esquema Nacional de Seguridad (en adelante ENS).

2. Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos del RPSI y que inspiran las actuaciones del Ayuntamiento de Cartagena en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal, de manera coherente con el Documento de Seguridad exigido por el artículo 88 del 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.

b) Gestión de activos de información: Los activos de información del Ayuntamiento se encontrarán inventariados y categorizados y estarán asociados al menos a un responsable técnico.

c) Seguridad ligada a las personas: se implantarán los 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: 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. En el supuesto de hacer uso de sistemas o servicios en modalidad Cloud, deberá existir un acuerdo de nivel de servicio (SLA) que establezca idéntico grado de seguridad física y atienda a las recomendaciones del Centro Criptológico Nacional en sus Guías CCN-STIC.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y de las comunicaciones. 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. Las técnicas de cifrado o encriptación deben ser lo suficientemente fiables como para garantizar la seguridad en las comunicaciones y operaciones, pero en modo alguno comprometer la usabilidad futura de los activos de información.

f) Control de acceso: se limitará 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. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad del Ayuntamiento.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. Para ello se estará a lo dispuesto en la restante normativa municipal reguladora de todos los aspectos asociados a la Administración Electrónica, y en particular a lo previsto en la "Ordenanza Municipal de Administración Electrónica" y sus Reglamentos de desarrollo.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. En todo caso, se proporcionará información a, y se atenderán las recomendaciones de, los Sistemas de Alerta Temprana del Centro Criptológico Nacional.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos del Ayuntamiento y sus entidades vinculadas o dependientes, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Artículo 4. Estructura organizativa.

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por el RPSI del Ayuntamiento de Cartagena y de sus entidades vinculadas o dependientes está compuesta por los siguientes agentes:

a) el Comité de Dirección de Seguridad de la Información,

b) el Director Técnico,

c) el Responsable de Seguridad,

d) el Responsable de la Información,

e) los Responsables de los Servicios y

f) los Responsables de los Sistemas.

Artículo 5. El Comité de Dirección de Seguridad de la Información.

1. Se crea el Comité de Dirección de Seguridad de la Información, compuesto por los siguientes miembros:

a) Presidente: El Alcalde, o Concejal Delegado de Interior, con competencias en tecnologías de la información y de las comunicaciones, o quien tenga delegadas tales competencias.

b) Director Técnico: con las competencias que la presente PSI le atribuye.

c) Vocales:

a. El Responsable de Seguridad.

b. Hasta un máximo de tres técnicos informáticos de los servicios y sistemas de información en uso en el Ayuntamiento y sus entidades vinculadas o dependientes.

c. Un Técnico competente para proponer medidas de impulso de la Administración Electrónica en el ámbito del Ayuntamiento.

d. Un Técnico en Administración Electrónica.

e. Un Letrado Municipal o Técnico de Administración General, que actuará como Secretario del Comité.

2.- Los vocales del CDSI y el Director Técnico serán nombrados por el Presidente del CDSI.

3.- El CDSI ejercerá las siguientes funciones:

a) Emitir propuestas de modificación y actualización permanente que se hagan sobre el presente RPSI.

b) Emitir propuestas acerca del resto de la normativa de seguridad de primer nivel definida en el artículo 11 del presente Reglamento.

c) Velar e impulsar el cumplimiento del RPSI y de su desarrollo normativo.

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

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

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

g) Impulsar la formación y concienciación en materia de seguridad de la información, en cooperación con la Unidad de Formación del Ayuntamiento de Cartagena.

h) Revisar el RPSI y las responsabilidades principales.

i) Difundir en el Ayuntamiento de Cartagena las normas y procedimientos derivados del RPSI y normativa de desarrollo, así como las funciones y obligaciones de todo el Ayuntamiento de Cartagena en materia de seguridad de la información.

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

k) Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.

4.- El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente y en el supuesto de incidente de seguridad con carácter de urgencia.

5.- El CDSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 6. El Director Técnico.

1. El Director Técnico es la persona que controla y supervisa el cumplimiento de las obligaciones impuestas por el presente RPSI, y normativa de aplicación, por parte del CDSI, y actúa como representante e interlocutor del mismo ante los órganos superiores. De igual modo, el Director Técnico coordina el funcionamiento del CDSI, así como de los responsables previstos en los apartados c), d), e) y f) del artículo 4 del presente RPSI.

2. Serán funciones del Director Técnico:

a) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa, resultando suficiente la mayoría, no la unanimidad, en caso de discrepancia.

b) Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.

c) Impulsar la estrategia de seguridad de la información definida por el CDSI

d) Supervisar las normas y procedimientos contenidos en el RPSI y normativa de desarrollo.

e) Supervisar y colaborar en las auditorías internas o externas necesarias para verificar el grado de cumplimiento del RPSI, normativa de desarrollo y leyes aplicables.

f) Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

g) Analizar y elevar al CDSI toda la documentación relacionada con la seguridad de los sistemas de información.

h) Poner en conocimiento del CDSI los informes emitidos por los responsables identificados en el presente RPSI.

Artículo 7. El Responsable de Seguridad.

1. El Responsable de Seguridad es la persona que propone al CDSI las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios del Ayuntamiento. En este sentido, propondrá al CDSI las medidas técnicas adecuadas para que la comunicación entre éste y sus demás miembros sea fluida e inmediata.

2. El Responsable de Seguridad será nombrado por el Presidente del CDSI.

3. El ámbito de actuación del Responsable de Seguridad abarcará todos los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del Ayuntamiento de Cartagena y de sus entidades vinculadas o dependientes, conforme al ámbito de aplicación del presente RPSI.

4. Serán funciones del Responsable de Seguridad, con la cooperación del CDSI, las siguientes:

a) Elaborar la normativa de seguridad de segundo y tercer nivel definida en la presente PSI, a proponer por el CDSI para su aprobación.

b) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

c) Desarrollar e implantar los controles y medidas destinados a garantizar la seguridad de los activos de información del Ayuntamiento y sus entidades vinculadas y dependientes.

d) Supervisar y realizar el seguimiento de aspectos tales como: principales incidencias en la seguridad de la información; elaboración y actualización de planes de continuidad; cumplimiento y difusión del RPSI.

e) Coordinar y controlar las medidas de seguridad de la información y de protección de datos del Ayuntamiento de Cartagena.

f) Supervisar los incidentes de seguridad producidos en el Ayuntamiento y sus entidades vinculadas o dependientes.

g) Seleccionar y establecer las funciones y obligaciones de los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos del Ayuntamiento de Cartagena, conforme a la estrategia de seguridad definida.

h) Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.

i) Garantizar la actualización del inventario de activos de los sistemas de información del Ayuntamiento de Cartagena.

j) Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.

k) Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en el Ayuntamiento de Cartagena.

l) Establecer los procesos y controles de supervisión del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.

m) Aplicar los procedimientos operativos de Seguridad.

n) Aprobar los cambios en la configuración vigente del Sistema de Información.

o) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

p) Elaborar informes periódicos de seguridad para el Director Técnico, que incluirán los incidentes más relevantes de cada periodo.

q) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos en colaboración con el Responsable de la Información y los Responsables de los Sistemas.

Artículo 8. El Responsable de la Información.

1. El Responsable de la Información será nombrado por el Presidente del CDSI.

2. El Responsable de la Información puede coincidir o no con el Responsable de Seguridad.

3. Son funciones del Responsable de la Información, en colaboración con el CDSI y, en el ámbito pertinente de competencias, con los Servicios del Ayuntamiento y de sus entidades vinculadas o dependientes:

a) Supervisar y controlar los cambios significativos en la exposición de los activos de información a las amenazas principales.

b) Asesorar en materia de seguridad de la información a las diferentes áreas operativas del Ayuntamiento de Cartagena.

c) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas.

d) Realizar auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

e) Velar por el buen uso de la información y, por tanto, de su protección.

f) Supervisar cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

g) Establecer los requisitos de la información en materia de seguridad.

h) Determinar los niveles de seguridad de la información.

i) Desarrollar, operar y mantener el sistema lógico y físico de información durante todo su ciclo de vida, de los sistemas de información existentes en el Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes.

Artículo 9. Los Responsables de los Servicios.

En el ámbito de sus competencias, los diferentes Jefes de Servicio del Ayuntamiento de Cartagena así como de sus organismos públicos dependientes y/o de aquellas entidades a las que le son aplicables el ámbito de actuación del presente Reglamento, adquieren la condición de Responsables del Servicio, con las obligaciones que se enuncian en lo que sigue:

a) Dentro de su ámbito de actuación y de sus competencias, cumplir y hacer cumplir los requisitos, en materia de seguridad, de los servicios, los sistemas y la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

b) Colaborar con el CDSI en la identificación de la información y los servicios existentes en su ámbito de actuación, con el objeto de determinar los niveles de criticidad de los mismos y definir las medidas de seguridad adecuadas a ellos, atendiendo al principio de proporcionalidad.

c) Si procede, designar, dentro de su ámbito de actuación y de acuerdo con la organización interna del servicio, a la persona o las personas que asumirán la responsabilidad de la aplicación cotidiana de las medidas de seguridad, sin menoscabo de la responsabilidad última del Jefe de Servicio, que en ningún caso queda exento de las obligaciones establecidas en la presente PSI.

Artículo 10. Los Responsables de los Sistemas.

1. Los Responsables de los Sistemas son las personas cuya obligación es desarrollar, operar y mantener el sistema lógico y físico de información durante todo su ciclo de vida, en cada uno de los sistemas de información existentes en el Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes.

2. En el ámbito de los sistemas de información de los que son responsables, los Responsables de los Sistemas podrán delegar las actividades de seguridad física o lógica en otro técnico instruido y cualificado en sistemas de información, sin que esto implique la delegación de la responsabilidad última de aquéllos.

3. Cada uno de los sistemas de información del Ayuntamiento y sus entidades vinculadas o dependientes a los que les sea de aplicación el presente RPSI, designará estos perfiles de acuerdo con su propia organización interna.

4. Serán funciones de los Responsables de los Sistemas:

a) Garantizar la correcta implantación de Sistemas de Climatización, Sistemas Anti-incendios, Cableado estructurado, Energía y suministro eléctrico, Cámaras de vigilancia, Controles de acceso físico a locales y CPD´S, Medidas de Seguridad en Ficheros.

b) Implantar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.

c) Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.

d) Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la supervisión de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

e) Asegurar que los controles de seguridad establecidos se cumplen estrictamente.

f) Asegurar que se aplican los procedimientos aprobados para manejar el sistema de información.

g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

h) Supervisar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

i) Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Artículo 11. Grupos de trabajo.

El CDSI podrá articular la creación de grupos de trabajo para la realización de actividades tales como estudios, trabajos e informes, que se estimen convenientes.

Artículo 12. Gestión de los riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados.

2. El CDSI se encargará de adoptar las medidas oportunas para analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.

3. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional, así como metodologías reconocidas en uso a nivel nacional e internacional.

Artículo 13. Estructura normativa.

1.- El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel normativo: constituido por el presente RPSI y las directrices generales de seguridad aplicables a los órganos del Ayuntamiento y a sus entidades vinculadas o dependientes a los que sea de aplicación el presente RPSI.

b) Segundo nivel normativo: constituido por las normas de seguridad desarrolladas por el Responsable de Seguridad. Estas normas de seguridad deberán:

1.-Limitarse única y exclusivamente al ámbito específico de las competencias del Ayuntamiento y de sus entidades vinculadas o dependientes. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por cada órgano o entidad vinculada o dependiente.

2.- Cumplir estrictamente con lo indicado en el ENS y con el primer nivel normativo enunciado en el presente artículo.

3.- Ser informadas por el CDSI y aprobadas mediante acuerdo de la Junta de Gobierno Local.

c) Tercer nivel normativo: Procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en el RPSI, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel normativo deberá:

1.- Limitarse única y exclusivamente al ámbito específico de las competencias del Ayuntamiento y de sus entidades vinculadas o dependientes. Este ámbito

vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por cada órgano o entidad vinculada o dependiente.

2.- Cumplir estrictamente con lo indicado en el ENS y con el primer y segundo nivel normativos enunciados en el presente artículo.

3.- Ser informado por el CDSI y aprobado mediante acuerdo de la Junta de Gobierno Local.

2.- Además de la normativa enunciada en el presente artículo, la estructura normativa podrá disponer, a criterio de los órganos competentes del Ayuntamiento, y siempre dentro del ámbito de sus competencias y responsabilidades, otros documentos normativos, en virtud de la potestad autorreguladora de la Administración Municipal, y previo informe del CDSI y aprobación mediante acuerdo de la Junta de Gobierno Local. En cualquier caso, siempre habrá de disponerse, de conformidad con lo previsto en el artículo 88 del 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, de Documento de Seguridad permanentemente actualizado.

3.- Ateniéndose a lo previsto en el ENS y a las Guías CCN-STIC del Centro Criptológico Nacional que lo desarrollan, el CDSI determinará las normas de distinto nivel a ser aprobadas y el orden y prioridad de las mismas.

4.- El personal de cada uno de los órganos del Ayuntamiento y sus entidades vinculadas o dependientes tendrá la obligación de conocer y cumplir, además del presente RPSI, y a los niveles en que resulte de su responsabilidad, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

Artículo 14. Protección de datos de carácter personal.

Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ayuntamiento y sus entidades vinculadas o dependientes las medidas de seguridad determinadas en las siguientes normativas:

a) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

b) 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.

c) Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

d) En lo que proceda, el 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).

Artículo 15. Formación y concienciación.

1. El Director Técnico desarrollará un plan anual de actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Ayuntamiento y de sus entidades vinculadas y dependientes, así como a la difusión entre los mismos del RPSI y de su desarrollo normativo.

2. El Director Técnico, en cooperación con la Unidad de Formación del Ayuntamiento, se encargará de promover las actividades de formación y concienciación en materia de seguridad.

Artículo 16.- Terceros.

Cuando el Ayuntamiento de Cartagena utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité de Dirección 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 Cartagena 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.

Disposición adicional única. Deber de colaboración en la implantación del RPSI.

Todos los órganos y unidades del Ayuntamiento y sus entidades vinculadas o dependientes prestarán su colaboración en las actuaciones de implantación del RPSI.

Disposición final única. Modificación y publicidad del RPSI y entrada en vigor

1. El presente RPSI será objeto de aprobación y publicación de acuerdo con los trámites legales oportunos.

2. El presente RPSI se publicará en la sede electrónica del Ayuntamiento y en su portal de transparencia.

3.- El presente RPSI entrará en vigor en el plazo establecido en el artículo 70.2 y 65 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, a partir de su publicación en el Boletín Oficial.

Segundo: Conceder un trámite de información pública por plazo de treinta días para la presentación de reclamaciones y sugerencias, entendiendo que en caso de que no se presenten alegaciones al Reglamento de Política de Seguridad de la Información del Excmo. Ayuntamiento de Cartagena, se considerará definitivamente aprobado.