D. ILDEFONSO COBO NAVARRETE, SECRETARIO GENERAL DEL EXCMO. AYUNTAMIENTO DE GRANADA.

CERTIFICO: Que el Excmo. Ayuntamiento Pleno, en su Sesión Ordinaria celebrada el día **veintitrés de febrero de dos mil veinticuatro**, entre otros acuerdos, adoptó el que con el núm. 63**,** literalmente dice:

Normativa de Seguridad denominada: Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada. (Expte 845/2023). Aprobación de la modificación.

Se presenta a Pleno expediente núm. 845/2023 de la Direccción Técnica de Ciberseguridad de la Concejalía Delegada de Recursos Humanos, Organización, Ciudad Inteligente, Digitalización e Innovación relativo a aprobación de modificación de la Normativa de Seguridad denominada: Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada, en el que consta informe emitido por la Directora General de Ciudad Inteligente, Digitalización e Innovación, de fecha 22 de enero de 2024, relativo a la necesidad de aprobación de la modificación de la Normativa de Seguridad denominada "Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada"; así como propuesta del Sr. Tte. de Alcalde Delegado de Recursos Humanos, Organización, Ciudad Inteligente, Digitalización e Innovación, de fecha 22 de enero de 2.024.

Se producen las siguientes intervenciones:
.....

Tras ello, se somete el expediente a votación obteniéndose el voto favorable de la unanimidad de miembros de la Corporación.

En consecuencia, aceptando dictamen de la Comisión Municipal de Economía y Hacienda, Recursos Humanos, Innovación y Comercio, de fecha 13 de febrero de 2.024, el Ayuntamiento Pleno, de acuerdo con propuesta del Tte. de Alcalde Delegado de Recursos Humanos, Organización, Ciudad Inteligente, Digitalización e Innovación, **acuerda** por unanimidad **aprobar** la modificación de la Normativa de Seguridad denominada "Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada" conforme al texto que se reproduce literalmente a continuación:

POLÍTICA DE CIBERSEGURIDAD Y DE PROTECCIÓN DE DATOS DEL AYUNTAMIENTO DE GRANADA

CAPÍTULO I.
Objeto y Principios Generales

POLÍTICA DE CIBERSEGURIDAD Y DE PROTECCIÓN DE DATOS DEL AYUNTAMIENTO DE GRANADA

El marco de relación entre la Administración Pública y la ciudadanía a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas el cual establece, en su artículo 13, el derecho de los ciudadanos a la protección y confidencialidad de sus datos y a la seguridad de los mismos cuando figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

En el mismo sentido, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, determina, en su artículo 156, que la política de seguridad en la utilización de medios electrónicos se realizará de acuerdo con las prescripciones establecidas en el Esquema Nacional de Seguridad, en el que se determinan los principios básicos y requisitos mínimos que han de garantizar la seguridad de la información tratada.

Ambas normas han sido objeto de desarrollo en virtud del 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.

La Administración Digital debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes con total seguridad y fiabilidad.

El Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica tenía como finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitieran a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. El ENS ha sido actualizado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, con la finalidad explícita de cumplir tres grandes objetivos: para alinear el ENS con el marco normativo y el contexto estratégico actual para garantizar la seguridad en la administración digital; para introducir el concepto de «perfil de cumplimiento específico» que permita a ciertos colectivos y tipos de sistemas alcanzar una adaptación del ENS más eficaz y eficiente y, en tercer lugar, para facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

El Esquema Nacional de Seguridad exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en la propia norma y desarrollará una serie de requisitos mínimos.

La creciente exposición digital amplía la superficie de exposición a ciberataques de ciudadanos, empresas y administraciones. Entre las dinámicas que marcan un mayor uso de las redes digitales se encuentra el aumento del teletrabajo, la irrupción de IoT y el despliegue de una mayor conectividad como las redes 5G. Consecuentemente, se está generando un aumento de la vulnerabilidad ante ciberataques en aparatos conectados a la red y servicios digitales. La prevención y la adaptación serán las claves para paliar estas vulnerabilidades mediante el impulso de una mayor anticipación, integración de recursos y un fortalecimiento de la resiliencia como indica la Estrategia de Seguridad Nacional 2021.

La Estrategia de Ciberseguridad de la Unión Europea presentada por la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, en diciembre de 2020, tiene como finalidad reforzar la resiliencia colectiva europea contra las ciberamenazas y ayudar a garantizar que todos los ciudadanos y las empresas puedan beneficiarse plenamente de unos servicios y herramientas digitales fiables y de confianza, correspondiendo a las Administraciones Públicas un papel destacado en la custodia de un ciberespacio libre y seguro.

Asimismo, 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, pretende sentar las bases de una normativa de privacidad que se adecue a la nueva realidad tecnológica y social, dando un paso más en la defensa de los derechos de los ciudadanos, en lo que hace referencia a su privacidad.

Por otra parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos en su artículo 1, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679, antes mencionado, completando sus disposiciones y garantizando los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución. De igual modo, la disposición adicional primera de esta ley orgánica establece que en los tratamientos de datos personales realizados en el ámbito del sector público se deben aplicar las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

La política de seguridad constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS.

Del mismo modo, determina que la política de seguridad debe ser coherente con lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos) y la normativa vigente en esta materia, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

En consonancia con esa previsión se aprobó la Política de Seguridad de la Información del Ayuntamiento de Granada en el marco del Esquema Nacional de Seguridad por la Junta de Gobierno Local el día treinta y uno de marzo de dos mil diecisiete. Esta política tiene que ser objeto de una revisión periódica. Esta necesidad de revisión se justifica aún más por el periodo de tiempo transcurrido desde su aprobación, por los cambios normativos que se han producido y por los cambios habidos en las distintas estructuras orgánicas del Ayuntamiento de Granada.

Por tanto, visto que es necesario adaptar las políticas de seguridad de la información y de protección de datos a la legislación vigente y a la realidad actual, y dado que están íntimamente ligadas, se considera conveniente aprobar una norma que las regule de manera conjunta y en la que se establezcan claramente las funciones, actividades y responsabilidades implicadas.

El contenido de esta Política cumple con el principio de seguridad jurídica, al ser coherente con el resto del ordenamiento jurídico autonómico, nacional y de la Unión Europea, generando un marco regulatorio que define el ámbito de aplicación, el marco organizativo y los instrumentos para desarrollar su contenido. La Política define también las medidas a adoptar y las funciones atribuidas a cada órgano competente en materia de ciberseguridad y de protección de datos personales, facilitando su actuación y la toma de decisiones.

La experiencia acumulada en la gestión de las materias indicadas, las referidas modificaciones normativas y los cambios organizativos habidos en estos sectores de la actividad administrativa hacen necesaria la presente norma para configurar una Política de Ciberseguridad y Protección de Datos Personales acorde con el momento actual.

La Política de Ciberseguridad y Protección de Datos define el marco de referencia que permite la gestión de la seguridad de la información en los sistemas del Ayuntamiento de Granada y la gestión de los datos personales, estableciendo el conjunto de directrices que rigen la forma en que nuestra organización gestiona y protege la información que trata y los servicios que presta. Seguridad y gestión entendidas como un proceso integral que incluye todos los elementos técnicos, humanos, materiales y organizativos de los diferentes sistemas de información.

CAPÍTULO I.
Objeto y Principios Generales

1. Objeto y ámbito de aplicación.

Es objeto de esta Política de Ciberseguridad y Protección de Datos establecer el marco común, las directrices básicas y el régimen organizativo para la gestión integral de la Seguridad de la Información y la organización competencial para la Protección de Datos Personales, garantizando el cumplimiento de la normativa vigente en ambas materias, contribuyendo así a la misión del Ayuntamiento de Granada, así como la creación del Comité General de Ciberseguridad y el Comité Técnico de Ciberseguridad del Ayuntamiento de Granada.

La Política de Ciberseguridad y Protección de Datos se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable el Ayuntamiento de Granada, organismos autónomos, sociedades mercantiles locales, fundaciones públicas locales y demás entidades del sector público institucional del Ayuntamiento de Granada. A tales efectos, los organismos autónomos y demás entes instrumentales deberán adherirse previamente a esta Política mediante la firma del correspondiente convenio.

Esta Política de Ciberseguridad y Protección de datos es de aplicación y de obligado cumplimiento para todo el personal del Ayuntamiento de Granada y de las entidades comprendidas en el alcance de esta Política, con independencia de cuál sea su destino, adscripción o relación con el mismo, incluyendo todas sus Concejalías, áreas de gobierno, grupos municipales, departamentos y órganos internos, así como para todos cuantos, con independencia de su condición funcionarial o laboral, personal propio o ajeno, estudiantes, becarios o en prácticas, tengan acceso a la información o a los datos personales de los que es responsable o encargado del tratamiento el Ayuntamiento de Granada. Así mismo, esta Política de Ciberseguridad y Protección de datos es de aplicación y obligado cumplimiento en todos los sistemas de información, servicios, información y procesos del Ayuntamiento de Granada.

2. Definiciones.

Las expresiones y términos utilizados en el presente decreto tendrán el significado indicado en el glosario de términos incluido en el Esquema Nacional de Seguridad vigente en el ámbito de la Administración electrónica, así como en las definiciones del artículo 4 del 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.

3. Misión del Ayuntamiento

El Ayuntamiento de Granada, para la gestión de sus intereses, y en el ámbito de sus competencias, sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población del municipio de Granada, todo ello bajo los preceptos de los diversos marcos normativos que le afectan.

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

4. Objetivos y misión de la Política de Ciberseguridad y Protección de Datos.

El Ayuntamiento de Granada ha establecido un marco de gestión de la seguridad de la información según lo establecido en el Esquema Nacional de Seguridad 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 la ciudadanía puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada protege a la información municipal 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 Granada.

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:

a) Contribuir desde la gestión de la ciberseguridad y la protección de datos a cumplir con la misión y objetivos establecidos por el Ayuntamiento de Granada.

b) 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, sobre la base de procesos de análisis de riesgos.

c) 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.

d) Proteger los recursos de información y servicios del Ayuntamiento de Granada y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales.

Todo ello, con el objetivo superior de implementar en los sistemas de información, procesos y servicios municipales la mejor adecuación a las medidas de seguridad que apliquen y contemple el ENS vigente y permita la Certificación de Conformidad con el ENS del Ayuntamiento de Granada.

5. Marco regulatorio.

El marco legal, con carácter general en materia de seguridad de la información, viene establecido por la siguiente legislación:

a) Serán de aplicación a la Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada las disposiciones en materia de seguridad de la información y protección de datos de carácter personal contenidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; en el 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; en la 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; Real Decreto Ley 12/2018, de 8 se septiembre, de Seguridad de las redes y sistemas de información que transpone la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión así como el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018.

b) El Esquema Nacional de Seguridad vigente que fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración y su normativa derivada.

c) Al tratamiento de la información que contenga datos de carácter personal le será aplicable el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

d) Ordenanza de Administración Electrónica del Ayuntamiento de Granada (BOP núm.247, de fecha 29 de diciembre de 2009), Decreto de 1 de septiembre de 2010 del Delegado del Área de Gobierno de Hacienda y Administración Pública por el que se crean la Sede Electrónica y el Registro Electrónico del Ayuntamiento de Granada y Normas aplicables a la Administración Electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Ciberseguridad.

e) Resultarán igualmente aplicables las normas jurídicas que regulen aspectos relacionados con el tratamiento de la información, tales como las que tengan por objeto la ciberseguridad, administración electrónica, el patrimonio documental o la información protegida, entre otras.

f) Asimismo, formarán parte del marco regulatorio de la Política de Ciberseguridad y de Protección de Datos del Ayuntamiento de Granada todos los instrumentos regulados en el Capítulo III.

6. Principios de la Política de Ciberseguridad y Protección de Datos.

Toda la actividad relacionada con el uso de los activos de información y el tratamiento de datos personales en el Ayuntamiento de Granada se regirá por los siguientes principios:

a) Alcance estratégico: La Política de Ciberseguridad y Protección de Datos contará con el compromiso de todos los niveles directivos de modo que la seguridad de la información y la protección de datos estén integradas y coordinadas con las decisiones estratégicas del Ayuntamiento de Granada.

b) Seguridad integral: La seguridad se entenderá como un proceso integral y planificado, constituido por todos los elementos técnicos, humanos, materiales, procedimentales y organizativos relacionados con los sistemas de información, evitando las actuaciones puntuales o tratamientos coyunturales.

c) Gestión de la seguridad basada en los riesgos: El análisis y la gestión de los riesgos serán parte esencial y permanente del proceso de seguridad. Mediante el análisis de riesgos se detectan los problemas de seguridad y con su correcta gestión se persigue reducirlos a un nivel aceptable mediante la selección e implantación de medidas de seguridad.

d) Prevención, detección, respuesta y conservación: La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección, respuesta y conservación, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o los servicios que presta.

e) Existencia de líneas de defensa: Los sistemas de información dispondrán de una estrategia de protección constituida por múltiples capas de seguridad dispuesta de forma que, cuando una de las capas sea comprometida, permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

f) Vigilancia continua: La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

g) Reevaluación periódica: La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

h) Diferenciación de responsabilidades: En los sistemas de información se diferenciarán el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

i) Ciclo completo y seguridad por defecto: Se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. La seguridad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

j) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación será proporcional, en sus costes económicos y operativos, a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

k) Responsabilidad proactiva: El responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de la información se hace conforme a la normativa española y europea en la materia.

l) Legitimación en el tratamiento de datos personales: Sólo se tratarán los datos de carácter personal cuando dicho tratamiento esté legitimado en alguna de las causas previstas en el Reglamento (UE) 2016/679.

m) Licitud, lealtad y transparencia: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

n) Limitación de la finalidad: Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

o) Minimización de datos: Los datos tratados serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que sean tratados.

p) Integridad y calidad: Se garantizará el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y, en su caso, actualización.

q) Limitación del plazo de conservación: Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que pudieran derivarse de su tratamiento.

Los datos podrán conservarse durante periodos más largos cuando sean tratados exclusivamente con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos de acuerdo con lo establecido en el Reglamento (UE) 2016/679. El tratamiento para estos fines se realizará con las medidas técnicas y organizativas adecuadas, respetando particularmente el principio de minimización de los datos personales, así como, cuando sea posible, su anonimización. En esta modalidad de tratamiento será a su vez de aplicación lo dispuesto en la normativa sobre archivos y documentación.

r) Confidencialidad: Quienes intervengan en el tratamiento estarán obligados a guardar el deber de secreto, incluso después de haber finalizado el proceso de tratamiento.

s) Profesionalidad: La seguridad de los sistemas de información estará implantada, atendida, revisada y auditada por personal cualificado y formado, que participará en todas las fases del ciclo de vida de los sistemas.

t) Prevención, disponibilidad y recuperación: Se desarrollarán planes de acción y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. Se asegurará el nivel de disponibilidad requerido para los activos y recuperación ante cualquier contingencia.

7. Requisitos mínimos y Directrices.

Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de ciberseguridad y protección de datos personales. La Política de Ciberseguridad y Protección de Datos se establecerá de acuerdo con los principios básicos señalados y se desarrollará aplicando los siguientes requisitos mínimos y directrices:

a) Protección de las instalaciones: Los activos de información se emplazarán en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad. Los sistemas y los activos de información ubicados en dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

b) Autorizaciones y controles de acceso: El acceso a la información estará debidamente controlado y limitado a las personas usuarias, procesos, dispositivos u otros sistemas de información autorizados, y exclusivamente a las funciones permitidas. A tal fin se implantarán los mecanismos de identificación y autenticación adecuados para cada activo.

c) Gestión de activos de información: Los activos de información se inventariarán y categorizarán. Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

d) Autorización de sistemas y soluciones: Se deberá autorizar los sistemas y soluciones antes de entrar en operación. Se controlará y limitará los accesos a los sistemas de información. Se configurará y diseñará los sistemas de información de forma que se garantice la seguridad y protección de datos por defecto

e) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que, debidamente autorizada, acceda a los activos de información conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

f) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

g) Registro de actividad: La actividad realizada por las personas usuarias de sistemas de información deberá ser registrada al objeto de verificar y auditar el buen uso de la información, siempre con plenas garantías a la intimidad y dignidad personal, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

La monitorización deberá realizarse motivando su necesidad y aplicando el principio de proporcionalidad, eligiendo la medida menos invasiva. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

h) Gestión de incidentes de seguridad: Los procedimientos de gestión permitirán identificar, registrar y dar una efectiva y pronta respuesta a los incidentes de seguridad, comunicando los procedentes a la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

i) Protección de las comunicaciones: La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, sin perjuicio de las actuaciones realizadas con fines de registro de actividad.

j) Especificaciones de seguridad: El desarrollo y mantenimiento de los sistemas de información irán acompañados de las especificaciones de seguridad y de los correspondientes procedimientos de control.

k) Adquisición de productos de seguridad y contratación de servicios de seguridad.: Se optará, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, por aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

l) Monitorización continua: se desarrollarán servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones del Ayuntamiento (Centro de Operaciones de Ciberseguridad (SOC)) integrado en la Red Nacional de Centros de Operaciones de Ciberseguridad.

m) Prevención ante otros sistemas de información interconectados: Se protegerá el perímetro de sistemas de información, en particular, si se conecta a redes públicas y se reforzarán las tareas de prevención, detección y respuesta a incidentes de seguridad.

n) Mínimo privilegio: los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios y la funcionalidad imprescindible para que la organización alcance sus objetivos.

o) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

p) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de ciberseguridad y protección de datos personales.

8. Uso aceptable de los sistemas de información y recursos informáticos.

Los sistemas de información, la información, la infraestructura y recursos informáticos del Ayuntamiento de Granada serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas informáticos y del software (sólo los administradores de sistemas, administradores de ciberseguridad, personal técnico informático habilitado y personal del C.A.U. están autorizados a ello).
- Facilitar el acceso de forma deliberada a las instalaciones o los servicios a personas no autorizadas.
- La creación o transmisión de material que cause congestión en la red o en los servidores, mediante programas concebidos a tal fin.
- Realizar cualquier tipo de ataque tanto a elementos internos como externos, intentar ganar acceso a facilidades o información para los que no se ha sido autorizado y, en general, sobrepasar o anular las protecciones de seguridad establecidas.
- La conexión a los servidores o a la red de cualquier equipo o elemento particular (no corporativo) sin aprobación del Responsable de Ciberseguridad.
- El cambio de ubicación o configuración de cualquier elemento de la red, ordenador, dispositivo o servidores sin la autorización del Responsable de Ciberseguridad o el Responsable de Sistemas.
- Realizar escuchas del tráfico que se transmite por la red.
- Destrucción o modificación malintencionada de la información de otros empleados o de los servicios.
- Violación de privacidad e intimidad de otros empleados o deterioro de su trabajo.

- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- Provocar daños físicos a equipos o infraestructura de cableado y comunicaciones.

9. Acceso a recursos informáticos corporativos.

a) Acceso a red corporativa: No se permitirá el acceso a la red, a los sistemas, aplicaciones o información corporativa a personas ni a dispositivos que no estén formalmente autorizadas para ello. En el caso de contratistas o de personas que desarrollen funciones para el Ayuntamiento de Granada, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con el Ayuntamiento de Granada para mantener el mismo nivel de seguridad que si fueran personal laboral o funcionario del Ayuntamiento. El Ayuntamiento de Granada controlará el acceso a los servicios en redes internas y externas y se asegurará que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red del Ayuntamiento y otras redes, los mecanismos adecuados de acceso y autenticación en el Sistema de Información para usuarios y equipos. Para evitar un uso malicioso de la red del Ayuntamiento de Granada existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

b) Acceso a recursos y aplicaciones software: Se elaborarán listas de software autorizado (listas blancas). Queda totalmente prohibida la instalación de otro software que no sea el autorizado y necesario para el correcto desarrollo de las funciones encomendadas por parte del Ayuntamiento de Granada. Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias. Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable del Sistema y autorizado por el Responsable de Ciberseguridad.

c) Control de Acceso: Se deberán garantizar los adecuados niveles de control de acceso en las diferentes capas de acceso a la información (red, sistema operativo y aplicaciones), evitando así el acceso no autorizado. Los controles tendrán en cuenta, entre otros, las necesidades específicas de cada sistema, siendo el nivel de control coherente con la clasificación de la información gestionada; se hará uso de distintos perfiles de usuario que los sistemas operativos y aplicativos permitan y se tendrá en cuenta la segregación de funciones cuando se requiera; se seguirán los procedimientos de autorización, revocación y revisión de permisos y de gestión de contraseñas. En relación a los accesos a través de redes, se deberán establecer controles específicos para garantizar que no se compromete la seguridad de la información, especialmente con la interconexión entre redes de otras organizaciones

o redes públicas (Internet). Se deberá mantener un adecuado nivel de concienciación de las personas comprendidas en el ámbito de aplicación de esta Política de Seguridad en relación a sus responsabilidades acerca del mantenimiento de las medidas de control de acceso, particularmente en el uso de sus credenciales y en la seguridad de la información que manejan.

10. Situaciones de movilidad y teletrabajo

El Ayuntamiento de Granada debe implementar la Política de Ciberseguridad y Protección de Datos en situaciones de movilidad y teletrabajo, implantando herramientas seguras de comunicación, fomentando el acceso seguro a los recursos tecnológicos municipales y estableciendo medidas robustas de identificación. La protección requerida será proporcional al riesgo que implique la modalidad del trabajo.

Debido a los problemas de inseguridad de Internet, no se debe transferir información por este medio de la organización a los domicilios particulares. En caso de teletrabajo, se deberá utilizar redes privadas virtuales (VPN). Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada esté libre de virus o código malicioso.

Cuando los equipos o la información propiedad del Ayuntamiento de Granada estén fuera de las instalaciones, el responsable de su seguridad es quien los está utilizando y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

CAPÍTULO II
Modelo de Gobernanza

11. Estructura organizativa.

Con carácter general, todas las personas usuarias de los sistemas de información del Ayuntamiento de Granada son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellas recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

El marco organizativo para la gestión de la Política de Seguridad de la información y Protección de Datos está constituido por:

a) Dirección (Junta de Gobierno Local)
b) Titular de la Concejalía con competencias delegadas en materia de Ciberseguridad y Protección de Datos
c) Comité General de Ciberseguridad
d) Comité Técnico de Ciberseguridad
e) Responsable de Ciberseguridad

f) Delegado/a de Protección de Datos
g) Responsable de la Información y del Servicio
h) Responsables del Sistema
i) Administradores de Ciberseguridad
j) Los Responsables y Encargados del tratamiento de datos personales
k) Rol Externo: Centro de Operaciones de Ciberseguridad (CoCS)
l) Rol Externo: Equipo de Respuesta a Incidentes de Seguridad (ERI)

12. Dirección (Junta de Gobierno Local)

Órgano colegiado que decide la misión y los objetivos de la Organización y aprueba y desarrolla la normativa derivada de esta Política.

13. Titular de la Concejalía con competencias delegadas en materia de Ciberseguridad y Protección Datos.

Órgano unipersonal que ejerce por delegación las competencias que le son propias. Ejerce la Presidencia del Comité General de Ciberseguridad.

14. Comité General de Ciberseguridad (CGENCSEG)

El Comité General de Ciberseguridad es el órgano colegiado de impulso, seguimiento y coordinación interna en materia de Ciberseguridad y Protección de Datos en el ámbito del Ayuntamiento de Granada.

El Comité General de Ciberseguridad se reunirá una vez al año con carácter ordinario y con carácter extraordinario a propuesta de la Presidencia o de un tercio de sus miembros.

Composición

Presidencia: Persona titular de la Concejalía en materia de Ciberseguridad y Protección Datos. Tendrá voto de calidad en la toma de decisiones del Comité. En caso de ausencia, vacante o enfermedad será sustituido por el Vicepresidente, y, en su defecto, por el miembro del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden.

Vicepresidencia: La persona titular de la Coordinación General en materia de Ciberseguridad y Protección Datos.

Secretaría: Responsable de Ciberseguridad, quien, como miembro de la Comisión, tendrá derecho a voto.

Vocales: las personas titulares de:

- la Secretaría General,
- la Intervención General,

- la Asesoría Jurídica,
- la Coordinación General de Alcaldía,
- la Dirección General en materia de Recursos Humanos,
- la Dirección General en materia de Ciberseguridad y Protección Datos,
- Responsable/s del Sistema,
- Delegado/a de Protección de Datos.

A requerimiento del Comité General de Ciberseguridad se convocará cualesquiera otros responsables, propios o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el Esquema Nacional de Seguridad y por la regulación en materia de Protección de Datos.

Funciones

Funciones del Secretario:

- Convocar las reuniones del Comité General de Ciberseguridad.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Impulsar la ejecución de las decisiones del Comité.

Funciones de los Vocales:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las funciones del Comité General de Ciberseguridad.

Todos los miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo el voto de la mayoría simple de sus miembros.

Funciones del Comité:

a) Asegurar el compromiso del Ayuntamiento de Granada con una efectiva gestión de la Ciberseguridad y Protección de Datos Personales y su mejora continua, coordinando los esfuerzos de las diferentes áreas municipales, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

b) Revisar regularmente la Política de Ciberseguridad y Protección de Datos y elevarla, a través de la Presidencia, para su aprobación por el órgano competente.

c) Elaborar la estrategia de evolución de la Organización en lo que respecta a la Ciberseguridad y Protección de Datos.

d) Apoyar la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de Seguridad de la Información a través de los órganos que se creen al respecto en las Administraciones Públicas.

e) Aprobar y coordinar las propuestas de los Responsables de Información y Servicios sobre los niveles de seguridad de la información y de los servicios y asumir las funciones de los Responsables de Información y Servicios en las actuaciones en que se considere necesario. Aprobar los niveles de riesgo y los riesgos residuales de cada sistema de información o servicio.

f) Velar por la disponibilidad de los recursos necesarios para el desarrollo de la Política de Ciberseguridad y Protección de Datos.

g) Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

1. Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones del organismo en materia de ciberseguridad y protección de datos personales.
2. Promover la divulgación de la Política de Ciberseguridad y Protección de datos así como las Normativas de Seguridad de la Información aprobadas y demás normativa derivada, promoviendo actividades de concienciación y formación en materia de ciberseguridad y protección de datos.
3. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Concejalías.
4. Proponer planes de mejora de la Ciberseguridad, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
5. Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

15. Comité Técnico de Ciberseguridad (CTECCSEG)

El Comité Técnico de Ciberseguridad queda adscrito al órgano directivo con rango de Dirección General con competencias en materia de Ciberseguridad y Tecnologías de la Información y Comunicaciones, como órgano colegiado para coordinar actuaciones destinadas al cumplimiento de los requisitos técnicos y operativos de la normativa de Seguridad de la Información y Protección de Datos Personales, y de la estrategia de Ciberseguridad aprobada por el Comité General de Ciberseguridad, en relación a los sistemas de información y servicios tecnológicos dependientes del citado órgano directivo.

El Comité Técnico de Ciberseguridad se reunirá con carácter ordinario cada tres meses y con carácter extraordinario a propuesta de la Presidencia o de un tercio de los vocales que la integran.

Composición

Presidencia: La persona titular del órgano directivo con rango de Dirección General con competencias en materia de tecnología, ciberseguridad y protección de datos. En caso de ausencia, vacante o enfermedad será sustituido por el Vicepresidente, y, en su defecto, por el miembro del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden.

Vicepresidencia: Responsable de Ciberseguridad

Secretaría: La persona que tenga asignada la jefatura con competencias en Ciberseguridad Corporativa y Confianza Digital que, como miembro del Comité Técnico de Ciberseguridad, tendrá así mismo derecho a voto.

Vocales:

- Máximo responsable técnico con competencias en la Administración Electrónica y la Transformación Digital municipal.
- Máximo responsable técnico con competencias en la Infraestructura y Telecomunicaciones municipales.
- Máximo responsable técnico con competencias en la Innovación y en Smartcity municipales.
- Delegado/a de Protección de Datos
- Jefatura con competencias en Administración de la Ciberseguridad
- Jefatura con competencias en Administración Electrónica
- Jefatura con competencias en Transformación Digital
- Jefatura con competencias en Internet

El Comité Técnico de Ciberseguridad podrá incorporar a su composición, con voz pero sin voto, a aquellos responsables/roles que se vean afectados por la toma de decisiones para recopilar ideas u opiniones de los mismos así como a personal municipal o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el Esquema Nacional de Seguridad y por la regulación en materia de Protección de Datos.

Funciones

Al Comité Técnico de Ciberseguridad le corresponden las siguientes funciones:

a) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la Política de Ciberseguridad y Protección de datos y del resto de la normativa de seguridad.
b) Elaborar o apoyar en la elaboración de Normativas de Seguridad de la Información, Instrucciones Técnicas de Ciberseguridad o Procedimientos Operativos de Ciberseguridad a petición del Responsable de Ciberseguridad o del Comité General de Ciberseguridad.
c) Analizar el cumplimiento de la Política de Ciberseguridad y Protección de datos y de su desarrollo normativo y realizar propuestas de mejora.
d) Analizar las medidas de seguridad de la información, de protección de datos personales y de los servicios electrónicos prestados por los sistemas de información y realizar propuestas de mejora.
e) Coordinar la correcta gestión de los incidentes de seguridad,
f) Analizar la operación del Centro de Operaciones de Ciberseguridad (CoCS) y las actuaciones del Equipo de Respuesta a Incidentes de Seguridad (ERI)

g) Aprobar Planes de Mejora de la Ciberseguridad para mitigar riesgos.

h) Controlar e informar regularmente del estado de la seguridad de la información, así como de las necesidades de formación del personal informático, las necesidades normativas y procedimentales y de las necesidades de medios materiales y/o personales en materia de ciberseguridad.

i) Velar por que la Ciberseguridad y Protección de Datos se tenga en cuenta en todos los proyectos de tecnologías de la información y las telecomunicaciones, así como durante el ciclo de vida completo de los sistemas de información.

Todas estas funciones del Comité Técnico de Ciberseguridad, se entienden sin perjuicio de las funciones que les corresponden a otros perfiles unipersonales que se detallan en esta Política de Ciberseguridad y Protección de datos.

16. Responsable de Ciberseguridad (CISO)

Funciona como supervisor de la seguridad de la operación del sistema y vehículo de reporte al Comité General de Ciberseguridad. Corresponde a una dirección ejecutiva de la organización, actualmente a la persona titular de la Dirección Técnica de Ciberseguridad del Ayuntamiento de Granada y será jerárquicamente independiente del rol de Responsable del Sistema.

A la Dirección Técnica de Ciberseguridad se le asignarán los recursos necesarios para posibilitar el adecuado cumplimiento de sus funciones en el ámbito de actuación asignado, dotándole del personal de apoyo administrativo y personal técnico experto que resulte necesario para el adecuado desarrollo de sus funciones.

Al Responsable de Ciberseguridad le corresponden las siguientes funciones:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.

b) Impulsar la formación y concienciación en materia de ciberseguridad dentro de su ámbito de responsabilidad.

c) Proponer e impulsar la elaboración de Normas de Seguridad de la Información y velar por su cumplimiento.

d) Dictar y aprobar las Instrucciones Técnicas de Ciberseguridad.

e) Informar en materia de ciberseguridad de la actividad desarrollada en su ámbito de actuación.

f) Coordinar el Sistema de Gestión de la Seguridad de la Información en su conjunto e impulsar su continuo y efectivo funcionamiento.

g) Proporcionar y validar la información requerida en su ámbito competencial, a efectos de elaborar el Informe del Estado de Seguridad a que hace referencia el Esquema Nacional de Seguridad.

h) Aprobar los Procedimientos Operativos de Ciberseguridad.

i) Adoptar las decisiones necesarias para satisfacer los requisitos de seguridad definidos por los responsables de la información y los responsables del

servicio, ejerciendo las funciones en materia de análisis y gestión de riesgos conforme al Esquema Nacional de Seguridad.

j) Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema, a partir de las medidas de seguridad requeridas conforme al ENS y del resultado del Análisis de Riesgos.

k) Promover auditorías periódicas para verificar el grado de conformidad de los sistemas de información con las prescripciones del Esquema Nacional de Seguridad.

l) Adoptar medidas de mejora en la gestión de la seguridad de la información. A tales efectos, elaborará, junto al Responsable del Sistema, Planes de Mejora de la Ciberseguridad, para su aprobación por el Comité Técnico de Ciberseguridad.

m) Determinar los criterios de acceso de las personas a los sistemas de información municipales.

n) Poner en conocimiento del Delegado/a de Protección de Datos y del Responsable de la Información y del Servicio los ciberincidentes que se produzcan.

o) Validar los Planes de Continuidad de Sistemas que elabore el Responsable del Sistema, que deberán ser aprobados por el Comité Técnico de Ciberseguridad y probados periódicamente por el Responsable de Sistemas.

p) Validar la adquisición municipal de soluciones hardware y software que sean conformes a los requisitos de seguridad establecidos.

q) Aprobar las directrices propuestas por el Responsable del Sistema para considerar la seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

r) Facilitar periódicamente al Comité General de Ciberseguridad un resumen de actuaciones en materia de ciberseguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema, particularmente del nivel de riesgo residual al que está expuesto el sistema.

s) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución. Supervisar la actividad del Centro de Operaciones de Ciberseguridad (CoCS) y las actuaciones del Equipo de Respuesta a Incidentes de Seguridad (ERI).

t) Ejercer de interlocutor con otras organizaciones en materia de Ciberseguridad, salvo en lo que corresponda al Delegado/a de Protección de Datos del Ayuntamiento de Granada.

u) Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, asigne a los responsables de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse «responsables de seguridad delegados», dependientes funcionalmente del responsable principal, que serán responsables de las actuaciones que se les deleguen.

17. Delegado/a de Protección de Datos (DPD)

Es la persona u órgano que se ocupa de vigilar por el cumplimiento de la normativa de protección de datos, de acuerdo a las funciones recogidas en el Reglamento Europeo de Protección de Datos (2016/679), en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LO 3/2018).

En virtud del principio de responsabilidad diferenciada, debe existir la necesaria separación de funciones entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS u otras figuras asimiladas, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

El Delegado/a de Protección de Datos se adscribe a la estructura orgánica de la Dirección en materia de Ciberseguridad del Ayuntamiento de Granada, con independencia competencial y funcional en el ejercicio de sus funciones.

El Delegado/a de Protección de datos tendrá las siguientes funciones:

a) La colaboración y apoyo al Responsable de Ciberseguridad del Ayuntamiento de Granada, en el desarrollo, mantenimiento y elaboración de la normativa que resulte necesaria sobre protección de datos.

b) Informar y asesorar en materia de protección de datos en el ámbito del Ayuntamiento de Granada.

c) Supervisar el cumplimiento del 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, del resto de disposiciones normativas aplicables y de las políticas por los responsables o los encargados en materia de protección de datos personales, incluidas la asignación de responsabilidades, la concienciación, formación del personal así como la realización de las auditorías correspondientes.

d) La interlocución de los órganos responsables o encargados del tratamiento ante las diversas Autoridades de Protección de Datos.

e) Actuar como punto de contacto de la autoridad de control en cuestiones relacionadas con los tratamientos, incluyendo la consulta previa a que se refiere el artículo 36 RGPD.

f) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

g) Emitir recomendaciones a las personas responsables o encargadas del tratamiento en materia de protección de datos.

h) Supervisar, según proceda en cada caso, las acciones formativas en materia de Protección de Datos personales conjuntamente con el Responsable de Ciberseguridad.

i) La comunicación inmediata a la persona titular de la Concejalía que tenga atribuidas las competencias generales sobre protección de datos, a los órganos directivos afectados y a la persona responsable o encargada del tratamiento cuando conozca la existencia de una vulneración relevante en materia de protección de datos personales.

j) Las resoluciones que le sean atribuidas por el ordenamiento jurídico en relación con las reclamaciones sobre protección de datos.

k) Las demás funciones que le atribuyan las normas en materia de protección de datos.

El Delegado/a de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

En el desempeño de sus funciones, el Delegado/a de Protección de Datos tendrá acceso a los datos personales y operaciones de tratamiento, no pudiendo, el responsable o el encargado del tratamiento oponer a este acceso la existencia de cualquier deber de confidencialidad o secreto.

18. Responsables de la Información (RI) y Responsables del Servicio (RS)

Los Responsables de la Información y del Tratamiento tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos de la información que manejan y, por lo tanto, de su protección. Si la información manejada incluye datos de carácter personal, los Responsables de la Información y los Responsables del Servicio deberán tener en cuenta, además, los requisitos derivados de la legislación correspondiente sobre protección de datos.

Los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos del servicio en materia de seguridad y, por tanto, la potestad de determinar los niveles de seguridad del servicio. Si la información manejada incluye datos de carácter personal, los Responsables de la Información y los Responsables del Servicio deberán tener en cuenta, además, los requisitos derivados de la legislación correspondiente sobre protección de datos.

Las Direcciones Generales o responsables de la unidad máxima que culmine la organización administrativa del área serán los Responsables de la Información y del Servicio. Asimismo, son responsables de la Información y del Servicio en sus ámbitos respectivos las personas titulares de la Jefatura de Policía Local y del Servicio de Prevención y Extinción de Incendios y Salvamento del Ayuntamiento de Granada (SPEIS). Les corresponden las siguientes funciones dentro de su ámbito de competencia:

a) Velar por una adecuada gestión de la seguridad de la información.
b) Decidir sobre la finalidad, contenido y uso de la información.
c) Determinar las categorías, niveles y medidas de seguridad aplicables a los sistemas de información.
d) Aprobar las medidas técnicas y organizativas necesarias para garantizar un nivel de ciberseguridad adecuado al riesgo para los derechos y libertades de las personas. Entre ellas se incluirán las medidas necesarias para poder demostrar que el tratamiento es conforme a lo establecido en el Reglamento (UE) 2016/679.
e) Aprobar los niveles de riesgo residuales del sistema de información o servicio.

f) Elaborar, mantener y actualizar el registro de actividades de tratamiento de datos personales en el ámbito de sus competencias y comunicarlo al Delegado/a de Protección de Datos.

g) Informar sobre situaciones y amenazas que afecten o puedan afectar al funcionamiento de sus unidades, así como al tratamiento de información que realicen o los servicios que presten.

h) Cumplir el deber de información, de acuerdo con el principio de transparencia y teniendo en cuenta los criterios que se establezcan.

i) Garantizar el cumplimiento del deber de confidencialidad y de las demás obligaciones relacionadas con los derechos de las personas interesadas en materia de protección de datos personales.

j) Realizar las evaluaciones de impacto de protección de datos preceptivas usando el tratamiento entrañe alto riesgo para los derechos y las libertades de las personas, con el asesoramiento del Delegado/a de Protección de Datos y los Responsables de la Seguridad y de los Sistemas.

k) Comunicar los incidentes de seguridad que pudieran producirse tanto al Delegado/a de Protección de Datos como al Responsable de la Ciberseguridad del Ayuntamiento de Granada.

l) Gestionar las cláusulas de encargo de tratamiento de datos con terceros en el ámbito de su Concejalía y verificar su cumplimiento.

m) Responder a los requerimientos que les envíen tanto el Responsable de Ciberseguridad como el Delegado/a de Protección de Datos del Ayuntamiento de Granada.

n) Atender a las auditorías que se realicen.

o) Cualquier otra que les atribuya la normativa básica aplicable en materia de seguridad de la información y protección de datos personales.

Cada Concejalía Municipal, así como Policía Local y Servicio de Prevención y Extinción de Incendios y Salvamento (SPEIS), designarán una persona intermediaria con la Dirección Técnica de Ciberseguridad, para colaborar y coordinar las funciones relativas a Ciberseguridad y Protección de Datos Personales.

19. Responsables del Sistema (RSIS)

El rol de Responsable del Sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida y toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación. Este rol no podrá coincidir con el de Responsable de la Información, con el de Responsable de Servicio ni con el de Responsable de Ciberseguridad. El rol de Responsable del Sistema corresponde, actualmente, al máximo responsable técnico con competencias en la administración electrónica y la transformación digital municipal así como al máximo responsable técnico con competencias en las infraestructuras y telecomunicaciones municipales.

Las funciones de Responsable del Sistema son las siguientes:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Conforme a las directrices del Responsable de Ciberseguridad y en coordinación con él, la implantación y control de las medidas específicas de seguridad del sistema y de que éstas se integren adecuadamente dentro del marco general de seguridad, incluyendo la determinación e implementación de las configuraciones autorizadas de hardware y software a utilizar en el sistema y sus modificaciones.

c) Informar al Responsable de Ciberseguridad sobre los incidentes de seguridad, vulnerabilidad y las anomalías observadas en la aplicación de las normas y procedimientos de seguridad.

d) Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, el acuerdo de la suspensión, será adoptado de manera conjunta por el responsable de la información afectada, los responsables del servicio afectado y con el Responsable de Ciberseguridad.

e) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

f) Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.

g) Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.

h) Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.

i) Elaborar Planes de Mejora de la Seguridad junto al Responsable de Ciberseguridad.

j) Elaborar Procedimientos Operativos de Ciberseguridad así como la documentación de seguridad del sistema para su aprobación por el Responsable de Ciberseguridad.

k) Establecer planes de continuidad, contingencia y emergencia y sus pruebas de verificación correspondientes.

l) Proponer los cambios que afecten a la seguridad del modo de operación del Sistema y elevarlos al Responsable de Ciberseguridad quién determinará su aprobación final.

m) Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.

n) Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente y ante incidentes de seguridad relevantes al Responsable de Ciberseguridad.

o) Impulsar la respuesta a incidentes de seguridad y la eliminación de vulnerabilidades en los sistemas de información bajo su responsabilidad.

p) Mantener y recuperar la información almacenada por el sistema y sus servicios asociados.

q) Colaborar en la elaboración de catálogos de activos y servicios, análisis de riesgos, evaluaciones de impacto, en la realización de auditorías, en acciones de asesoramiento y en cualquier otra actividad relacionada con la Seguridad de la Información en que sea necesaria su participación

20. <u>Administradores de Ciberseguridad (ADMCSEG)</u>

Persona/as encargadas de la implementación, gestión y mantenimiento de las medidas de seguridad que sean de aplicación a los sistemas de información de acuerdo a las directrices del Responsable de Ciberseguridad. Los Administradores de Ciberseguridad pueden comprender perfiles distinguidos en función de la especialización técnica en ciberseguridad:

- de cumplimiento normativo y confianza digital.
- de gestión y mantenimiento de medidas de seguridad aplicables al sistema.

Las funciones comunes de los distintos perfiles del Administrador de Ciberseguridad son:

a) Monitorizar el estado de la seguridad del sistema.
b) Aplicar los Procedimientos Operativos de Ciberseguridad aprobados e informando al Responsable de Ciberseguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
c) Elaborar Procedimientos Operativos de Ciberseguridad y asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y se registren con la frecuencia deseada, de acuerdo con esta Política y normativa derivada.
d) Colaborar en la elaboración de catálogos de activos y servicios, análisis de riesgos, evaluaciones de impacto, en la realización de auditorías, en acciones de asesoramiento y en cualquier otra actividad relacionada con la Ciberseguridad en que sea necesaria su participación.
e) Coordinar el proceso de respuesta ante los ciberincidentes que se produzcan en el sistema bajo la supervisión del Responsable de Ciberseguridad, Responsable/s de Sistema, así como la coordinación de actuaciones del Centro de Operaciones de Ciberseguridad (CoCS) y el Equipo de Respuesta a Incidentes de Seguridad (ERI).

Las funciones específicas del perfil de cumplimiento normativo y confianza digital son:

f) Cumplimiento normativo en ciberseguridad. Impulso al Sistema de Gestión de Seguridad de la Información
g) Implementación de estrategias municipales de ciberseguridad. Gestión de la identidad corporativa, certificados y sellos municipales. Evaluación de tecnologías de ciberseguridad y su adecuación en los contratos municipales.
h) Planificación, supervisión e implementación de la arquitectura de seguridad de los sistemas y servidores municipales. Evaluación de riesgos, ciberinteligencia y respuesta a ciberincidentes. Auditorías de seguridad.

i) Fomento de la cultura y concienciación en materia de ciberseguridad en el Ayuntamiento de Granada.

Las funciones específicas del perfil de gestión y mantenimiento de medidas de seguridad aplicables al sistema son:

j) Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema.
k) Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de ciberseguridad del sistema.
l) Verificar y realizar el seguimiento de los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
m) Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de la actividad, de forma que ésta se ajuste a lo autorizado.
n) Asegurar que los controles para empleo de software autorizado en el sistema son cumplidos estrictamente y que no se usa software no autorizado.
o) Garantizar la seguridad de la red, apoyándose en el Centro de Operaciones de Ciberseguridad (CoCS) y en el Administrador de la Red.
p) Configurar los elementos de seguridad integrados en la red, como son los cortafuegos, NAC, enrutadores, etc. atendiendo a cuestiones funcionales y de seguridad, apoyándose en el Administrador de la Red.
q) Impulsar la eliminación de vulnerabilidades en los sistemas de información.

21. Los Responsables y Encargados de tratamiento de datos personales.

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otra entidad que, solo o junto con otros, determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.

La identidad del responsable del tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del Reglamento General de Protección de Datos.

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento

22. Rol Externo: Centro de Operaciones de Ciberseguridad (CoCS)

Bajo la responsabilidad y dirección del Responsable de Ciberseguridad, el Centro de Operaciones de Ciberseguridad (CoCS) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación

diaria de los sistemas TIC a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque. El CoCS puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el Responsable de Ciberseguridad.

El Centro de Operaciones de Ciberseguridad (CoCS) deberá estar integrado en la Red Nacional de Centros de Operaciones de Ciberseguridad y puede llevar a cabo las siguientes funciones:

a) Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.

b) Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.

c) Operación y actualización de los dispositivos de defensa.

d) Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad (ERI).

e) Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.

f) Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.

g) Análisis forense digital y de seguridad.

h) Servicio de cibervigilancia que posibilite la prospectiva sobre las ciberamenazas.

23. Rol Externo: Equipo de Respuesta a Incidentes de Seguridad (ERI)

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el Comité Técnico de Ciberseguridad y funcionales del Responsable de Ciberseguridad y posibles alertas recibidas del Centro de Operaciones de Ciberseguridad (CoCS). El ERI puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el Responsable de Ciberseguridad. Entre sus funciones se destacan las siguientes:

a) Aplicación de inteligencia para la detección, respuesta coordinada, investigación de ciberataques y ciberamenazas y resolución de incidentes de seguridad, siempre en coordinación con el CoCS y el Responsable de Ciberseguridad.

b) Llevar a cabo el registro, seguimiento y resolución de los incidentes de seguridad en los sistemas bajo su responsabilidad.

c) Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

d) Realizar análisis forense digital y de seguridad cuando la complejidad del incidente así lo requiera, en coordinación con el Responsable de Ciberseguridad.

e) Proponer al Responsable de Ciberseguridad acciones inmediatas a corto plazo si se detecta un comprometimiento de la información que pudiera tener consecuencias graves.

f) Asegurar los elementos críticos del sistema, si se ha visto comprometida la seguridad del mismo.

g) Determinar, hasta donde sea posible, el modo, los medios, los motivos y el origen del incidente, colaborando con el Responsable de Ciberseguridad en la obtención de conclusiones y aprendizaje del mismo, de modo que se posibilite la prevención de incidentes similares en el futuro.

CAPÍTULO III
Desarrollo de la Política de Ciberseguridad y Protección de Datos

24. Instrumentos de desarrollo de la Política.

La Política de Ciberseguridad y Protección de Datos se desarrollará por medio de:

a) Normas de Seguridad de la Información.
b) Instrucciones Técnicas de Ciberseguridad.
c) Procedimientos Operativos de Ciberseguridad.
d) Guías Técnicas de Ciberseguridad.

Las Normas de Seguridad de la Información uniformizan el uso de aspectos concretos del sistema, indicando el uso correcto y las responsabilidades de los usuarios y son de obligado cumplimiento para el personal del Ayuntamiento de Granada. Serán aprobadas por la Junta de Gobierno Local, estableciéndose en ellas las directrices y principios generales aplicables a los siguientes aspectos de la Seguridad de la Información:

a) Gestión de la Política de Ciberseguridad y Protección de datos.
b) Organización de la seguridad y responsabilidades.
c) Seguridad ligada al personal.
d) Clasificación y control de activos.
e) Control de accesos y gestión de claves.
f) Seguridad física y del entorno.
g) Seguridad operacional.
h) Seguridad de las comunicaciones.
i) Adquisición, desarrollo y mantenimiento de sistemas.
j) Gestión de incidentes de seguridad.
k) Gestión de la continuidad del negocio.
l) Conformidad legal.

Cada uno de estos aspectos de la seguridad podrá ser desarrollado en una o varias normas de seguridad.

Las Instrucciones Técnicas de Ciberseguridad complementan o desarrollan las directrices establecidas en esta Política de Seguridad o en las Normas de Seguridad de la Información derivadas y son de obligado cumplimiento para el personal del

Ayuntamiento de Granada. Su aprobación corresponde al Responsable de Ciberseguridad.

Los Procedimientos Operativos de Ciberseguridad, en los que se concretarán de forma detallada las acciones a desarrollar en un proceso crítico relacionado con la seguridad. Su aprobación corresponde al Responsable de Ciberseguridad.

Las Guías Técnicas de Ciberseguridad, de carácter meramente informativo, constituyen una ayuda a las personas usuarias del sistema de información municipal para aplicar de forma correcta las medidas de seguridad. Su aprobación corresponde al Responsable de Ciberseguridad.

Forman parte de los instrumentos de desarrollo de la Política de Ciberseguridad y Protección de Datos los acuerdos adoptados por el Comité General de Ciberseguridad y por el Comité Técnico de Ciberseguridad.

25. Gestión de documentos relativos a la Política.

Corresponde a la Dirección competente en materia de Ciberseguridad la gestión documental de las normas, instrucciones, procedimientos generales, procedimientos operativos y guías técnicas de seguridad, definiendo su estructura, categorización, trazabilidad y requisitos de acceso, sin perjuicio de las facultades atribuidas al Comité General de Ciberseguridad.

26. Revisión de la Política de Ciberseguridad y Protección de Datos.

La Política de Ciberseguridad y Protección de Datos será revisada por el Comité General de Ciberseguridad a intervalos planificados, que no podrán exceder los dos años de duración o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Ciberseguridad y Protección de Datos deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con esta Política.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

27. Sanciones previstas por incumplimiento.

El incumplimiento de esta Política de Ciberseguridad y Protección de Datos y de la normativa en materia de seguridad podrá conllevar responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la normativa sobre régimen disciplinario de los empleados públicos.

CAPÍTULO IV
Gestión de la Política de Ciberseguridad y Protección de Datos

28. Ciberincidentes y brechas de seguridad

Se atenderá especialmente a la seguridad de los sistemas de información y se dispondrá de un proceso integral para hacer frente a los incidentes que contemple las medidas de detección, contención, reacción y recuperación y que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.

Se notificarán al Centro Criptológico Nacional (CCN-CERT) aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información, de acuerdo con lo dispuesto en la normativa reguladora del Esquema Nacional de Seguridad (ENS).

De conformidad con lo dispuesto en el artículo 33 del RGPD, el Ayuntamiento adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse, a través del procedimiento establecido al efecto por el Consejo de Transparencia y Protección de Datos de Andalucía o por la Agencia Española de Protección de Datos (AEPD).

Igualmente, el Ayuntamiento adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

29. Deber de información a la Corporación municipal, colaboración y confidencialidad

En el supuesto de que los sistemas de información del Ayuntamiento de Granada sufran un ciberincidente categorizado, según el Esquema Nacional de Seguridad, con nivel de peligrosidad o impacto alto, muy alto o crítico, el Titular de la Concejalía con competencias delegadas en materia de Ciberseguridad y Protección de Datos comunicará, a la mayor brevedad posible, no siendo nunca superior el plazo a 3 días hábiles, desde su conocimiento, la información disponible sobre la incidencia de seguridad al Alcalde/sa así como a los/as concejales portavoces de los distintos grupos políticos municipales con representación en el Ayuntamiento, quienes tienen el deber de colaborar así como guardar la debida confidencialidad de dicha información durante las actuaciones llevadas a efecto en el marco de la resolución del ciberincidente.

Queda expresamente prohibido difundir o comentar públicamente información alguna, incluso en el caso de que sea de conocimiento público, en todo caso hasta la resolución del ciberincidente.

Igualmente, el Titular de la Concejalía con competencias delegadas en materia de Ciberseguridad y Protección de Datos informará regularmente de los avances realizados en la investigación, las medidas de seguridad adoptadas y, finalmente, de la resolución del ciberincidente.

30. Análisis y Gestión de Riesgos.

La gestión de riesgos es un factor esencial para una exitosa gestión de la Seguridad de la Información. En ella deberán colaborar todos los participantes en la gestión de la Seguridad de la Información y protección de datos personales, según sus competencias y funciones.

Todos los sistemas y servicios prestados sujetos a esta Política de Ciberseguridad y Protección de Datos deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se realizará:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Responsable de Ciberseguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

En particular, para realizar el análisis de riesgos, como norma general se utilizará la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

Los riesgos residuales serán determinados por el Responsable de Ciberseguridad. Los niveles de Riesgo residuales esperados sobre cada Información o servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas) deberán ser aceptados previamente por el Responsable de esa Información o Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Ciberseguridad al Comité General de Ciberseguridad, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

31. Datos de carácter personal

El Ayuntamiento de Granada trata datos personales en el ejercicio de sus competencias y de acuerdo a la normativa vigente. El tratamiento de datos personales se ajustará a las obligaciones y principios recogidos en el Reglamento Europeo de

Protección de Datos 679/2016, así como en lo estipulado por la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Todos los sistemas de información del Ayuntamiento de Granada que traten datos de carácter personal se ajustarán a la normativa y asignará las medidas de seguridad técnicas y organizativas necesarias para la correcta protección de los datos personales en base al riesgo que implique cada tratamiento y siempre en defensa de los derechos y libertades de las personas interesadas.

El Ayuntamiento de Granada en cumplimiento de la normativa vigente en materia de Protección de Datos Personales designó un Delegado de Protección de Datos, con las funciones que recoge el Reglamento 679/2016 y la Ley Orgánica 3/2018, y que está a disposición de la ciudadanía para atender cualquier cuestión relacionada con la aplicación de la normativa de protección de datos, pudiendo contactarse con el mismo a través de la dirección de correo electrónico dpd@granada.org

32. Colaboración en materia de Ciberseguridad y Protección de Datos Personales.

Estas dos áreas de actividad se encuentran intrínsecamente relacionadas, por ello se establece como criterio de relación entre el Responsable de Ciberseguridad y el Delegado de Protección de Datos los principios de cooperación y colaboración en todas aquellas actuaciones que afecten a los campos de actuación de ambas partes, de forma que se consensuarán las decisiones a tomar, con pleno respeto al reparto competencial legalmente establecido, a la legislación vigente y el contenido de la presente Política de Ciberseguridad y Protección de Datos.

33. Registro de Actividades de Tratamiento de datos personales.

La Concejalía competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales establecerá los criterios para la elaboración del Registro de las Actividades de Tratamiento de datos de carácter personal del Ayuntamiento de Granada.

El responsable del tratamiento en el ámbito de sus competencias llevará y mantendrá actualizado el Registro de Actividades de Tratamiento de datos de carácter personal, que incluirá la información a la que se refiere el artículo 30 del Reglamento (UE) 2016/679, y se documentará de acuerdo con los criterios a que se refiere el apartado 1 de este artículo.

El responsable del tratamiento comunicará al Delegado de Protección de Datos el Registro de Actividades de Tratamiento de Datos que gestiona en su ámbito de actuación, así como sus modificaciones.

El Ayuntamiento de Granada hará público un inventario de sus actividades de tratamiento accesible a través del Portal Web del Ayuntamiento de Granada. Para

ello, cada responsable de tratamiento comunicará al Delegado de Protección de Datos la información necesaria para su formación, en el modelo que se establezca.

34. Formación y concienciación

El Ayuntamiento de Granada deberá adoptar las medidas necesarias para que su personal reciba la formación específica adecuada para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios, así como en materia de protección de datos personales de la Administración municipal.

La Dirección competente en materia de Ciberseguridad conjuntamente con la Concejalía competente en materia de formación de personal del Ayuntamiento de Granada:

a) Desarrollarán acciones de formación, concienciación e información en materia de Ciberseguridad y de Protección de Datos Personales.
b) Procurarán que las personas que utilicen los sistemas de información gestionados en el ámbito de sus competencias, o que accedan a la información en ellos contenidos, reciban de forma efectiva información sobre las obligaciones que suponen el uso o acceso.
c) Dispondrán los medios necesarios para que las personas con responsabilidad en la administración u operación tecnológica de los sistemas de información reciban la formación necesaria para desarrollar su actividad acorde a los requisitos y necesidades de una correcta gestión de la Seguridad de la Información y una efectiva aplicación de las medidas de protección que correspondan.

El Comité General de Ciberseguridad y el Comité Técnico de Ciberseguridad promoverán la formación y concienciación del personal en las materias de Ciberseguridad y Protección de Datos dentro de sus ámbitos de actuación.

El Responsable de Ciberseguridad y el Delegado de Protección de Datos del Ayuntamiento de Granada colaborarán en el diseño y planificación de las acciones formativas e informativas que afecten a estas materias para garantizar la coherencia, evitar duplicidades y adecuarlas a las necesidades reales de la organización.

35. Obligaciones del personal

Todas las personas que traten información del Ayuntamiento de Granada, de manera automatizada o no automatizada, o tengan acceso a sus sistemas de información, tienen las siguientes obligaciones:

a) Conocer y respetar la Política de Ciberseguridad y Protección de Datos, así como las Normas de Seguridad de la Información, Instrucciones Técnicas de Ciberseguridad y Procedimientos Operativos de Ciberseguridad que la desarrollen y que le afecten.
b) Acceder a los datos personales solo cuando tenga autorización, en virtud de las funciones o tareas asignadas, y guardar el deber de confidencialidad.

c) Utilizar los datos únicamente para los fines para los cuales han sido recabados, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral.

d) No divulgar las contraseñas de acceso a los sistemas y de las aplicaciones informáticas que contengan datos de carácter personal, y custodiar con diligencia los documentos en soporte papel que los contengan.

e) Solicitar las autorizaciones necesarias para almacenar información en dispositivos portátiles o tratar fuera de las dependencias administrativas datos de carácter personal.

f) No utilizar con fines distintos a los propios del servicio los medios digitales puestos a su disposición.

g) Notificar, con carácter de urgencia y según los procedimientos establecidos, eventos que puedan suponer un incidente de seguridad o evidencien una debilidad que pueda implicar posteriores incidentes.

h) Colaborar, en su caso, en la resolución de incidentes de seguridad y en la realización de acciones preventivas.

i) Bloquear el equipo asignado cuando se ausente del puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

j) Participar en la gestión de la Seguridad de la Información cuando corresponda según las funciones de su puesto de trabajo.

k) No realizar acciones intencionadas que perjudiquen la seguridad de los sistemas tecnológicos o de información, ni la información que contienen.

l) Colaborar y participar en las auditorías sobre Seguridad de la Información y Protección de Datos Personales cuando sea requerido.

m) Asistir a las sesiones de formación y concienciación en materia de Ciberseguridad y Protección de datos, a las que sean convocados.

El personal del Ayuntamiento de Granada tiene la obligación de conocer y cumplir esta Política de Ciberseguridad y Protección de datos, así como la normativa de seguridad aprobada. A tales efectos, desde la Dirección competente en materia de Ciberseguridad se dará la publicidad necesaria en el Portal del Personal Municipal, correo electrónico y otros medios de difusión.

36. Obligaciones de personas externas al Ayuntamiento de Granada.

En el caso de personas vinculadas a entidades externas que hagan uso de recursos tecnológicos municipales, el uso se limitará a los recursos, tareas y actividades circunscritas en los términos del contrato o acuerdo que regula la relación entre esa entidad y el Ayuntamiento de Granada y deberán cumplir esta Política y normativa de seguridad que les sea de aplicación.

Los ciudadanos que realicen trámites utilizando los servicios de Administración Electrónica, o que accedan a páginas web o sistemas públicos del Ayuntamiento de Granada, no están afectados por las obligaciones señaladas en el apartado anterior de este artículo, si bien, podrán aprobarse normas o recomendaciones específicas para el uso o acceso a esos servicios o sistemas que les

pudieran afectar, en cuyo caso serían debidamente informados en el acceso a los mismos.

37. Terceras partes

Cuando el Ayuntamiento de Granada preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Ciberseguridad y Protección de Datos, se establecerán canales para reporte y coordinación de los respectivos Responsables de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Granada utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña 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 garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su relación con Acuerdo.

La organización prestataria de servicios al Ayuntamiento deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información, así como la gestión de los incidentes para el ámbito del servicio que provea. Este POC de seguridad, será el propio Responsable de Seguridad de la organización contratada o formará parte de su área o tendrá comunicación directa con la misma.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad 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. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por el Ayuntamiento de Granada y deberán formalizar su relación como encargados de tratamientos.

CAPÍTULO V
Aprobación, entrada en vigor y normativa derogada

38. Aprobación y entrada en vigor

Esta Política de Ciberseguridad y Protección de datos entrará en vigor desde la fecha de su aprobación por Acuerdo del Excmo. Ayuntamiento Pleno y estará vigente hasta que sea reemplazada por la aprobación de una nueva norma en la materia por el mismo órgano que la aprobó. Todo ello, sin perjuicio de los cambios o modificaciones que sean aprobados.

39. Normativa derogada

Quedan derogadas todas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta Política de Ciberseguridad y Protección de Datos del Ayuntamiento de Granada.

Se certifica con la salvedad a que se refiere el artículo 206 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, y a reserva de los términos que resulten de la aprobación del acta correspondiente.

Y para que así conste, expido la presente en Granada, en la fecha abajo indicada.