SESIÓN ORDINARIA CELEBRADA POR LA JUNTA DE GOBIERNO LOCAL EL DÍA TREINTA Y UNO DE MARZO DE DOS MIL DIECISIETE.

En la ciudad de Granada y en la Sala de Reuniones de Alcaldía del Palacio Consistorial, siendo las nueve horas y cinco minutos del día treinta y uno de marzo de dos mil diecisiete, bajo la Presidencia del Excmo. Sr. Alcalde-Presidente, Don Francisco Cuenca Rodríguez, se reúnen los miembros de la Junta de Gobierno Local: Tenientes de Alcalde Doña Ana Muñoz Arquelladas y Don Baldomero Oliver León, los Concejales y Concejalas Doña Raquel Ruz Peis quien actúa como Concejala-Secretaria al amparo de lo dispuesto en el artículo 17.4 del Reglamento Orgánico Municipal, Don Miguel Ángel Fernández Madrid, Doña Jemima Sánchez Iborra, Don Eduardo José Castillo Jiménez y Doña María de Leyva Campaña.

Asimismo asisten Don Ildefonso Cobo Navarrete, Secretario General, Don Gustavo García-Villanova Zurita, Vicesecretario General, en funciones de Órgano de Apoyo al Concejal-Secretario, y el Interventor de Fondos Don Francisco de Paula Aguilera González, con el fin de celebrar la presente sesión ordinaria para la que previamente han sido citados.

NUEVAS TECNOLOGÍAS

296

Aprobación de la Política de Seguridad de la Información del Ayuntamiento de Granada en el marco del Esquema Nacional de Seguridad.

Visto expediente **núm. 99/2017** de Nuevas Tecnologías relativo a la **aprobación de la Política de Seguridad de la Información del Ayuntamiento de Granada en el marco del Esquema Nacional de Seguridad.**

Visto el informe de fecha 28 de marzo de 2017, emitido por la Subdirectora de Calidad y Seguridad Tecnológica, la Responsable de Seguridad y el Responsable de Apoyo de Calidad y Procedimiento, que lleva el conforme del Coordinador General de Economía, Personal, Contratación y Smart City, en relación a la necesidad de aprobación de la Política de Seguridad del Ayuntamiento de Granada, que en resumen dice:

"El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias.

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral. La seguridad es una función transversal en las administraciones públicas, caracterizada por tratarse de un proceso integral constituido por todos los elementos humanos, técnicos, materiales y organizativos, relacionados con un sistema. Es por ello, que la seguridad debe abarcar cada etapa del ciclo de vida del sistema y sus documentos (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción), así como de los sistemas que lo soportan (análisis, diseño, desarrollo, implementación, operación, mantenimiento y obsolescencia).

El aspecto principal del ENS es, sin duda, que todos los órganos superiores de las AA.PP. deberán disponer de su política de seguridad que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos.

La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Real Decreto 3/2010, de 8 de enero.

Asimismo esta Política de Seguridad de la Información debe ajustarse a lo establecido en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

En la disposición transitoria del Real Decreto 3/2010, se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad, requiriéndose en primer lugar preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.

Así, dentro de este marco normativo se ha preparada desde el Área competente en materia de nuevas tecnologías el siguiente texto que contiene la Política de la Seguridad de la Información del Ayuntamiento de Granada: (se contiene en la propuesta)"

Por ello se estima procedente y así a propuesta del Teniente de Alcalde Delegado de Economía, Hacienda, Personal, Contratación, Organización y Smart City, la Junta de Gobierno Local por unanimidad **acuerda:** Aprobar la Política de Seguridad del Ayuntamiento de Granada conforme al texto que se inserta a continuación:

"1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Junta de Gobierno Local del Ayuntamiento de Granada, el día XX de xxxxxxx de 2017.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

La entrada en vigor de la presente Política de Seguridad de la Información del Ayuntamiento de Granada supone la derogación de cualquier otra que existiera a nivel de los diferentes departamentos municipales.

2. OBJETIVO

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

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

La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en el Ayuntamiento de Granada.

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 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:

- Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por el Ayuntamiento de Granada.
- 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.
- 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.
- Proteger los recursos de información del Ayuntamiento de Granada y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

3. ALCANCE.

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

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

4.- PRINCIPIOS Y DIRECTRICES.

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

Prevención.

El Ayuntamiento de Granada debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad (en adelante, ENS) regulado mediante Real Decreto 3/2010, de 8 de enero, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política de Seguridad de la Información, los órganos directivos responsables deben:

- Autorizar los sistemas o los servicios antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.

Detección.

Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, estos órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

Respuesta.

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

Recuperación.

Para garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5. MARCO NORMATIVO.

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

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.
- Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen del sector Público.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 1/2014, de Transparencia de Andalucía.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Modificado por Ley 39/2015 y RD 668/2015, de 17 de julio)
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración Electrónica.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de carácter personal.
- Orden HAP/1949/2014, de 13 de octubre, por la que se regula el Punto de Acceso General de la administración General del Estado y se crea su sede elctrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas.
- Decreto del Alcalde, de 17 de enero de 2005, por el que se regula la Atención al Ciudadano en el Ayuntamiento de Granada.
- Ordenanza de Administración Electrónica.(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.

- Normas aplicables a la Administración Electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información.

6. ESTRUCTURA.

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

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

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

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

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

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

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

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

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

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

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

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

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobados por el Responsable de

Seguridad de la Información o por los Responsables de la Información o los de los Servicios, según su ámbito de competencia.
Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

7.- ORGANIZACIÓN

La organización de la seguridad de la información en el Ayuntamiento de Granada queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.
La organización de la seguridad de la información en el Ayuntamiento de Granada está participada por:

- Junta de Gobierno Local
- Comité Municipal de Seguridad de la Información
- Coordinador del Comité Municipal de Seguridad de la Información
- Responsable del Sistema
- Responsable de Seguridad ENS
- Responsable de Seguridad LOPD
- Administrador/es de la Seguridad

7.1. Junta de Gobierno.

La Junta de Gobierno de la Ciudad de Granada, mediante la aprobación del presente Acuerdo, asegura el compromiso de las autoridades del Ayuntamiento de Granada en la aplicación del Esquema Nacional de Seguridad.

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

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

- Aprobar la Política de Seguridad de la Información del Ayuntamiento de Granada y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento los esquemas nacionales de interoperabilidad y seguridad.
- Constituir y realizar el nombramiento de los integrantes del Comité Municipal de Seguridad de la Información (comité MSI).
- Aprobar el desarrollo organizativo que permita el cumplimiento de los esquemas nacionales de interoperabilidad y seguridad en el ámbito de la organización municipal.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité MSI.

7.2. Comité Municipal de Seguridad de la Información

Una vez aprobada la Política de Seguridad de la Información se constituirá el Comité Municipal de Seguridad de la Información designado por la Junta de Gobierno Local.

El Comité MSI tiene las siguientes funciones:

- Elaborar y proponer las revisiones de la Política de Seguridad de la Información del Ayuntamiento de Granada, para su posterior aprobación por la Junta de Gobierno Local.
- Elaborar y proponer el desarrollo normativo que permita el cumplimiento de los esquemas nacionales de seguridad e interoperabilidad, en el ámbito de la organización municipal. Difundir los acuerdos aprobados por el Comité a toda la organización municipal
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Recabar de los Responsables de Seguridad informes relativos a incidentes de seguridad y velar y facilitar los medios necesarios para su resolución.
- Recabar de los Responsables de los departamentos municipales informes regulares del estado de seguridad de la información de la organización municipal y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la Junta de Gobierno Local.
- Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de los distintos departamentos municipales.
- Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica del Ayuntamiento de Granada. Velar porque la seguridad de la información sea parte del proceso de planificación de la organización municipal.
- Llevar a cabo acciones de concienciación, formación y motivación del personal municipal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos municipales, usuarios y ciudadanos y la protección de su información.
- Promover inversiones de carácter horizontal para garantizar la disponibilidad de recursos para atender a las diferentes necesidades de seguridad de la información.
- Realizar propuestas de racionalización del gasto en materia de seguridad en la utilización de medios electrónicos.
- Elaborar y proponer las políticas sectoriales que complementen a la política de seguridad de la información, en aras del cumplimiento de los esquemas nacionales de seguridad e interoperabilidad. Sin ánimo de exhaustividad, al menos habrán de ser desarrolladas las siguientes:
    - Política de privacidad
    - Política de firma electrónica y certificados electrónicos

- Política de redes sociales
- Política de gestión de documentos electrónicos

El funcionamiento de este Comité supone, al menos, el desempeño de los siguientes roles, que tendrán carácter permanente:

- Coordinador del Comité MSI
- Responsable de Seguridad ENS
- Responsable de Seguridad LOPD
- Responsable de Sistemas
- Responsable del área de recursos humanos
- Responsable del área jurídica

Cuando lo justifique la complejidad de la materia a tratar, bien de la información o del servicio, se pondrán convocar a los distintos responsables del servicio y de la información afecta.
El Coordinador del Comité Municipal de Seguridad de la Información -que se corresponderá con un nivel jerárquico de Coordinador General- será el responsable de impulsar la implementación de la presente Política. En particular, el Coordinador del Comité MSI ejercerá formalmente el rol de Responsable de Seguridad de la Información según lo previsto en el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad.

7.3.- Responsable de la Información y servicio

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

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

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

7.4.- Responsable de Seguridad ENS.

Corresponde al nivel de una Dirección Ejecutiva u Operativa.
Formalmente, y con carácter de representación del Ayuntamiento de Granada, la asunción de responsabilidades del rol de Responsable de Seguridad según lo previsto en el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad, lo ejercerá el Coordinador del Comité MSI.

El rol de Responsable de Seguridad ENS asumirá las siguientes funciones desde un punto de vista operativo y ejecutivo (no formal):

a) Asunción de las funciones incluidas en los artículos 10, 27.3, 34.6, Anexo I (apartado 2.3) y Anexo II (apartados 2.1.b y 2.2.b) del Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.
b) Adicionalmente este perfil será responsable operativo de todas aquellas cuestiones de índole tecnológico en el marco de la seguridad de la información municipal
c) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
d) Analizar y elevar al Comité Municipal de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.

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

En ningún caso estas funciones suponen una exoneración de la responsabilidad que corresponde al Responsable de la Información o Responsable del Servicio, así como de las obligaciones del personal.

7.5.- Responsable de Seguridad LOPD

Corresponde al nivel de una Dirección Ejecutiva u Operativa.
Formalmente, y con carácter de representación del Ayuntamiento de Granada, la asunción de responsabilidades del rol de Responsable de Seguridad según lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, lo ejercerá el Coordinador del Comité MSI.

El rol de Responsable de Seguridad LOPD asumirá las siguientes funciones desde un punto de vista operativo y ejecutivo (no formal):

a) Asunción de las funciones asignadas al Responsable de Seguridad en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, así como las previstas en el Documento de Seguridad del Ayuntamiento de Granada.
b) Adicionalmente este perfil será responsable operativo de todas aquellas cuestiones de índole jurídico en el marco de la seguridad de la información municipal

En ningún caso estas funciones suponen una exoneración de la responsabilidad que corresponde al Responsable de la Información o Responsable del Servicio, así como de las obligaciones del personal.

7.6.- Responsable de Sistemas

Corresponde al nivel de una Dirección Ejecutiva u Operativa en el ámbito de las Tecnologías de la Información y de las Comunicaciones.
Sus funciones serán 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) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas especificas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d) El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
e) Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
f) Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
g) Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité Municipal de Seguridad de la Información.

h) Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
i) Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

7.7.- Administrador de la Seguridad del Sistema

Corresponde al nivel de un empleado cualificado en seguridad informática de sistemas. Podrá nombrarse como tal a varias personas para cada Sistema.

Sus funciones serán las siguientes:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información, bajo la coordinación con el Responsable del Sistema.
b) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
c) Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
d) Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
e) Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
f) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
h) 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.
i) Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j) Monitorizar el estado de la seguridad del sistema.

7.7.- Grupo de Seguridad de la Información

En el marco de la presente Política, se constituye el grupo de seguridad de la información con el objetivo de abordar operativamente y canalizar cualquier actividad, actuación o incidente relativo a la seguridad de la información municipal y darle respuesta eficaz y eficiente desde un punto de vista multidisciplinar (tecnológico, jurídico, administrativo, etc..) o bien, caso de ser necesario, darle traslado informado al Comité MSI.
El grupo de seguridad de la información está constituído, al menos, por:

- Responsable de Seguridad ENS
- Responsable de Seguridad LOPD
- Responsable de Sistema
- Administradores de la Seguridad

Las funciones asociadas al grupo de seguridad de la información son:

a) Asistir y apoyar al Comité MSI en todas las tareas que le sean derivadas y encomendadas.
b) Abordar cualquier actuación en materia de seguridad de la información desde una perspectiva multidisciplinar, integrando enfoques y medidas de seguridad derivadas de la aplicación del ENS y de la aplicación de LOPD de forma consensuada.
c) Investigar, analizar, diseñar, recomendar y apoyar la implementación de las mejores prácticas de seguridad para las tecnologías de información, tanto de infraestructura como de procedimientos, así como medir su eficacia y eficiencia.
d) Coordinar el proceso de administración de incidentes de seguridad de la información en el ámbito de TI.

e) Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
f) Asesorar a las distintas áreas del Ayuntamiento en materia de seguridad de la información en el ámbito de TI.
g) Coordinar las funciones de gestión de riesgos de tecnologías de información.
h) Investigar, analizar, evaluar, diseñar, apoyar la implementación y monitorizar los procesos requeridos por el departamento de TI, mediante la utilización de las mejores prácticas relacionadas con el aseguramiento de la calidad informática.
i) Llevar a cabo acciones de concienciación, formación y motivación del personal municipal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos municipales, usuarios y ciudadanos y la protección de su información.

En el caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el Comité Municipal de la Seguridad de la Información atendiendo a las mayores exigencias derivadas de la seguridad de la información.

8.- ANÁLISIS Y GESTIÓN DE RIESGOS

8.1. Justificación

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.
El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

8.2. Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité Municipal de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.
Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.
Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.
Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

8.3. Directrices de tratamiento

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

8.4. Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.
Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de esa Información.
Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de ese Servicio.
Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité Municipal de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

8.5. Necesidad de realizar o actualizar evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.

9.- DATOS DE CARÁCTER PERSONAL.

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

10.- OBLIGACIONES DEL PERSONAL

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

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

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

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

11 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 Seguridad de la Información, se establecerán canales para el reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de 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 deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

12.-REVISIÓN.

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