AJUNTAMENT TORRENT
C/. Ramón y Cajal, 1 46900 – TORRENT (Valencia)
☎ 961111111 961111873
actes@torrent.es
www.torrent.es
torrent perlaconvivència

REGLAMENTO DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE

CAPÍTULO I. POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Artículo 1. Objeto del Reglamento

El objeto del presente Reglamento es regular las condiciones básicas para la aplicación de las necesarias medidas de seguridad para la protección de los datos de carácter personal y, en general, de toda la información existente en los sistemas municipales.

Su alcance será tanto los datos automatizados como los no automatizados o manuales, existentes o que se traten tanto por el propio Ayuntamiento como por los Organismos Públicos dependientes.

Artículo 2. Principios de la Seguridad de la Información

La política de Seguridad de la Información de la Corporación tiene por objetivo proteger sus activos de información contra todo tipo de amenazas, sean internas o externas, deliberadas o accidentales. La seguridad de la información se considera fundamental para el correcto funcionamiento de los servicios y sistemas de información. Esta política afecta a toda la información que pueda considerarse sensible para nuestra organización y, especialmente, los datos de carácter personal.

La necesidad de establecer distintas medidas que garanticen la seguridad de los ficheros que contengan datos de carácter personal viene recogida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD. El objeto de la LOPD es garantizar y proteger, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La finalidad del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 es, entre otras, establecer las medidas de seguridad de ficheros que contengan datos de carácter personal, tanto medidas técnicas como organizativas, que garanticen la seguridad de dichos datos y que han de cumplir tanto ficheros (manuales y automatizados), como centros de tratamiento o locales, equipos, sistemas, programas y personal que intervengan en el tratamiento de los datos. Entre las obligaciones para cualquier entidad responsable de ficheros con datos personales, como lo es la Corporación municipal, se encuentra la de elaborar e implantar esa normativa de seguridad mediante un documento de seguridad, de obligado cumplimiento para todo el personal con acceso a dichos datos y a los sistemas de información.

La política de seguridad de la información del Ayuntamiento seguirá cuatro principios básicos:

- Garantizar la privacidad de los datos de los ciudadanos.
- Proteger la información sensible.

- Asegurar el correcto funcionamiento de los sistemas de información.
- Cumplir la normativa vigente que sea aplicable.

Esta seguridad permitirá compartir información entre su personal, e incluso con terceros, pero garantizando su protección y los derechos de los afectados, siguiendo tres principios básicos que son esenciales para el correcto ejercicio de las funciones de la Corporación, su propia imagen y el cumplimiento de la legalidad vigente:

1. CONFIDENCIALIDAD: Se deben proteger los sistemas y la información contra accesos o divulgación no autorizados, asegurando que sólo quienes estén autorizados pueden acceder a la información. Todo el personal está obligado al deber de secreto en todo momento.

2. INTEGRIDAD: Se debe garantizar la exactitud de la información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta, asegurando que la información y sus métodos de proceso son exactos y completos. El principio de calidad de la información implica que los datos sean ciertos y puestos al día.

3. DISPONIBILIDAD: Se debe asegurar que los Sistemas y la Información puedan ser utilizados por los usuarios autorizados en la forma y tiempo requeridos; en la disponibilidad también se incluye su posible recuperación en caso de desastre (recuperación de copias de respaldo o backup).

La preservación de la confidencialidad, la integridad y la disponibilidad de la información, abarca además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad, el no repudio y la conservación de la información.

Artículo 3. Proporcionalidad de las medidas al nivel de confidencialidad

La información, con independencia de su naturaleza, soporte o ubicación, debería clasificarse para su correcto uso y gestión. Las medidas de seguridad que se apliquen deben ser proporcionales a dicha clasificación, que debe hacerse en virtud de su sensibilidad y/o criticidad; es decir, en función de su valor e importancia estratégica para la Corporación. Se deberían aplicar los siguientes cuatro niveles:

a. PÚBLICA: información de uso público y con la finalidad de ser distribuida. Su revelación no implica perjuicio a la Corporación ni a terceros.

b. INTERNA: informaciones que no han sido aprobadas para conocimiento público fuera del Ayuntamiento o del departamento propietario de la información. Suele ser accesible para un gran número de colaboradores, pero no está dirigida al público. Esta es la categoría por defecto en la que recaen todas las informaciones que no encajan claramente en ninguna otra.

c. RESTRINGIDA: información de uso propio de un área, departamento o proyecto, a la que no puede tener acceso el resto de la organización. Se aplicará a informaciones cuya difusión indebida puede acarrear perjuicios

financieros, consecuencias legales o daño en la imagen de la Corporación o de terceros.

d. CONFIDENCIAL: información sensible o que incluye datos de carácter personal. Debe estar protegida por su alta trascendencia, impacto financiero, potencial de fraude, consecuencias legales o daño en la imagen de la Corporación o de terceros. El acceso y la distribución de esta información debe estar controlado y la misma debe permanecer protegida en todo momento de la forma más segura posible.

Artículo 4. Ámbito de aplicación

El ámbito de aplicación de este Reglamento de Seguridad de los Sistemas de Información será todo tipo de actividad de la Corporación y los Organismos Públicos dependientes, relacionada con los datos protegidos, tanto en tratamientos manuales como automatizados.

Los recursos que, por servir de medio directo o indirecto para tratar los datos, están regulados por esta normativa son todos los sistemas de información de tratamiento de los ficheros protegidos, y en particular:

a) Los datos de los ficheros de carácter personal, declarados ante la Agencia Estatal de Protección de Datos (ya sean manuales, automatizados o mixtos), así como sus copias totales o parciales.
b) Las aplicaciones o programas informáticos establecidos, o que se establezcan en el futuro, para acceder y tratar dichos ficheros.
c) Los ordenadores y servidores (hardware) y el entorno de sistema operativo, bases de datos y comunicaciones (software), así como las redes de comunicaciones, con las que se traten los datos protegidos.
d) Los puestos de trabajo, tanto locales como remotos, desde los que se pueda tener acceso a algún dato protegido.
e) Los locales de ubicación o centros de tratamiento donde se encuentren ubicados los ordenadores que contienen ficheros protegidos.
f) Los almacenes de soportes o lugares donde se guarden los soportes que contengan copias totales o parciales de datos de los ficheros.
g) Los armarios, archivadores, cajones y resto de elementos de almacenamiento de documentos, así como los locales de archivo, donde existan datos bajo protección.
h) Los encargos, convenios o contratos con terceros (encargados del tratamiento) que accedan o traten datos personales por cuenta del Ayuntamiento.
i) Y en general todos los sistemas de información, manuales, automatizados o mixtos, con los que se traten los recursos protegidos.

CAPITULO II. ESTRUCTURA ORGANIZATIVA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 5. Responsable de los ficheros

Según la normativa vigente de protección de datos el responsable del fichero o tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

El responsable de los ficheros encomienda varias de sus funciones a la Junta de Seguridad de los Sistemas de Información, así como a los Responsables de Seguridad y a los Gestores de cada Fichero, según se indica en los siguientes artículos, manteniendo como sus obligaciones directas las siguientes:

a) Asegurar que todo tratamiento de datos de carácter personal que realice el Ayuntamiento y sus Organismos Públicos se hace con absoluto respeto a todos los principios legales y facilitando el ejercicio de los derechos por los afectados.

b) Promocionar y facilitar el cumplimiento de las políticas y medidas de seguridad de la información.

c) Facilitar todos los medios que razonablemente sean requeridos para implantar las medidas que se establezcan en el Documento de Seguridad, así como para la mejora continua de los controles de seguridad definidos.

Artículo 6. Junta de Seguridad de los Sistemas de Información

Para la gestión de la seguridad de la información en el Ayuntamiento y sus Organismos Públicos se establece la Junta de Seguridad de los Sistemas de Información del Ayuntamiento y sus Organismos Públicos (JSSI), compuesta por:

- Presidente: Concejal Delegado competente en materia de Régimen Interior e Información.
- Vocales:
  * Concejal Delegado competente en materia de Modernización.
  * Funcionario que esté designado como Responsable de Seguridad en sus aspectos legales.
  * Funcionario que esté designado como Responsable de Seguridad en sus aspectos técnicos o informáticos.
  * Otros dos funcionarios municipales.
- Secretario: Secretario de la Corporación o funcionario en quien delegue.

Mediante Decreto de Alcaldía se aprobarán los nombramientos para dicha Junta de Seguridad de los Sistemas de Información, así como los suplentes.

Artículo 7. Funciones de la Junta de Seguridad de los Sistemas de Información

La Junta de Seguridad de los Sistemas de Información del Ayuntamiento y sus Organismos Públicos (JSSI) tendrá atribuciones para realizar las siguientes funciones:

a) Definir el Documento de Seguridad de los Sistemas de Información de la Corporación, tal como se precisa en el siguiente capítulo de este Reglamento.

b) Definir y gestionar el plan de implantación de las normas establecidas en el Documento de Seguridad, tanto las organizativas y legales como las técnicas, con los cambios en los medios y formas de trabajo que se precisen.

c) Difundir las normas del Documento de Seguridad para que todo el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como de las consecuencias en que pudiera incurrir en caso de incumplimiento. Adicionalmente, preparará y organizará la difusión periódica de información sobre seguridad (circulares, recordatorios, nuevas normas, u otros).

d) Vigilar el cumplimiento por toda la Corporación de las normas y procedimientos establecidos para la seguridad de la información. Promocionar el cumplimiento y la mejora continua de los controles de seguridad que se definan y que todas dichas medidas se mantengan operativas.

e) Coordinar y asegurar que se contestan adecuadamente en plazo y forma todas las posibles solicitudes de Acceso, Rectificación, Cancelación u Oposición que presenten los afectados.

d) Preparar, para todos los ficheros con datos personales, su correspondiente Disposición General Reguladora según el Real Decreto 1720/2007 y comprobar que se ha aprobado por el órgano de gobierno adecuado, se ha publicado y se ha notificado al Registro General de Protección de Datos de la Agencia Española de Protección de Datos, manteniendo actualizadas las inscripciones de ficheros en el mismo. También adoptará las medidas que corresponda para evitar que se inicie la recolección de datos personales para un fichero sin que se cumplan previamente las obligaciones legales.

f) Vigilar que se mantiene actualizado el Documento de Seguridad, y en general toda la normativa interna, adaptada a los cambios que se produzcan en la Corporación, en sus sistemas de información y en los ficheros, así como a la legislación o normativa aplicable.

g) Requerir que se realicen todas las revisiones periódicas de verificación que se indiquen en el Documento de Seguridad (especialmente la auditoria bienal obligatoria) y analizar los Informes periódicos de los Responsables de Seguridad, así como tomar las decisiones que correspondan. Colaborar activamente para la realización de dichas revisiones, así como procurar todos

los medios requeridos razonablemente para subsanar las deficiencias que se detectaran en dichas revisiones. Elevará los informes que se consideren oportunos a Alcaldía.

h) Analizar las incidencias de seguridad que se puedan producir, con los informes de los Responsables de Seguridad y del Gestor o Gestores afectados, y tomar las medidas precisas para paliar su impacto y evitar su repetición.

Artículo 8. Responsables de Seguridad de los Sistemas de Información

Los Responsables de Seguridad son los encargados de coordinar y controlar las medidas definidas en Documento de Seguridad de los Sistemas de Información. Uno será el encargado de los aspectos legales, y el otro de los aspectos técnicos o informáticos. Ambos tendrán funciones asignadas sobre todos los ficheros o tratamiento de datos personales, tanto automatizados como manuales.

En ningún caso esta designación supondrá una exoneración de la responsabilidad que corresponde al Responsable de los Ficheros, de acuerdo con lo establecido en la normativa vigente.

Mediante Decreto de Alcaldía se aprobarán los nombramientos de estos Responsables de Seguridad de los Sistemas de Información.

Artículo 9. Responsable de Seguridad Legal de los Sistemas de Información

Son funciones y obligaciones del Responsable de Seguridad Legal, siempre en permanente coordinación con el Responsable de Seguridad Técnica, las siguientes:

a) Definir y proponer a la JSSI, las normas o procedimientos de tipo legal referentes a la seguridad de los Sistemas de Información, así como los cambios posteriores de las mismas (entre otras posibles, la regulación de los nuevos ficheros y su inscripción, el deber de información en la recopilación de datos, las cláusulas de confidencialidad en los contratos con terceros y el tratamiento de solicitudes de acceso, rectificación, cancelación y oposición o la normativa sobre videovigilancia).

b) Difundir, cumplir y hacer cumplir todas las normas de seguridad de tipo legal que se establezcan en el Documento de Seguridad para los Ficheros protegidos. Especialmente promover y coordinar la puesta en marcha de dichas normas.

c) Controlar el cumplimiento de la normativa de seguridad en sus aspectos legales, realizando todas las verificaciones periódicas que considere oportunas para comprobar las normas y recursos de seguridad.

d) Ante cualquier incidencia o incumplimiento de la normativa de aspectos legales, se encargará de su anotación en el Registro de Incidencias y, junto

con el Gestor del Fichero que correspondiera, de la investigación del problema, de los planes de actuación y métodos de aislamiento de la incidencia y de las acciones correctoras y preventivas oportunas.

e) Preparar las contestaciones a todas las posibles solicitudes de Acceso, Rectificación, Cancelación u Oposición que presenten los afectados, coordinando a los servicios afectados y asegurando que se contestan adecuadamente en plazo y forma.

f) Aquellas otras tareas o funciones que le encargue la Junta de Seguridad de los Sistemas de Información, a la cual informará en todo caso de sus actuaciones.

El Responsable de Seguridad Legal contará con la colaboración del personal de Asesoría Jurídica y de Secretaría y Administración General (internos o externos) para la realización de todas las tareas asignadas, pero siempre llevando a cabo él mismo la labor de supervisión.

Artículo 10. Responsable de Seguridad Técnica de los Sistemas de Información

Son funciones y obligaciones del Responsable de Seguridad Técnica, siempre en permanente coordinación con el Responsable de Seguridad Legal, las siguientes:

a) Definir y proponer a la JSSI, las normas o procedimientos de tipo técnico, organizativo e informático referentes a la seguridad de los Sistemas de Información, así como los cambios posteriores de las mismas

b) Difundir, cumplir y hacer cumplir todas las normas de seguridad de tipo organizativo e informático que se establezcan en el Documento de Seguridad para los Ficheros protegidos. Especialmente promover y coordinar la puesta en marcha de dichas normas.

c) Controlar el cumplimiento de la normativa de seguridad en sus aspectos organizativos e informáticos, realizando todas las verificaciones periódicas que considere oportunas para comprobar las normas y recursos de seguridad.

d) Promover e implantar todas aquellas medidas de seguridad de protección de datos que considere oportunas para incrementar la seguridad y mejorar las normas del Documento de Seguridad. En especial:

   i. Promover e implantar cuantas medidas preventivas, de vigilancia o correctivas considere adecuadas para garantizar la seguridad de los Ficheros y recursos protegidos (confidencialidad, integridad y disponibilidad).
   ii. Implantar los controles y medios técnicos necesarios para impedir la instalación de productos o programas o cualquier otro dispositivo, que permita o facilite el incumplimiento de las medidas de seguridad que se establezcan en el Documento de Seguridad.

iii. Vigilar el correcto uso de los medios puestos a disposición de los usuarios.
iv. Informar a la JSSI y a los Gestores de los Ficheros que pudieran estar afectados, de los nuevos controles técnicos que se instalen y cualquier desviación o anomalía detectada en los existentes.

e) Habilitar y mantener el Registro de Incidencias. Ante cualquier incidencia de seguridad en la protección de la información, se encargará de registrarla y, junto con el Gestor del Fichero que correspondiera, de la investigación del problema, de los planes de actuación y métodos de aislamiento de la incidencia y de las acciones correctoras y preventivas oportunas.

g) Aquellas otras tareas o funciones que le encargue la Junta de Seguridad de los Sistemas de Información, a la cual informará en todo caso de sus actuaciones.

El Responsable de Seguridad Técnica (o Informática) contará con la ayuda del personal del Servicio de Modernización y Telecomunicaciones, o Administradores de Sistemas (internos o externos), para la realización de todas las tareas de tipo técnico, pero siempre llevando a cabo él mismo la labor de supervisión.

Artículo 11. Gestores de ficheros

Cada fichero con datos personales tendrá asignado un Gestor del Fichero (que podrá coincidir con el encargado del departamento, servicio o unidad de la Corporación que trate dicho Fichero), el cual actuará siempre por delegación del Responsable del Fichero. Cada Gestor tiene encomendada la protección de sus Ficheros.

Mediante Decreto de Alcaldía se aprobarán los nombramientos para estos Gestores de Ficheros.

Son funciones de cada Gestor de Fichero, sin menoscabo de las indicadas en otros artículos de este Reglamento, las siguientes:

a) Proteger sus Ficheros con datos personales, según el nivel asignado para su protección. Para ello deberá cumplir y hacer cumplir en el ámbito de sus competencias todas las normas que se establezcan en el Documento de Seguridad para sus Ficheros.

b) Informar de la normativa de seguridad y de la obligatoriedad de su cumplimiento a todos los usuarios de los Sistemas de Información de su servicio o unidad, tanto usuarios ya existentes como nuevos, a los que se les haya dado, o se les vaya a dar, autorización de acceso a algún datos protegido.

c) Promover todas aquellas mejoras en las medidas de seguridad de la información que considere oportunas para incrementar la calidad de los datos y mejorar las normas del Documento de Seguridad, proponiendo los cambios al mismo y en el resto de la normativa interna, que considere adecuados.

d) Colaborar con la JSSI, y especialmente con los Responsables de Seguridad, en todas las cuestiones que razonablemente estos le soliciten.

h) Aquellas otras tareas o funciones que le encargue la Junta de Seguridad de los Sistemas de Información.

CAPÍTULO III. EL DOCUMENTO DE SEGURIDAD

Artículo 12. El Documento de Seguridad de los Sistemas de Información

La Corporación debe disponer de un Documento de Seguridad de los Sistemas de Información que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, y que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

La Junta de Seguridad de los Sistemas de Información se encargará de definir el Documento de Seguridad de los Sistemas de Información del Ayuntamiento y sus Organismos Públicos, con las normas o instrucciones, formularios y registros. El mismo deberá mantenerse en todo momento actualizado y deberá revisarse siempre que se produzcan cambios relevantes en los Sistemas de Información o en la organización de los mismos, así como deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Adicionalmente, los Responsables de Seguridad podrán provisionalmente implantar aquellas mejoras técnicas u organizativas que, de forma motivada, bien por su escaso impacto o tamaño o bien por su urgencia, no sea aconsejable esperar a la edición y aprobación de una nueva versión de la norma que correspondiera del Documento de Seguridad. En todo caso, se deberá emitir dicha nueva versión de esa norma en un plazo razonable.

No se podrá utilizar ningún dato de carácter personal para fines distintos de los especificados en su finalidad, según la inscripción de cada Fichero en el registro de la Agencia Estatal de Protección de Datos.

Todos los empleados y colaboradores internos y externos de la Corporación, y en general cualquier persona que tenga acceso a los datos de los Ficheros protegidos, bien a través de los Sistemas de información habilitados para acceder a los mismos, o bien a través de cualquier otro medio de acceso, estarán obligados a cumplir lo establecido en dicho Documento de Seguridad y sujetos a las consecuencias en que pudieran incurrir en caso de incumplimiento.

Igualmente, todos los usuarios, y todos los que intervengan en cualquier fase del tratamiento de los datos de carácter personal (incluidos los posibles externos encargados del tratamiento, contratistas o colaboradores) están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que

subsistirán aun después de finalizar sus relaciones con el Ayuntamiento u Organismo Público que correspondiera.

Artículo 13. Contenido del Documento de Seguridad de los Sistemas de Información

El Documento de Seguridad de los Sistemas de Información deberá al menos incluir todas las medidas y normas a las que obligue la normativa vigente. Entre otras posibles deberá contener:

a. Identificación del alcance y recursos protegidos por la normativa interna: con las normas adecuadas para mantener identificados los ficheros con datos personales, los sistemas de información, las aplicaciones informáticas con las que se traten los datos protegidos, los locales de ubicación de dichos datos, tanto automatizados como no, y aquellos otros que se vean adecuados

b. Protección física y del entorno: incluyendo entre otras las medidas de seguridad para el puesto de trabajo, controles de red, locales de ubicación con acceso restringido, trabajo con datos fuera de los locales habituales.

c. Controles de acceso a los Sistemas de Información: como identificación y autenticación, Intentos reiterados de acceso, registro automático de accesos a ficheros de nivel alto, asignación de permisos y lista de usuarios autorizados

d. Gestión de Soportes informáticos, dispositivos portátiles, transmisiones y copias de datos protegidos: que incluirá las normas que se consideren oportunas, tales como autorizaciones y registro de entradas y salidas de soportes y transmisiones, controles sobre dispositivos portátiles, copias o ficheros temporales con datos de carácter personal.

e. Continuidad de las operaciones y copias de respaldo, con las medidas de seguridad tanto de datos automatizados como de redes y equipos para asegurar unos servicios mínimos ante una incidencia, así como la recuperación de los datos.

f. Desarrollo y mantenimiento de sistemas automatizados, con instrucciones para la seguridad en el desarrollo de software, pruebas sin datos reales, gestión del cambio de aplicaciones o sistemas, u otros que se consideren adecuados a una organización como el Ayuntamiento de Torrent y sus Organismos Públicos.

g. Tratamiento de Ficheros no automatizados o documentos en papel, con las medidas comunes para toda documentación en papel y aquellas otras para los datos especialmente protegidos.

h. Normas de uso de Internet y del correo electrónico para los usuarios de la Corporación, detallando las dirigidas a la privacidad, la seguridad de estos

servicios y el bloqueo de contenidos. Se definirán normas específicas para la posible cancelación de estos servicios ante situaciones de riesgo para la seguridad o ante incumplimientos de la legislación vigente, así como la posibilidad de acceder al contenido de los correos electrónicos por los órganos municipales competentes.

i. Normas para facilitar el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

j. Normas para informar al afectado de sus derechos en la recogida datos, envíos de información y Videovigilancia.

k. Normativa para regular el acceso a los datos protegidos por terceros, o el tratamiento por los mismos, como las cláusulas de tratamiento confidencial.

l. Tratamiento de incidencias, con normativa para su notificación y registro.

m. Controles e informes periódicos de evaluación de la normativa de seguridad, con las verificaciones e informes oportunos que permitan tanto vigilar el cumplimiento de la normativa como potenciar su mejora.

DISPOSICION FINAL

Única.- El presente Reglamento entrará en vigor a los quince días hábiles de la publicación de su texto íntegro en el Boletín Oficial de la Provincia de Valencia.

* APROBACIÓN INICIAL PLENO 11 JUNIO 2009
* APROBACIÓN DEFINITIVA DECRETO 2510/2009
* EDICTO B.O.P. 31 OCTUBRE 2009